UNIVERSITY OF
NOVI SAD

FACULTY OF
TECHNICAL SCIENCES

Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure

- Ph. D. Thesis -

Supervisor:	Candidate:
Goran Sladić, PhD, full professor	Milan Stojkov

Novi Sad, 2022.

Milan Stojkov: *Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure*

SERBIAN TITLE:
Model za praćenje usklađenosti između bezbednosnih standarda i prioritizaciju zahteva u kritičnim infrastrukturama

SUPERVISOR:
Goran Sladić, PhD, full professor

LOCATION:
Novi Sad, Serbia

DATE:
May 2022

UNIVERZITET U NOVOM SADU **OBRAZAC - 5a**
FAKULTET TEHNIČKIH NAUKA

KLjUČNA DOKUMENTACIJSKA INFORMACIJA[1]

Vrsta rada:	Doktorska disertacija
Ime i prezime autora:	Milan Stojkov
Mentor (titula, ime, prezime, zvanje, institucija)	dr Goran Sladić, redovni profesor, Fakultet tehničkih nauka
Naslov rada:	Model za praćenje usklađenosti između bezbednosnih standarda i prioritizaciju zahteva u kritičnim infrastruktirama
Jezik publikacije (pismo):	Engleski jezik, latinica
Fizički opis rada:	Stranica: 222/Poglavlja: 5/Referenci: 212/Tabela: 18/ Slika: 12/Grafikona: 0/Priloga: 0
Naučna oblast:	Elektrotehničko i računarsko inženjerstvo
Uža naučna oblast (naučna disciplina):	Primenjene računarske nauke i informatika
Ključne reči / predmetna odrednica:	zaštita kritičnih infrastruktura, standardi, usklađenost sa standardima, bezbednosni zahtevi, prioritizacija zahteva

[1] Autor doktorske disertacije potpisao je i priložio sledeće Obrasce:
5b – Izjava o autorstvu;
5v – Izjava o istovetnosti štampane i elektronske verzije i o ličnim podacima;
5g – Izjava o korišćenju.
Ove Izjave se čuvaju na fakultetu u štampanom i elektronskom obliku i ne koriče se sa tezom.

Rezime na jeziku rada:	Disertacija se bavi istraživanjem u oblasti informacione bezbednosti. Prikazan je model koji uniformno predstavlja gradivne jedinice bezbednosnih zahteva koji su definisani u različitim standardima, stručnim smernicama i regulativama za kritične infrastrukture. U tu svrhu analizirane su strukture zahteva najzastupljenijih standarda. Model je proširen komponentama za prioritizaciju i istovremeno praćenje implementacije i usklađenosti sličnih zahteva izabranih iz različitih bezbednosnih publikacija. Definisana su četiri kriterijuma za prioritizaciju odabira zahteva za implementaciju: rezultat analize rizika, zavisnosti između učesnika zaduženih za implementaciju zahteva, nivo važnosti zahteva za usklađenost i pripadnost zahteva odgovarajućem domenu. Takođe je definisan radni okvir sa skupom aktivnosti koje prate elemente predloženog modela za potrebe demonstracije njegove praktične primenjivosti.
Datum prihvatanja teme od strane nadležnog veća:	04/11/2021
Datum odbrane: (Popunjava odgovarajuća služba)	
Članovi komisije: (titula, ime, prezime, zvanje, institucija)	**Predsednik:** dr Miroslav Zarić, vanredni profesor, Fakultet tehničkih nauka Novi Sad **Član:** dr Aleksandar Erdeljan, redovni profesor, Fakultet tehničkih nauka Novi Sad **Član:** dr Vladimir Vujović, vanredni profesor, Elektrotehnički fakultet u Istočnom Sarajevu **Član:** dr Željko Vuković, docent, Fakultet tehničkih nauka Novi Sad **Mentor:** dr Goran Sladić, redovni profesor, Fakultet tehničkih nauka Novi Sad
Napomena:	

UNIVERSITY OF NOVI SAD
FACULTY OF TECHNICAL SCIENCES

KEY WORD DOCUMENTATION[2]

Document type:	Doctoral dissertation
Author:	Milan Stojkov
Supervisor (title, first name, last name, position, institution)	Ph.D. Goran Sladić, Full Professor, Faculty of Technical Sciences
Thesis title:	Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure
Language of text (script):	English language, latin script
Physical description:	Pages: 222/Chapters: 5/References: 212/Tables: 18/ Illustrations: 12/Graphs: 0/Appendices: 0
Scientific field:	Electrical and computer engineering
Scientific subfield (scientific discipline):	Applied Computer Science and Informatics
Subject, Key words:	Critical Infrastructure Protection, standards, standard compliance, security requirements, requirement prioritization

[2] The author of doctoral dissertation has signed the following Statements:
5б – Statement on the authority,
5в – Statement that the printed and e-version of doctoral dissertation are identical and about personal data,
5г – Statement on copyright licenses.
The paper and e-versions of Statements are held at the faculty and are not included into the printed thesis.

Abstract in English language:	This thesis presents research in the field of information security. We present a model that uniformly represents the building blocks of the security requirements that are defined in various standards, security guidelines, and regulations for Critical Infrastructure. We analyze the structure of the requirements in the most commonly used standards for this purpose. We have extended the model with components to prioritize and track the implementation and compliance of similar requirements selected from different security publications. We define prioritization criteria for selecting the requirements for implementation that rely on four factors: risk assessment results, essence levels of the requirements set that is analyzed, dependency graph of the social actors involved in the implementation, and the domain affiliation of the requirement. We also define a framework with a set of activities that follow the elements of the proposed model to demonstrate its practical applicability.
Accepted on Scientific Board on:	04/11/2021
Defended: (Filled by the faculty service)	
Thesis Defend Board: (title, first name, last name, position, institution)	**President:** Ph.D. Miroslav Zarić, Associate Professor, Faculty of Technical Sciences, Novi Sad **Member:** Ph.D. Aleksandar Erdeljan, Full Professor, Faculty of Technical Sciences, Novi Sad **Member:** Ph.D. Vladimir Vujović, Associate Professor, Faculty of Electrical Engineering, Istočno Sarajevo **Member:** Ph.D. Željko Vuković, Assistant Professor, Faculty of Technical Sciences, Novi Sad **Supervisor:** Ph.D. Goran Sladić, Full Professor, Faculty of Technical Sciences, Novi Sad
Note:	

Acknowledgements

Throughout the writing of this thesis, I have received a great deal of support and assistance.

I would first like to thank my supervisor, Professor Goran Sladić, whose expertise was invaluable in formulating the research questions and who ultimately pushed me to finish my thesis. Your insightful feedback allowed me to sharpen my thinking and brought my work to a higher level.

I would like to acknowledge my colleagues, both from academia and industry, for their support, patience, and the opportunity for collaboration.

Finally, I would like to thank my parents and friends for their unconditional love and support. You are always there for me.

Abstract

Modern systems are constantly under cyber and physical threats. The harm that can be done to power grids, transport networks, and information and communication systems is indescribable. These systems are essential for the maintenance of vital societal functions, and their malfunction may negatively impact the security of one country and its citizens. We call them Critical Infrastructure systems. To protect them, they must implement sophisticated security controls. Doing this without guidance or traceability can create a false sense of security. Security standards, guidelines, and regulations provide a systematic approach to protecting critical assets. They facilitate security knowledge and best practices that can provide a satisfactory level of security. The emergence of new threats forces regulatory bodies to increase the number of standards. Often, product providers that operate in multiple geographical regions face the obligation to comply with multiple standards simultaneously. This situation can introduce ambiguity within organizations regarding which standards they should align with and understand their similarities and differences. These activities also include planning, prioritizing, and tracking requirement implementation. Further, to enhance the security of the system or organization by satisfying security requirements, understanding the risks that they must address is essential. We address these issues and provide steps for conducting the mentioned activities through this research.

We perform a comprehensive analysis of the requirements from different security standards and guidelines. We find that the structure of the requirements is similar and propose the definition of an extensible model that can represent new requirements from the arbitrary standards applicable to the critical infrastructure sectors. During the analysis, we go through the existing models, frameworks, and tools to detect their advantages and limitations to accumulate that knowledge and propose solutions. We define our methodology for model definition and its extension. It starts with the description of security standards, guidelines, and regulations selection process. Further, we discuss the outputs of the analysis and how they can be used as elements of our model. Then we define our implementation prioritization criteria. It relies on four factors: risk assessment results, essence levels of the requirements set that is analyzed, dependency graph of the social actors involved in the implementation, and the domain affiliation of the requirements. Next, we present the framework that uses the proposed model to confirm the practical applicability of the model and to identify its advantages and eventual limitations. For each framework activity, we present security concepts and explain their contribution. Finally, we evaluate our approach through a case study where we demonstrate the applicability of the model and framework to the one Smart Grid standard.

Keywords: Critical Infrastructure Protection, standards, standard compliance, security requirements, requirement prioritization

Rezime

U proteklim decenijama, sistemi koji treba da olakšaju svakodnevni život pogođeni su promenama koja je donela digitalna revolucija. Upravljanje potrošnjom dobara poput električne energije, nafte, gasa, ili vode postalo je mnogo lakše i efikasnije. Upravo takvi sistemi predstavljaju mete od interesa za maliciozne aktere, koji vođeni raznim motivima podstiču na digitalni rat. Zbog toga organizacije posebnu pažnju posvećuju bezbednosti svojih sistema i resursa. Ovde se posebno ističu sistemi koji se zajedničkim imenom nazivaju kritične infrastrukture (engl. Critical Infrastructure). Evropska komisija definiše kritične infrastrukture kao *resurse ili sisteme koji su suštinski važni za održavanje vitalnih društvenih funkcija i nad kojima načinjena šteta, usled prirodnih katastrofa, terorizma, kriminalnih aktivnosti ili malicioznih radnji, može imati dalekosežni negativni uticaj po bezbednost Evropske Unije i opšte dobro njenih stanovnika* [9]. U tu grupu spadaju sistemi električnih mreža, vode, gasa i nafte, nuklearni, transportni, hemijski, zdravstveni, finansijski sistemi i mnogi drugi. Akcenat ove disertacije je upravo na prepoznavanju i rešavanju nekih od bezbednosnih izazova sa kojima se takvi sistemi susreću.

Napadi su sve više usredsređeni na operacione tehnologije (engl. Operatation Technology — OT) i industrijske kontrolne sisteme (engl. Industrial Control Systems — ICS) koji se koriste za upravljanje kritičnim infrastrukturama. Godinama unazad, sektori kritičnih infrastruktura postali su dosta zavisni od industrijskih kontrolnih sistema kao što su SCADA (engl. Supervisory Control and Data Acquisiton),

PLC (engl. Programmable Logic Controllers) i distribuiranih kontrolnih sistema (engl. Distributed Control Systems – DCS) za nadzor, kontrolu i upravljanje fizičkim uređajima poput senzora, pumpi, ventila, brojila, itd. Takođe, ovi sistemi se često integrišu sa drugim sistemima namenjenim za poslovanje kao što su platni sistemi, informacioni sistemi, kao i svi drugi koji pored namenskog (industrijskog) zahtevaju korišćenje i hardvera i softvera opšte namene. Komunikacija između takvih sistema postaje neizbežna, ali ujedno stvara i veliki izazov da se sistemi adekvatno obezbede. U prošlosti su se sistemi kritičnih infrastruktura projektovali sa fokusom na bezbednost, pouzdanost i dostupnost, pri čemu su glavne bezbednosne kontrole bile fizičke kapije i brave. Time je stvorena pogrešna slika da su sistemi bezbedni i da se njihova bezbednost ne treba unapređivati. Ovome doprinosi i činjenica da u javnosti nije bilo previše informacija o napadima do pre nešto više od jedne decenije. Stuxnet je jedan od najpoznatijih i najkomplikovanijih napada na industrijske kontrolne sisteme otkriven 2010. godine [24]. Cilj napada bio je da se nanese šteta iranskim nuklearnim sistemima. Meta su bile Windows mašine povezane sa PLC kontrolerima gde je preko 14000 mašina inficirano iskorišćavanjem ranjivosti i postepenim napredovanjem kroz celokupni sistem. Sličnih primera ima još, ali uglavnom sa malo tehničkih detalja. Luiijf i Klaver opisuju alat sa bazom podataka o incidentima u sistemima kritičnih infrastruktura koja je popunjavana u intervalu od 15 godina, gde navode da je većina informacija došla iz medija i zvaničnih izveštaja koji nisu bili toliko detaljni [31]. Zbog svoje velike važnosti, energetski sektor se navodi kao jedna od glavnih meta napada u sklopu kritičnih infrastruktura. Centar za studije rizika Univerziteta u Kembridžu i osiguravajuća kuća Lloyd kreirali su hipotetički scenario za nestanak struje u Sjedinjenim Američkim Državama koji bi mogao da pogodi američku ekonomiju sa 243 milijarde dolara štete, a koja se u najekstremnijoj verziji može popeti na hiljadu milijardi [32]. Kako bi se ublažila potencijalna šteta, svi ti sistemi moraju biti zaštićeni postavljanjem bezbednosnih mehanizama i održavanjem bezbednosti na svim slojevima sistema (engl. defense in depth). Primenjeni mehanizmi doprinose zaštiti ljudi, procesa i tehnologija koje se koriste. Podizanje bezbednosnih postavki organizacija i kritičnih sistema može se ostvariti kombinovanjem različitih pristupa neophodnih za očuvanje nacionalne bezbednosti i ekonomije. Svi mehanizmi zajedno mogu se posmatrati kao principi zaštite kritičnih infrastruktura (engl. Critical Infrastructure Protection – CIP), a mogu se postići korišćenjem različitih tehnika [45]:

- širenjem baze znanja i razmenom informacija;
- redovnom procenom ranjivosti sistema i pojačavanjem bezbednosnih kontrola;
- testiranjem različitih hipotetičkih scenarija napada i odbrana;
- redovnom revizijom korišćenih bezbednosnih kontrola;
- implementacijom bezbednosnih kontrola definisanih kroz zahteve relevantnih bezbednosnih standarda.

Razmena informacija jedan je od pristupa za širenje baze znanja o novim trendovima na poljima napadačkih i odbrambenih tehnika. Ova aktivnost prepoznata je i na nacionalnom nivou, te danas postoje organizacije poput nacionalnih CERT tela (engl. Computer Emergency Response Team) ili još specifičnijih tela poput Centra za analizu i razmenu informacija o električnoj energiji u Sjedinjenim Američkim Državama (engl. Electricity Information Sharing and Analysis Center – E-ISAC), Centra za analizu i razmenu informacija o nafti i prirodnom gasu (engl. Oil and Natural Gas Information Sharing and Analysis Center – ONG-ISAC) i sličnih tela u zemljama Evropske Unije, Japanu, Kanadi, itd. Ovakav vid saradnje predstavlja dobar pristup za jačanje veza između različitih entiteta kritičnih infrastruktura. Učesnici u razmeni informacija su razni, od državnih tela, preko privatnih sistema kritičnih infrastruktura i IT kompanija, do nezavisnih istraživača. Razmena informacija može imati i negativne efekte na kompanije. Campbell i drugi [53] u svojoj studiji ispituju ekonomske posledice po organizacije posle objava o bezbednosnim propustima i nalaze dokaze o negativnom uticaju na cene akcija na berzi.

Odeljenje za unutrašnju bezbednost Sjedinjenih Američkih Država (engl. The United States Department of Homeland Security) objavilo je u svojim dokumentima nacionalnu bezbednosnu strategiju koja prepoznaje procene ranjivosti sistema kao ključne aktivnosti za zaštitu kritičnih infrastruktura [55, 56]. Redovne procene ranjivosti sistema i ofanzivno penetraciono testiranje su aktivnosti koje treba redovno sprovoditi i koje omogućuju unapređenje zrelosti postavljenih odbrambenih mehanizama. Pošto su ove tehnike invazivne, ne preporučuje se njihovo izvođenje u produkcionom okruženju, već u odgovarajućim sistemima za testiranje [58]. Prednosti redovnih sprovođenja ovih aktivnosti su razne: identifikacija poznatih ranjivosti pre napadača, kreiranje spiska inventara svih korišćenih uređaja u mreži, prepoznavanje rizika koji postoje u sistemu, ušteda vremena i resursa, usaglašavanje sa zahtevima bezbednosnih standarda i regulativa, itd. Koristeći rezultate ovih aktivnosti moguće je i kvantifikovati verovatnoću napada [63].

Testiranje različitih hipotetičkih scenarija napada i odbrana dodatni je pristup koji može imati svoje prednosti za podizanje spremnosti organizacija za pravovremene reakcije. Ove aktivnosti mogu se organizovati na nacionalnom nivou ili samo sa pojedinim organizacijama koje upravljaju kritičnim sistemima. Franchina i drugi [65] navode da je jedan od načina za zaštitu kritičnih infrastruktura implementacija programa edukacije i organizovanja treninga iz oblasti bezbednosti. Kao primere prezentuju različite aktivne i pasivne tehnike od organizovanja seminara, do vežbi koje se izvode uz pomoć računara i specijalizovanih softvera. U energetskom sektoru su poznati događaji poput GridEx [68] koji organizuje NERC (engl. North American Electric Reliability Corporation) i Cyber Storm [69] koji organizuje CISA (engl. Cybersecurity and Infrastructure Security Agency).

Redovne revizije predstavljaju sistemski pristup ispitivanju bezbednosti organizacije, njenih zaposlenih, procesa i sistema. One uključuju provere korišćenih bezbednosnih kontrola, upravljačkih praksi, prepoznatih rizika i usklađenosti sa različitim standardima i regulativama na nivou sistema ili kompletne organizacije. Revizije su zamišljene kao formalniji vid provere koji se sastoji od prolaska kroz listu zahteva koja proverava da li su bezbednosni mehanizmi implementirani i funkcionišu kako je to definisano različitim standardima ili najboljim preporukama. Potreba za bezbednosnim revizijama može biti vođenja različitim motivima, od toga da se prethodno desio bezbednosni incident, do promena koje diktiraju standardi uvođenjem novih i redefinisanjem postojećih zahteva. Sa druge strane, sprovođenje bezbednosnih revizija ima i dosta prednosti pošto se na taj način formalno testiraju bezbednosne kontrole, identifikuju procepi u bezbednosnim postavkama, proverava usklađenost sa standardima i najvažnije, navodi na redovno sprovođenje analize rizika.

Države širom sveta prepoznale su važnost računarske bezbednosti i u te svrhe razvijeni su različiti standardi, regulative i preporuke koje će specificirati odgovarajuće bezbednosne zahteve. Bezbednosni standardi i preporuke publikovani od strane eminentnih tela kao što su ISO (engl. International Organization for Standardization), NIST (engl. National Institute of Standards and Technology) i Centar za Internet bezbednost (engl. Center for Internet Security – CIS) predstavljaju važne kolekcije akumuliranog znanja pretočenog u formalne zahteve koji mogu da pomognu vladinim i privatnim organizacijama ne samo da povećaju nivo bezbednosti svojih kritičnih infrastruktura, već i da dobiju javnu potvrdu za to u vidu priznatih sertifikata. Prvi standardi bili su više tehnički orijentisani poput tzv. “Narandžaste knjige” (engl. the Orange Book) [73] i provera usaglašenosti bezbednosnih kontrola sa zahtevima bila je mnogo rigoroznija. Proces sertifikacije sprovodili su državni organi, a procenu su radili eksperti u saradnji sa samim korisnicima. Kasnije je došlo do ekspanzije broja standarda i stručnih smernica koji su u zahtevima razmatrali i menadžerske aspekte. Negativna strana povećavanja broja raspoloživih standarda je pad u transparentnost pri evaluaciji. Danas postoje sertifikacione kuće koje vrše usluge provere usaglašenosti sa zahtevima. One mogu da isključe korisnike iz samog procesa sertifikacije i definišu svoje kriterijume za procenu kao i cenu usluge. Bez obzira na proces sertifikacije, veći broj zahteva obezbedio je veću pokrivenost domena koji treba da budu zaštićeni. Implementacijom standardizovanih kontrola propisanih standardima dobija se veće poverenje klijenata, snabdevača i partnera u sposobnost organizacije da reaguje na nove bezbednosne izazove. Ipak, u praksi se ispostavlja da sistematski pristup očuvanju bezbednosti koji standardi propisuju nije zaživeo. Izveštaj američkih državnih tela [81] pokazuje da su svega tri sektora kritičnih infrastruktura (sistemi voda i otpadnih voda, državne ustanove i vojne industrijske baze) u većoj meri poprimile upotrebu NIST radnog okvira za unapređenje bezbednosti kritičnih infrastruktura (engl. Framework for Improving Critical Infrastructure Cybersecurity) koji važi za jedan sveobuhvatan skup smernica za očuvanje bezbednosti sistema [82].

Bitno je napomenuti da se prethodno pomenute revizije i standardi u velikom broju slučajeva dopunjuju. Obično zvanične revizije koje za cilj imaju sertifikaciju organizacije ili sistema prate zahteve određenih standarda koji su u širokoj upotrebi i imaju uglavnom zadovoljavajuću strukturu. Odabir i implementacija kontrola za uspešno zadovoljenje propisanih zahteva ume da bude dosta kompleksan postupak. Većini inženjera fali potrebno znanje [90] i to može dovesti do kreiranja sistema koji su nebezbedni i podložni greškama [91]. Organizacije se obično u startu opredele za jedan primarni standard sa kojim se usaglašavaju. Činjenica je da različiti standardi izdati od strane različitih priznatih nacionalnih, regionalnih i internacionalnih tela imaju slične zahteve. To može stvoriti dilemu sa kojim standardom se uskladiti i razumeti koje su sličnosti i razlike između ponuđenih opcija. Jedan način na koji bi se ovo moglo rešiti jeste da se standardi međusobno uporede. Ova aktivnost podrazumeva uporednu analizu zahteva čijom implementacijom će se dobiti viši nivo zaštite u odnosu na propratne troškove i napor koji je potrebno uložiti za to [45]. Složenost ovog postupka raste sa povećanjem broja standarda jer proces poređenja svakog standarda sa svakim postaje neskalabilan. Organizacije koje posluju u više država vrlo često se susreću sa obavezama da budu usklađene sa više nacionalnih i regionalnih standarda u isto vreme. Takođe, priprema za implementaciju, interne revizije i sprovođenje analize rizika mogu biti veoma izazovne aktivnosti. Analiza rizika se ponekad radi nesinhronizovano sa bezbednosnim aktivnostima uglavnom zbog prirode organizacione strukture umesto da ove aktivnosti budu blisko povezane.

Ovo istraživanje inspirisano je izazovima koji su vezani za rad sa zahtevima različitih bezbednosnih standarda. Kao rešenje za problem uporedne analize zahteva iz više različitih standarda, definisan je proširivi model koji može da predstavi nove bezbednosne zahteve koji su primenjivi na kritične infrastrukture. Model bi se mogao koristiti u aplikacijama koje bi pomogle u rezonovanju o različitim standardima, kao i prioritizaciji i praćenju implementacije bezbednosnih kontrola u cilju zadovoljenja zahteva.

U nastavku je definisan problem koji ova disertacija obrađuje kroz sledeća dva istraživačka pitanja:

(1) Da li se može razviti proširiv model za reprezentaciju zahteva iz bezbednosnih standarda primenjivih na kritične infrastrukture?

(2) Kako se mogu dobiti informacije o zrelosti bezbednosne infrastrukture organizacije ili sistema u odnosu na zahteve definisane u proizvoljnim bezbednosnim standardima, a da se pri tom koristi domensko i organizaciono znanje za sprovođenje analize rizika, planiranje i praćenje unapređenja bezbednosti?

Na osnovu prethodno definisanih istraživačkih pitanja i motivacija, definisane su sledeće hipoteze:

(1) **Hipoteza:** *Moguće je definisati model za reprezentaciju zahteva iz različitih bezbednosnih standarda, stručnih smernica i regulativa za kritične infrastrukture. Model treba da omogući predstavljanje* *prikladnih informacija koje su zajedničke za zahteve iz različitih publikacija, i time se dozvoli njihova unakrsna komparacija.*

(2) Hipoteza: *Moguće je definisati kriterijume za prioritizaciju zahteva, da pored rizika, uključuju kompleksnost koju unose zavisnosti između različitih uloga učesnika iz organizacione strukture zaduženih za implementaciju zahteva, nivo važnosti zahteva za usklađenost i pripadnost zahteva određenom domenu.*

(3) Hipoteza: *Moguće je proširiti model da pruža jedinstveni domensko-orijentisani pogled koji dozvoljava istovremeno praćenje implementacije sličnih zahteva izabranih iz različitih bezbednosnih standarda, stručnih smernica i regulativa za kritične infrastrukture.*

Iz prethodno definisanih hipoteza izvode se primarni ciljevi ove disertacije pri čemu očekivani rezultati uključuju sledeće:

(1) *Definisanje modela koji uniformno predstavlja gradivne jedinice bezbednosnih zahteva koji su definisani u različitim publikacijama. Ovaj cilj odnosi se na prvo istraživačko pitanje, a obrađen je kroz Poglavlje 3.*

(2) *Proširenje modela komponentama za istovremeno praćenje i prioritizaciju implementacije sličnih zahteva izabranih iz različitih bezbednosnih standarda, stručnih smernica i regulativa za kritične infrastrukture. Ovaj cilj odnosi se na drugo istraživačko pitanje, a obrađen je kroz Poglavlje 3.*

(3) *Konstrukcija radnog okvira u skladu sa predloženim modelom, kao i validacija kojom bi se potvrdila praktična primenljivost navedenog modela i identifikovale sve njegove prednosti i eventualni nedostaci. Detalji ovog cilja obrađeni su kroz Poglavlje 4.*

Ovim istraživanjem predstavlja se jedno moguće rešenje za definisanje modela koji ima sve relevantne elemente za adekvatno predstavljanje bezbednosnih zahteva iz različitih tipova publikacija, kao i njihovo međusobno poređenje u cilju planiranja i praćenja implementacije. Definisani su kriterijumi za prioritizaciju odabira zahteva za implementaciju koji direktno zavise od četiri faktora: rezultata analize rizika, zavisnosti između učesnika zaduženih za implementaciju zahteva, nivoa važnosti zahteva za usklađenost i pripadnosti zahteva odgovarajućem domenu. Primenom ovakvog modela moguće je dovesti informacije iz različitih publikacija u standardizovani oblik koji će dalje olakšati rad i softversku automatizaciju. Radni okvir baziran je na prethodnom modelu i sadrži niz koraka koji vode korisnike kroz proces analize, planiranja i praćenja zadovoljenja bezbednosnih zahteva. Takođe, može poslužiti kao osnova za alat koji bi automatizovao aktivnosti koje se odnose na popunjavanje baze novim zahtevima, klasifikaciju zahteva u odgovarajuće domene, analizu zahteva i kvantifikaciju rezultata sprovedenih revizija.

Model i radni okvir mogu koristiti organizacije koje softver ili usluge nude u više geografskih regiona kako bi demonstrirale svoju bezbednosnu usklađenost sa više standarda, stručnih smernica ili regulativa čiji su zahtevi definisani na različitim nivoima detalja, kao i svi ostali koji žele da razumeju šta su i kako izgledaju standardizovani bezbednosni zahtevi. Takođe, pružena je mogućnost planiranja prioritizacije implementacije bezbednosnih zahteva odabranih standarda koja uključuje i sprovođenje analize rizika, te predloženo rešenje mogu koristiti i svi ostali pružaoci usluga koji žele da povećaju zrelost bezbednosti svoje organizacije ili sistema. Deo modela za opis bezbednosnih zahteva može biti pretočen i korišćen kao format za razmenu bezbednosnih zahteva između aplikacija kojima je primarna namena upravo rad sa bezbednosnim zahtevima u cilju kreiranja bezbednosnih planova za organizacije ili sisteme.

Disertacija je organizovana u pet poglavlja. U **Poglavlju 1** dat je detaljan opis motivacije iz prethodnog dela rezimea. Takođe su definisana istraživačka pitanja i hipoteze na koje se odgovara.

Poglavlje 2 daje pregled relevantne literature iz oblasti disertacije.

U cilju razmatranja prve hipoteze i prvog istraživačkog pitanja, istražuju se modeli za prezentaciju bezbednosnih zahteva, što je tema odeljka 2.1. Nhlabatsi i drugi [96] klasifikuju pristupe za modelovanje u četiri klase: pristupi zasnovani na ciljevima, zasnovani na modelima, problemski orijentisani i procesno orijentisani. Pristupi zasnovani na ciljevima detektuju i koriste ciljeve za određivanje bezbednosnih zahteva. Značajni predstavnici su Secure Tropos [97, 98] i antimodeli [100]. Secure Tropos proširuje metod agentski orijentisanog razvoja softvera Tropos [99] bezbednosnim konceptima poput bezbednosnih ograničenja, zavisnosti, ciljeva i bezbednih entiteta. Antimodeli konstruišu dva modela, željeni i antimodel pun ranjivosti koje su potrebne da bi se ostvarili anticiljevi. Na taj način, rezultati dva modela se akumuliraju kako bi se definisali novi bezbednosni zahtevi. Pristupi zasnovani na modelima zagovaraju da pravljenje modela pomaže u razumevanju problema koji se rešava. Predstavnici ovog pristupa su UML ekstenzije UMLSec [102] i SecureUML [103] obogaćene bezbednosnim simbolima. Problemski orijentisani pristupi nude alate za analizu problema koji nosi razvoj softvera. Lin i drugi [105] definišu zahteve malicioznih korisnika koje treba sprečiti na osnovu kojih se izvode bezbednosnih zahtevi koje treba zadovoljiti. Procesno orijentisani pristupi zagovaraju pristupe koji se zasnivaju na više koraka koje treba obaviti u analizi bezbednosnih zahteva. Jedan takav pristup je System Quality Requirements Engineering (SQUARE) koji u devet koraka nudi mehanizme za izbor, kategorizaciju i prioritizaciju bezbednosnih zahteva primenjivih na informacione sisteme i aplikacije [109]. Analizom različitih modela identifikovani su sledeći koncepti neophodni za očuvanje bezbednosti organizacija i sistema: bezbednosni zahtevi, imovina kojom se raspolaže, pretnje, bezbednosni ciljevi, bezbednosne kontrole, ranjivosti i rizici.

U literaturi se može naći nekoliko pokušaja da se na osnovu ovih koncepata napravi jedinstveni model primenjiv na bezbednosne standarde. Beckers i drugi [121] definišu konceptualni model koji sadrži koncepte izdvojene iz različitih standarda. Autori kreiraju obrazac čiji delovi odgovaraju konceptualnom modelu. Ovaj pristup omogućava korisnicima da na vrlo visokom nivou porede standarde kako bi se odlučili za jedan koji će dalje pratiti. Model je zasnovan na konceptima iz nekolicine standarda koji su po tipu i strukturi isti, te je količina informacija dobijena ovim putem nedovoljna da bi model zaživeo u široj upotrebi. NIST Cybersecurity Framework (CSF) definiše još jedan pogled kroz koji se mogu analizirati bezbednosni zahtevi [82]. U pitanju je troslojni radni okvir koji definiše aktivnosti potrebne za dostizanje bezbednosnih ciljeva, interpretaciju i upravljanje bezbednosnim rizicima i prilagođavanje svih aktivnosti organizacije koja ga praktikuje. CSF svojim konceptima idejno dosta utiče na rešenje koje je prezentovano u ovoj disertaciji. Radni okvir definiše domene u koje se svrstavaju bezbednosni zahtevi na osnovu funkcija koje imaju u procesu zaštite sistema i nudi primere za nekoliko poznatih standarda. Predloženi pogled kroz funkcije može biti prilično krut za pojedine zahteve i posledično onemogućava finiju granulaciju pri klasifikaciji zahteva. Daljim pregledom postojeće literature [125, 127, 128], može se zaključiti da postoji veliki broj standarda iz oblasti bezbednosti koji specificiraju zahteve na organizacionom ili sistemskom nivou i to na različitim nivoima detalja. Ovi radovi se ne bave direktno modelima za prezentaciju bezbednosnih zahteva ali daju smernice na koji način analizirati standarde.

Odeljak 2.2 opisuje analizu softverskih alata koji za cilj imaju samostalne procene otpornosti na napade i usklađenost sa standardima [129]. Analiza ovih alata je bitna zbog načina na koji se upotrebljavaju kao i elemenata koje poseduju, a koji su značajni za model koji se u disertaciji definiše. Od svih analiziranih alata, najkompletniji je Cyber Security Evaluation Tool (CSET) koji može poslužiti kao centralizovana baza bezbednosnih zahteva [130]. Pošto je alat namenjen za samostalnu procenu usklađenosti bezbednosti sa bezbednosnim zahtevima, definiše niz koraka koje treba odraditi pre evaluacije i dobijanja rezultata. Evaluacija bezbednosne postavke počinje biranjem nivoa bezbednosti koji se cilja kako bi se adekvatan upitnik prikazao korisniku. Takođe, alat dozvoljava korisniku da odabere standarde u odnosu na koje se vrši procena kao i mogućnost da se arhitektura evaluiranog sistema nacrta kako bi se stavio poseban akcenat na pojedine komponente. Od korisnika se zahteva da na svako pitanje da odgovor i priloži dokument koji ga potkrepljuje. Na kraju se prikazuje rezultat koji sadrži informacije o procentu usklađenosti sistema sa zahtevima kao i prioritet kojim treba adresirati zahteve koji nisu ispunjeni. Alat ima i određena ograničenja. Analiza je više okrenuta individualnim komponentama nego celokupnom sistemu koji se evaluira zbog čega grafički prikaz arhitekture ima vrlo malu vrednost. Iako je moguće označiti više standarda pri pokretanju upitnika, uporedna analiza dva ili više standarda nije moguća, već se odgovori na svaki zahtev moraju dati odvojeno iako su neki zahtevi isti ili dovoljno slični da je isti odgovor primenjiv. Takođe, nejasni su kriterijumi rangiranja neispunjenih zahteva što dodatno limitira korišćenje ovog alata. Slični alati poput Control System Cyber Security Self-Assessment Tool (CS2SAT) [133] i Cyber Resilience Review Self-Assessment Package (CRR) [134] imaju još jednostavniju izvedbu. Sa druge strane, ideja koju nudi Open Security Controls Assessment Language (OSCAL), iako u ranoj fazi razvoja, čini se obećavajućom [140]. OSCAL nudi šemu za razmenu informacija o bezbednosnim planovima i izveštajima izraženu u eXtensible Markup Language (XML), JavaScript Object Notation (JSON), i YAML Ain't Markup Language (YAML) formatima. Takođe je pogodna za razmenu bezbednosnih zahteva iz različitih standarda između aplikacija. Šema je prilično kompleksna i upotreba pojedinih elemenata koji bi trebali da obezbede proširivost bezbednosnih zahteva još uvek nije dokumentovana. U trenutnoj fazi razvoja, fokus šeme je stavljen samo na nekolicinu standarda koji su u upotrebi najviše u Sjedinjenim Američkim Državama.

U cilju razmatranja druge hipoteze i drugog istraživačkog pitanja, u narednim odeljcima istražuju se postojeći mehanizmi kao kandidati za proširenje našeg osnovnog modela. U odeljku 2.3 predstavljeni su najuticajniji modeli kojima se može opisati zrelost sistema. Gilsinn i Schierholz su uveli koncept vektora nivoa bezbednosti kako bi opisali faktore zaštite koji su potrebni da bi se sistem obezbedio [142]. Ovi nivoi predstavljaju kvalitativni pristup za definisanje zrelosti sistema. Postoji četiri tipa nivoa: ciljani, planirani, postignuti i nivo za koji sistem ima mehanizme da ga dostigne. Svakom tipu nivoa može biti pridružena jedna od četiri vrednosti koja opisuje koji nivo zaštite sistema organizacija može da očekuje:

- Nivo 1 — podrazumeva zaštitu od jednostavnog i slučajnog narušavanja bezbednosti izazvanih loše definisanim polisama i procedurama;
- Nivo 2 — podrazumeva zaštitu od namernog narušavanja bezbednosti pomoću jednostavnih napadačkih tehnika;
- Nivo 3 — podrazumeva zaštitu od namernog narušavanja bezbednosti pomoću sofisticiranih napadačkih tehnika za koje napadač mora imati određeno domensko znanje;
- Nivo 4 — podrazumeva zaštitu od namernog narušavanja bezbednosti pomoću širokog spektra sofisticiranih napadačkih tehnika za koje napadač mora imati određeno domensko znanje i značajne resurse.

Sa druge strane, Cybersecurity Capability Maturity Model (C2M2) je više okrenut organizacijama i njihovom bezbednosnim programima [143]. Pruža smernice za evaluaciju praksi, procesa i bezbednosnih kontrola koje organizacija koristi. Capability Maturity Model Integration (CMMI) je još opštiji jer se može primeniti na bilo koje procese, ne isključivo bezbednosne [141]. Oba modela definišu slične skale kojima se opisuje nivo zrelosti procesa počevši od nepostojanja istih, do adekvatno definisanih, redovno praktikovanih i unapređivanih. Rezultat procene na kojem se nivou zrelosti nalaze bezbednosne kontrole i procesi koji se koriste u organizaciji i primenjuju na sistemima izuzetno je važan pokazatelj u kojim segmentima organizacija treba da radi na podizanju nivoa bezbednosti koji bi bio u skladu sa postavljenim ciljevima poslovanja.

U odeljku 2.4 prezentovani su često korišćeni načini za analizu rizika kao jedne od glavnih aktivnosti koje treba sprovoditi u cilju poboljšanja bezbednosti. Detaljno su predstavljena dva standardizovana pristupa — NIST SP 800-30 Revision 1 [116] i ISO/IEC 27005:2011 [146]. NIST SP 800-30 pruža smernice za sprovođenje procene rizika federalnih sistema i organizacija organizovane u nekoliko koraka. Sadrži obiman skup ranjivosti i pretnji koje mogu da postoje u sistemu. Takođe, nudi način da se i kvantitativno izrazi rizik kao proizvod verovatnoće da će pretnja iskoristiti ranjivost sistema i uticaja koji će imati na poslovanje. Ovo je najčešći način za kvantifikaciju rizika i kod drugih metoda. ISO/IEC 27005:2011 daje smernice za proces upravljanja rizikom za organizacije koje implementiraju svoj Information Security Management System (ISMS) u skladu sa standardom ISO/IEC 27001. Takođe, nudi smernice za izražavanje rizika na kvantitativan i kvalitativan način. Poput NIST SP 800-30, ISO/IEC 27005:2011 sadrži obiman skup pretnji i ranjivosti koji se mogu koristiti kako baza znanja pri sprovođenju analize rizika.

Kako je tema disertacije i prioritizacija implementacije bezbednosnih zahteva, postojeće tehnike su takođe analizirane u odeljku 2.5. Postoje različite metode za prioritizaciju različitih zahteva [155], pri čemu se većina predloženih metoda može primeniti i na bezbednosne zahteve. Achimugu i drugi [156] navode da su mnoge od postojećih tehnika sklone greškama, teško se skaliraju i nedovoljno uključuju ljudski faktor pri definisanju prioriteta. U osnovi većine postojećih pristupa koriste se metode za donošenje odluka na osnovu skupa kriterijuma poput analitičkog hijerarhijskog procesa (engl. Analytical Hierarchy Process - AHP) [159], TOPSIS (engl. Technique for Order Preference by Similarity to the Ideal Solution) [160] i SAW (engl. Simple Additive Weighting) [161]. AHP pokušava da pojednostavi procenu u skladu sa svim definisanim kriterijumima tako što formira hijerarhije, međusobno poredi relevantne kriterijume u hijerarhiji i skuplja rezultate koje dodatno opisuje težinama. TOPSIS zahteva računanje najduže i najkraće udaljenosti od negativnog i pozitivnog idealnog rešenja, respektivno. Svakom kriterijumu pridružuje težinu i računa geometrijsko rastojanje između ponuđenih alternativa i alternative koja ima najbolji rezultat po svakom kriterijumu. SAW metoda definiše da se završni rezultat svake alternative između kojih se bira računa kao suma svih proizvoda kriterijuma kojima su dodate težine relativne u odnosu na svaki od kriterijuma. Sva tri pristupa koriste težinske faktore u odlučivanju te se oni moraju adekvatno rasporediti. Analiza literature koja pokriva pitanje prioritizacije zahteva pokazala je da se različiti faktori moraju uzeti u obzir. Ti faktori uključuju lakoću kojom se kriterijumi mogu koristiti, koji je nivo uključenosti korisnika koji učestvuju u samoj implementaciji, koliko precizni rezultati moraju biti i kako analiza rizika može da utiče na prioritet.

Poglavlje 3 čini glavni deo ove disertacije. U ovom poglavlju predstavljena je metodologija za kreiranje modela i komponente za njegovo proširenje. Opisana je metodologija za kreiranje i validaciju modela u tri koraka. U sklopu prvog koraka, napravljena je analiza dostupne literature koja stavlja akcenat na bezbednosne standarde, stručne smernice i regulative koji su primenjivi na kritične infrastrukture u cilju izbora adekvatnih predstavnika čija struktura će se dalje analizirati. Postupak i rezultati su opisani u odeljku 3.1. Sistematska analiza literature je potrebna za bolje upoznavanje sa najčešće korišćenim bezbednosnim publikacijama i njihovom mogućom primenom na sektore od interesa za ovu disertaciju. Zbog velikog broja publikacija koje danas postoje, treba prepoznati koje publikacije služe kao uzor za sve novonastale kako bi se izbegla analiza previše strukturno sličnih standarda koji će ograničiti upotrebu definisanog modela. Na primer, nemački IT-Grundschutz [172] je baziran na ISO/IEC 27001 [173], dok Cyber Assessment Framework (CAF) koji se koristi u Velikoj Britaniji [174] referencira ISO/IEC 27001, ISO/IEC 27002 [175] i IEC 62443 [176] u skoro svakom poglavlju. Detektovanjem onih publikacija koje se najčešće spominju u kontekstu kritičnih infrastruktura eliminisaće se izvedeni standardi čije se mapiranje na osnovne svodi na relativno trivijalni postupak. U literaturi se mogu naći različiti kvalitativni [177, 178, 179] i kvantitativni pristupi [128] za analizu standarda. Strategija predložena u disertaciji kombinuje oba pristupa, a započinje sa kvantitativnim. Ovaj pristup zahteva pretragu baza naučnih radova poput Google Scholar, Semantic Scholar, Institute of Electrical and Electronics Engineers (IEEE), Springer and Association for Computing Machinery (ACM). Pretraga po različitim kombinacijama ključnih reči generisala je veliki skup rezultata sa dosta šuma te je nad njime primenjen set kvalitativnih zahteva koji će izdvojiti samo bezbednosne publikacije koje imaju odgovarajuće karakteristike koje bi se mogle detaljnije analizirati. Skup kvalitativnih kriterijuma je definisan u prethodnom istraživanju [45].

U odeljku 3.1 predstavljeni su rezultati i ograničenja analize u sklopu prvog koraka. Finalni skup publikacija koje su korišćene za dalju analizu broji četiri publikacije:

- IEC 62443-3-3:2013
- ISO/IEC 27001 i 27002
- NIST SP 800-53
- NERC CIP

IEC 62443 je internacionalna serija standarda koja pokriva detalje od osnovnih koncepata do bezbednosti pojedinačnih komponenti. IEC 62443-3-3:2013 je najviše koriščeni standard iz ove serije. Odabran je kao predstavnik standarda koji pokriva značajne bezbednosne aspekte sistema, a ne organizacije.

ISO/IEC 27001:2013 je globalno priznati standard koji pruža radni okvir za sistematsko postizanje bezbednosti kroz implementaciju ISMS. Zajedno sa ISO/IEC 27002:2013 odabran je kao predstavnik globalno priznatih standarda koji je primenjiv i na različite sektore i organizacije van kritičnih infrastruktura.

NIST SP 800-53 je stručna smernica koja je tehnološki neutralna te se

može primeniti u različitim sektorima. Federalna tela i tela povezana sa njima u Sjedinjenim Američkim Državama zahtevaju usklađenost sa smernicama koje ova publikacija propisuje. Ova publikacija u finalnom skupu za analizu predstavlja klasu stručnih smernica.
NERC CIP je regulativa koja se primenjuje u Sjedinjenim Američkim Državama na sistemima za upravljanje električnom mrežom i transportom električne energije. Zahtevi koje propisuje NERC CIP sve više se primenjuju i u drugim delovima sveta. NERC CIP se sastoji od skupa publikacija koje sadrže bezbednosne zahteve koji pokrivaju aspekte od identifikacije resursa koje treba koristiti, preko upravljanja bezbednošću sistema do mehanizama fizičke zaštite. Ova publikacija izabrana je kao predstavnik regulativa sa najviše pojavljivanja u dobijenim rezultatima. U odeljku 3.1 opisana su i obrazloženja za isključivanje pojedinih publikacija iz dalje analize.

Preostali odeljci trećeg poglavlja opisuju aktivnosti sprovedene u drugom koraku. U ovom koraku, u odeljku 3.2, analizirane su strukture četiri izabrane publikacije. Tokom analize, utvrđeno je da istovremeno poređenje zahteva više od dve publikacije može da dovede do grešaka. Iz tog razloga predložen je novi pogled na publikacije koje se analiziraju. Ovaj pogled podrazumeva da se zahtevi klasifikuju u domene i tako dalje posmatraju. Različiti autori [130, 192, 195, 196, 197] definišu 26, 18, 18, 17 i 10 domena, respektivno. IEC 62443 3-3, ISO/IEC 27001, NIST800-53 i NERC CIP definišu svojih 7, 14, 20, 12 domena, respektivno. Na osnovu analize postojećih domena i zahteva iz četiri posmatrane publikacije, definisan je skup od 24 domena koji pravi finiju granulaciju zahteva u odnosu na postojeća rešenja. Pripadnost zahteva domenima prepoznat je kao jedan od kriterijuma za prioritizaciju implementacije zahteva. U nastavku odeljka 3.2 opisana je kvantifikacija domena u te svrhe. Odeljak 3.3 daje opis o jednom od proširenja osnovnog modela i drugom kriterijumu prioritizacije — nivoima važnosti zahteva za usklađenošću sa standardima. Ponuđeni model za nivoe važnosti je dvodimenzionalan. Prva dimenzija tiče se važnosti zahteva za postizanje određenog nivoa bezbednosti, dok se druga bavi zrelošću same implementacije. Definisana skala za prvu dimenziju je kvantitativna:

- zahtev je obavezan i mora biti zadovoljen — nivo 3;
- zahtev ima visok prioritet i treba biti zadovoljen ukoliko postoje uslovi za to — nivo 2;
- zahtev je poželjan, ali niskog prioriteta — nivo 1;
- zahtev nije neophodno adresirati — nivo 0.

Dodeljeni nivoi biće upotrebljeni za kvantifikaciju prioriteta implementacije zahteva. Definisana skala za drugi dimenziju je kvalitativna:

- Nije primenjivo — bezbednosne kontrole nije potrebno implementirati jer bezbednosnih zahtevi nisu primenjivi na sistem ili organizaciju koja se razmatra;
- Bez implementacije – bezbednosne kontrole nisu implementirane;
- Inicijalno stanje — bezbednosne kontrole su implementirane stohastički sa niskim nivoom zrelosti i mogućnosti praćenja napretka;
- Upravljano — bezbednosne kontrole su implementirane i dokumentovane da budu u skladu sa zahtevima, ali ne postoji jasan plan za buduća poboljšanja u slučaju organizacione promene ili promene sistema; napredni zahtevi nisu implementirani;
- Definisano — bezbednosne kontrole su unapređenje u odnosu na prethodno stanje i napredni zahtevi su implementirani ako postoje; procesne i tehnološke invarijante su definisane gde je to moguće;
- Upravljano kvantitativno — bezbednosne kontrole se kvantitativno analiziraju u cilju identifikacije odstupanja i implementacije narednih unapređenja;

- Optimizivano — bezbednosne kontrole se kontinualno poboljšavaju korišćenjem inovativnih tehnologija i učenjem na osnovu prethodnih iskustava.

Odeljak 3.3 uvodi i koncept ključnih pokazatelja učinka (engl. Key Performance Indicator) kao predlog za opis i praćenje performansi u procesu implementacije i zadovoljenja prezentovanih nivoa.

Odeljak 3.4 opisuje treći kriterijum prioritizacije, element koji unose zavisnosti između različitih uloga učesnika iz organizacione strukture zaduženih za implementaciju zahteva. Organizaciona struktura može biti različita, ali to ne menja činjenicu da su ljudi ti koji implementiraju bezbednosne kontrole da bi zadovoljili zahteve. Zavisnosti koje oni mogu da naprave međusobno mogu biti prilično kompleksne. Ideja za modelovanje socijalnih učesnika u procesu implementacije preuzeta je iz i* (iZvezda) radnog okvira [208]. i* omogućava pravljenje modela koji reprezentuje jednu organizaciju. Identifikuje sve ključne ljude u organizaciji koji su bitni za potrebe dostizanja definisanog cilja i modeluje ih kao učesnike koji zavise jedni od drugih. Koncepti definisani u i* radnom okviru prilagođeni su potrebama ove disertacije tako da se definiše graf zavisnosti učesnika (engl. Actor Dependency Graph). Na ovaj način mogu se pratiti sve zavisnosti između učesnika u procesu implementacije zahteva i detektovati kompleksni grafovi koji predstavljaju signal za podizanje prioriteta implementacije.

U odeljku 3.5 opisan je poslednji kriterijum prioritizacije, rezultat analize rizika. Takođe je opisan kriterijum za izbor metode za računanje prioriteta zahteva. Odabrana je SAW metoda i demonstriran je postupak određivanja redosleda implementacije zahteva iz hipotetičkog skupa od četiri zahteva. Na kraju poglavlja, model sa svim relevantnim elementima predstavljen je korišćenjem UML (engl. Unified Modeling Language) notacije radi lakše čitljivosti.

U sklopu poslednjeg koraka, u **Poglavlju 4** predstavljen je radni okvir kao mehanizam za potvrdu upotrebljivosti predloženog modela. Kroz odeljak 4.1 opisani su koraci za uključivanje zahteva iz novih standarda i inicijalnu postavku svih relevantnih informacija koje će obezbediti praćenje usklađenosti među standardima i prioritizaciju implementacije bezbednosnih zahteva. U odeljku 4.2 predstavljena je studija slučaja koja pokriva primer organizacije koja razvija industrijski sistem za upravljanje pametnim mrežama. Predstavljena je analiza standarda za pametne mreže NISTIR 7628 koji nije bio deo analize kako bi se potvrdila praktična primenljivost modela i identifikovale njegove prednosti i nedostaci. Na jednom scenariju propisanom NISTIR 7628 standardom, demonstrirana je prioritizacija implementacije bezbednosnih zahteva koja prati sve aktivnosti predstavljenog radnog okvira. U poslednjem odeljku 4.3 otvorena je diskusija o predstavljenim rezultatima ove disertacije.

Poglavlje 5 predstavlja poslednje poglavlje ove disertacije. U ovom poglavlju navedeni su doprinosi ove disertacije. Ključni doprinosi mogu se sumirati na sledeći način:

- Definisan je model za reprezentaciju bezbednosnih zahteva koji se može koristiti za praćenje implementacije i procene usklađenosti sa više standarda, stručnih smernica i regulativa u isto vreme na uniforman način.

- Definisan je kriterijum prioritizacije za potrebe implementacije bezbednosnih zahteva sa kojima organizacija ili sistem nisu usaglašeni. Kriterijum prioritizacije počiva na četiri faktora: rezultatima analize rizika, zavisnostima između učesnika zaduženih za implementaciju zahteva, nivoima važnosti zahteva za usklađenost i pripadnosti zahteva odgovarajućem domenu.

- Definisan je radni okvir i opisane su smernice za njegovo korišćenje za potrebe demonstracije primene modela.

Na samom kraju poglavlja, dat je pregled pravaca daljeg istraživanja. Jedan od pravaca daljeg istraživanja uključuje proširivanje baze znanja i modela elementima koje diktiraju novi standardi koji stavljaju akcenat na koncepte i tehnologije poput računarstva u oblaku, računarstva na ivici i internet stvari. Ovo potencijalno može uticati na ograničenje

koje nameće radni okvir, a koje zahteva da se u slučaju definisanja novih domena klasifikacija postojećih zahteva mora raditi ispočetka. Buduće istraživanje treba da reši trenutno ograničenje uvođenjem dinamičke reklasifikacije zahteva bez posredovanja eksperata za bezbednost. Takođe, predložena je provera primenjivosti modela na standarde koji se bave privatnošću podataka. Za kraj, predloženo je da se svi rezultati daljih istraživanja integrišu u alat otvorenog koda koji bi služio u svrhe formalnih revizija bezbednosti organizacija i njihovih sistema.
Ključne reči: zaštita kritičnih infrastruktura, standardi, usklađenost sa standardima, bezbednosni zahtevi, prioritizacija zahteva.

Table of Contents

Abstract i

Rezime iii

List of Figures xxvii

List of Tables xxix

List of Equations xxxi

List of Abbreviations xxxiii

1 Introduction 1
- 1.1 Problem area 3
  - 1.1.1 Critical Infrastructure 3
  - 1.1.2 Critical Infrastructure Protection 7
- 1.2 Motivation and Problem Statement 20
- 1.3 Research Hypotheses and Goals 23
- 1.4 Thesis Structure 24

2 Research review 27
- 2.1 Models for Requirement Representation 27
- 2.2 Self-assessment Tools for Cybersecurity Resilience and Standard Compliance 34
- 2.3 Maturity Models 38

2.4 Risk Assessment Methods 42
2.5 Techniques for Requirement Prioritization 47
2.6 Thesis Position 49

3 Model for Requirement Representation 51
3.1 Publication Selection 52
3.1.1 Selected Standards 56
3.1.1.1 IEC 62443-3-3:2013 (ISA 99) 56
3.1.1.2 ISO/IEC 27001 and 27002 58
3.1.1.3 NIST SP 800-53 60
3.1.1.4 NERC CIP 61
3.1.1.5 Excluded Publications 62
3.2 Security Controls Classification 64
3.3 Assurance Model 78
3.4 Actors 81
3.5 Prioritization Criteria 85
3.6 Model 94

4 Model Validation 103
4.1 Security Assessment Framework for Critical Infrastructure 103
4.1.1 The Seeding Phase 106
4.1.2 The Assessment Phase 109
4.1.3 The Implementation Tracking Phase 112
4.2 Case Study – Smart Grid Industrial Control System . . 115
4.3 Discussion 127

5 Conclusion 133
5.1 Contributions of the Thesis 135
5.2 Future Work 137

Bibliography 139

List of Figures

1.1 SCADA network architecture 5
1.2 The Purdue Model for ICS 10

3.1 Three-stage research methodology 52
3.2 UML class diagram of the core model elements 94
3.3 UML class diagram of the proposed model 97

4.1 Process for import of new requirements 108
4.2 Results of the compliance assessment phase 111
4.3 Initial setup for requirement implementation tracking . 114
4.4 NISTIR 7628 summary numbers per domain 121
4.5 SG.IA-5 Device Identification and Authentication Enhancement 1 as a model instance 122
4.6 SG.IA-5 Enhancement 1 – complete initial setup 125
4.7 Requirement Model to OSCAL Catalog Model mapping 130

List of Tables

2.1 NIST SP 800-30 Level of Risk Assessment Scale 45

3.1 Publication occurrences in the study 55
3.2 List of domains by different authors 68
3.3 List of domains in selected publications 71
3.4 List of defined domains with scores 74
3.5 Mapping of the i* elements to our model 84
3.6 Risk Level Criterion 89
3.7 Essence Level Criterion 90
3.8 Actor Dependency Graph Criterion 90
3.9 Domain Affiliation Criterion 90
3.10 Suitability Rating Matrix 91
3.11 Final requirements priorities 93
3.12 Explanation of connections 100

4.1 Framework activities 105
4.2 NISTIR 7628 requirements mapping to domains 119
4.3 Compliance Assessment Results 123
4.4 Suitability Rating Matrix for Vendor A assessment . . 126
4.5 Final requirement priorities for Vendor A 126

List of Equations

2.1 Risk Assessment Formula 44
2.2 Likelihood Formula 44
3.1 Normalized Performance Rating of Alternatives 88
3.2 Preference Value of Alternatives 88

List of Abbreviations

ACM	Association for Computing Machinery
ADG	Actor Dependecy Graph
AHP	Analytical Hierarchy Process
AI	Artificial Intelligence
BES	Bulk Electric Systems
CAF	Cyber Assessment Framework
CCSMM	Community Cyber Security Maturity Model
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentiality, Integrity and Availability
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CMMI	Capability Maturity Model Integration
CRR	Cyber Resilience Review

CS2ST	Control System Cyber Security Self-Assessment Tool
CSET	Cyber Security Evaluation Tool
CSF	Cybersecurity Framework
DA	Domain Affiliation
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DoDI	Department of Defense Instruction
E-ISAC	Electricity Information Sharing and Analysis Center
EE-ISAC	European Energy Information Sharing and Analysis Centre
EL	Essence Level
ENISA	The European Union Agency for Cybersecurity
EPCIP	European Programme for Critical Infrastructure Protection
ERP	Enterprise Resource Planning
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IACS	Industrial Automation and Control Systems

ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
INL	Idaho National Laboratory
IoT	Internet of Things
ISA99	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
JE-ISAC	Japan Electricity Information Sharing and Analysis Center
KPI	Key Performance Indicator
MIL	Maturity Indicator Level
MIS	Management Information Systems
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
ONG-ISAC	Oil and Natural Gas Information Sharing and Analysis Center

OT	Operations Technology
PCI DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PLC	Programmable Logic Controllers
PPT	People, Process, Technology
PRISMA	Preferred Reporting Items for Systematic Review and Meta-Analyses
RL	Risk Level
RTU	Remote Terminal Unit
SAL	Security Assurance Levels
SAW	Simple Additive Weighting
SCADA	Supervisory Control And Data Acquisition
SDL	Security Development Lifecycle
SETA	Security Education, Training and Awareness
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprises
SP	Special Publication
SQUARE	System Quality Requirements Engineering
TCSEC	Trusted Computer System Evaluation Criteria
TOPSIS	Technique for Order Preference by Similarity to the Ideal Solution

TTP	Tactics, Techniques, and Procedures

Chapter 1

Introduction

When we step aside and reflect on what technology has done to improve the quality of life in the past couple of decades, we should not argue that it was a lot. We must not believe that the era of the Digital Age is at its peak, but quite a few ideas have been lucky to see the daylight and change modern life, from the World Wide Web to digital transformation through Industry 4.0 to digital currencies such as Bitcoin [1] and Ethereum [2]. The World Wide Web made a considerable leap and connected the world in a way that was not possible before. It made it much easier for people to exchange information. Industry 4.0 revolutionizes the way that companies manufacture and improve their products by integrating new technologies such as the Internet of Things (IoT), cyber-physical systems, augmented and virtual reality, cloud computing, big data analytics, machine learning, and Artificial Intelligence (AI) [3, 4]. Cryptocurrencies and digital solutions based on blockchains introduced decentralization to transactions to omit intermediary fees and preserve security aspects. These blockchain ideas led to a new iteration of the World Wide Web called Web 3.0 [5]. With every breakthrough, good or bad, there is a possibility that worse things can emerge from that. Even though the primary goal for resources such as electric power, oil, gas, or water is to use them for everyone's well-being, they represent the opportunity for the bad actors to use them in digital warfare to harm individuals and the whole businesses and nations. This is why the security posture of each system needs to be assessed using multiple proven approaches.

The systems where security must be a top priority are Critical Infrastructure (CI) systems. Systems such as power grids, transport networks, and information and communication systems are essential for maintaining vital societal functions, and their malfunction may negatively impact one country's security and, ultimately, citizens. This thesis describes research that aims to mitigate some of the current problems in Critical Infrastructure. Uplifting the security posture of CI organizations and systems can be accomplished by combining different approaches. We focus on security requirements defined in recognized standards, guidelines, and regulations since they can help CIs establish security practices systematically. This thesis will refer to standards, guidelines, and regulations as security publications. The requirements analysis will help us define a model for security cross-standard compliance tracking and requirement prioritization for their implementation. To achieve this, we need to analyze different factors that form strong dependencies around the requirements to make a natural coherence. Section 1.1 provides the necessary background to understand specific problems, implications, and the concepts relevant to our research. Section 1.1.1 gives a brief overview of Critical Infrastructure as the problem area in which the results should be applied. Section 1.1.2 focuses on Critical Infrastructure Protection (CIP) as a concept that accumulates the means to protect vital CIs. From this discussion, we express motivation for solving identified problems in Section 1.2. Section 1.3 specifies the exact problems our work addresses and describes our hypothesis and research goals. In Section 1.4, we finish with the structure of the thesis.

1.1 Problem area

1.1.1 Critical Infrastructure

In the Report of the USA President's Commission on Critical Infrastructure Protection from 1997, the term infrastructure is interpreted as *a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services* [6]. The USA Patriot Act of 2001 defines critical infrastructure as *systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters* [7]. The USA Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience even defines sixteen critical infrastructure sectors [8]:

- chemical,
- commercial facilities,
- communications,
- critical manufacturing,
- dams,
- defense industrial base,
- emergency services,
- energy,
- financial services,
- food and agriculture,

- government facilities,
- healthcare and public health,
- information technology,
- nuclear reactors, materials, and waste,
- transportation system,s and
- water and wastewater systems.

European Commission defines CI similarly as *an asset or system that is essential for maintaining vital societal functions. The damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact on the security of the European Union and the well-being of its citizens* [9]. We can say that these definitions are pretty elaborative, and their interpretation can be considered similar wherever in the world.

All these critical infrastructure sectors modernized in terms of new equipment they use, such as programmable logic controllers (PLC), supervisory control and data acquisition (SCADA), and distributed control systems (DCS) for monitoring, control, and operation of physical devices such as sensors, valves, meters, and pumps. The industrial control systems (ICS) or industrial automation and control systems (IACS) — frequently substituted for operations technology or OT — is a generic term used to describe various control systems. ICS is used for controlling and monitoring the industrial processes used in energy, utilities, manufacturing, and other industrial sectors, many of which are critical. We can comprehend them as auto-integrator of life support systems, bringing hardware, software, and networks together to operate our critical infrastructure. A typical SCADA system comprising a control network and the corporate network is presented in Figure 1.1.

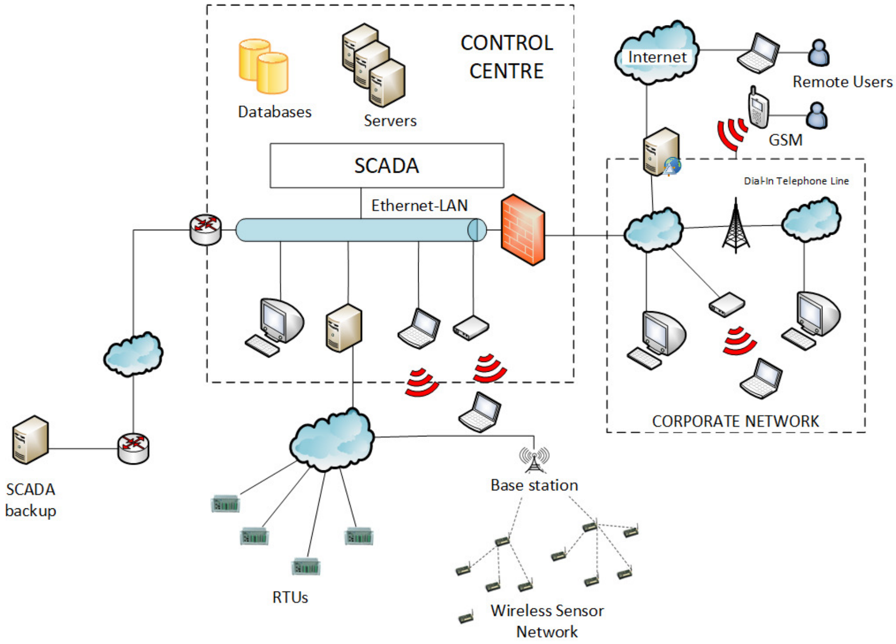


Figure 1.1: SCADA network architecture

The control network receives measurements or alarms from substations and does the control tasks such as opening or closing the pump. The corporate network is in charge of performing operations related to the system's general supervision. Both networks can use different protocols.

CI systems are often integrated with business systems such as enterprise resource planning (ERP), management information systems (MIS), billing systems, and other systems that require everyday hardware and software to extend their operations and optimize costs. These integration points open more attack vectors making CI systems more challenging to secure. From the architectural point of view, critical infrastructure systems can be analyzed in two ways — in isolation and as an integral part of one enormous ecosystem. By analyzing each system in isolation, we can observe each critical infrastructure as a unique field of research with its own set of problems. Here, we can establish a satisfactory security level, but this isolated approach would ignore the natural dependencies and interdependencies that naturally exist between these different systems. Rinaldi et al. in [10] define four types of interdependencies that can be found between infrastructures that, if compromised, could result in a domino effect disrupting the regular work of the system:

- Physical interdependency — if the state of one infrastructure is dependent on the outputs of the other;
- Cyber interdependency — if the states of the infrastructure depend on information transmitted through the information infrastructure;
- Geographic interdependency — if a local environmental event can create state changes in all infrastructures;
- Logical interdependency — if the state of one infrastructure depends on the other via a mechanism that is not considered a physical, cyber, or geographic connection.

For example, most studies involve linkages between water, energy, and food sectors [11, 12, 13, 14, 15, 16, 17]. The energy sector often only refers to hydropower generation [12], without considering other electricity generation such as solar power and wind power, raw resources production such as oil, natural gas, and coal, and comprehensive energy uses such as transportation, agriculture, and commercial energy consumption. Virtually all industries rely on electric power, meaning that all sectors eventually have some dependence on the energy sector. Lauge et al. [18] analyze how the failure of one critical infrastructure to deliver products and services in different periods impacts other critical infrastructures. The survey that was done among CI experts showed that the health sector is the most dependent CI for long-term failure. In contrast, the water and financial sectors are the least dependent CIs for failure periods of less than two hours and more than one week. Nonetheless, having these dependencies or not, operations in these sectors would be much more difficult without using the software solutions [19, 20].

With this information, we can conclude that collaboration between the systems is inevitable, and IT (and OT) networks are unfortunately converging and resulting in the evolution of a new threat landscape.

1.1.2 Critical Infrastructure Protection

In the past, CI systems were built with a primary focus on safety, reliability, and availability. Physical security controls like gates and locks were used as primary protection mechanisms. As a result, the community developed false beliefs about their cybersecurity (such as the air gap, proprietary protocols, and security through obscurity), which were sufficient to justify zero-intervention policies. Support for these beliefs was further strengthened because there was no evidence of any reported cyberattack, especially against ICS, until around 2010. With increasing digitalization — such as Industry 4.0 and Smart Grid networks — the use of these beliefs has eroded or disappeared altogether. Still, there is common agreement among the experts that these systems need to better address security [21, 22].

We witnessed famous attacks in the past, as mentioned by Miller et al. [23], but there is still a modest amount of publicly available information about them. Stuxnet was one of the most famous and most complex attacks on ICS when it was discovered in 2010 [24]. The goal was to damage Iranian nuclear systems. The targets were Windows machines connected to PLCs, and over 14,000 machines were infected by several exploiting vulnerabilities and advancing through the network. In Ukraine, electric distribution companies' networks were compromised with BlackEnergy malware that triggered a series of steps that resulted in power outages for over 80,000 people for 1 to 6 hours [25]. Iranian hackers attacked Rye Brook Dam in the United States during the maintenance period allowing technicians only to monitor and not control the SCADA system [26]. Wolf Creek nuclear facility in the

United States was attacked using spearphishing [27]. Triton is malware that targeted safety instrumented systems in the Middle East's oil and gas petrochemical facilities [28]. Safety instrumented systems are designed to prevent equipment failures and incidents such as fire and explosions. Ransomware attacks affected one of the world's largest meat producers, Brazilian JBS Foods, and the United States Colonial Pipeline, which eventually paid a significant amount of money [29, 30]. To analyze the consequences of CI disruptions and failures, Luiijf and Klaver [31] use the internal Critical Infrastructure Incidents Database tool with 13498 records for 10390 CI incident cases that occurred in 15 years, where the primary methods that are used for data collection are daily public news from media across the world and official reports. If we look at all these attacks, the energy sector can be recognized as one of the main targets of cyber-attacks against critical infrastructure. A joint report called Business Blackout issued by Lloyd's and the University of Cambridge's Centre for Risk Studies defines a hypothetical scenario of an electricity blackout in the United States that could cause a total impact on the United States economy at $243bn, or even more than $1trn in the most extreme scenarios [32]. These are only a few examples of attacks on CIs, but unquestionably there were more.

This led to ongoing efforts worldwide to increase protective measures referred to as Critical Information Protection. CIP implies *all activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructures to deter, mitigate and neutralize a threat, risk, or vulnerability* [33]. There is no clear consensus yet if CIP is different from the general computer, network, and information security when we know that many CI system components are not very different from, e.g., home workstations and network equipment [34]. However, CIP gains attention from academia and industry and evolves as time passes. Also, it has become a primary goal for many countries [35]. Dunn Cavelty and Suter [36] distinguish between three levels of protection goals for CIP and where they can be found:

- Goal described on a strategic level in national security strategy documents (e.g., National Strategy for Homeland Security in the United States [37], National Security Strategy in the Netherlands [38]);

- Goals described in dedicated CIP documents (e.g., National Infrastructure Protection Plan in the United States [39], National Strategy and Action Plan for Critical Infrastructure in Canada [40]);

- Goals described in sector-specific documents (e.g., Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan for Energy in the United States [41]).

These examples only prove that CIP is being taken more seriously than ever before.

Threat actors can use a variety of tactics, techniques, and procedures (TTP) to compromise systems on each level of the Purdue Model regardless of the type of the system architecture. The Purdue Model is the industry-adopted reference model that shows the interconnections and interdependencies of a typical ICS's components [42]. In Figure 1.2, this model divides the system architecture into six layers starting at layers 5 and 4, which is the Internet Demilitarized Zone (DMZ), flowing down through the enterprise DMZ to level 3, the control and operation layer, where the communication with local points connect with human-machine interfaces at level 2 and then ultimately the interaction with level 1 controllers such as PLCs and Remote Terminal Units (RTUs) that monitor and control level 0 field devices.

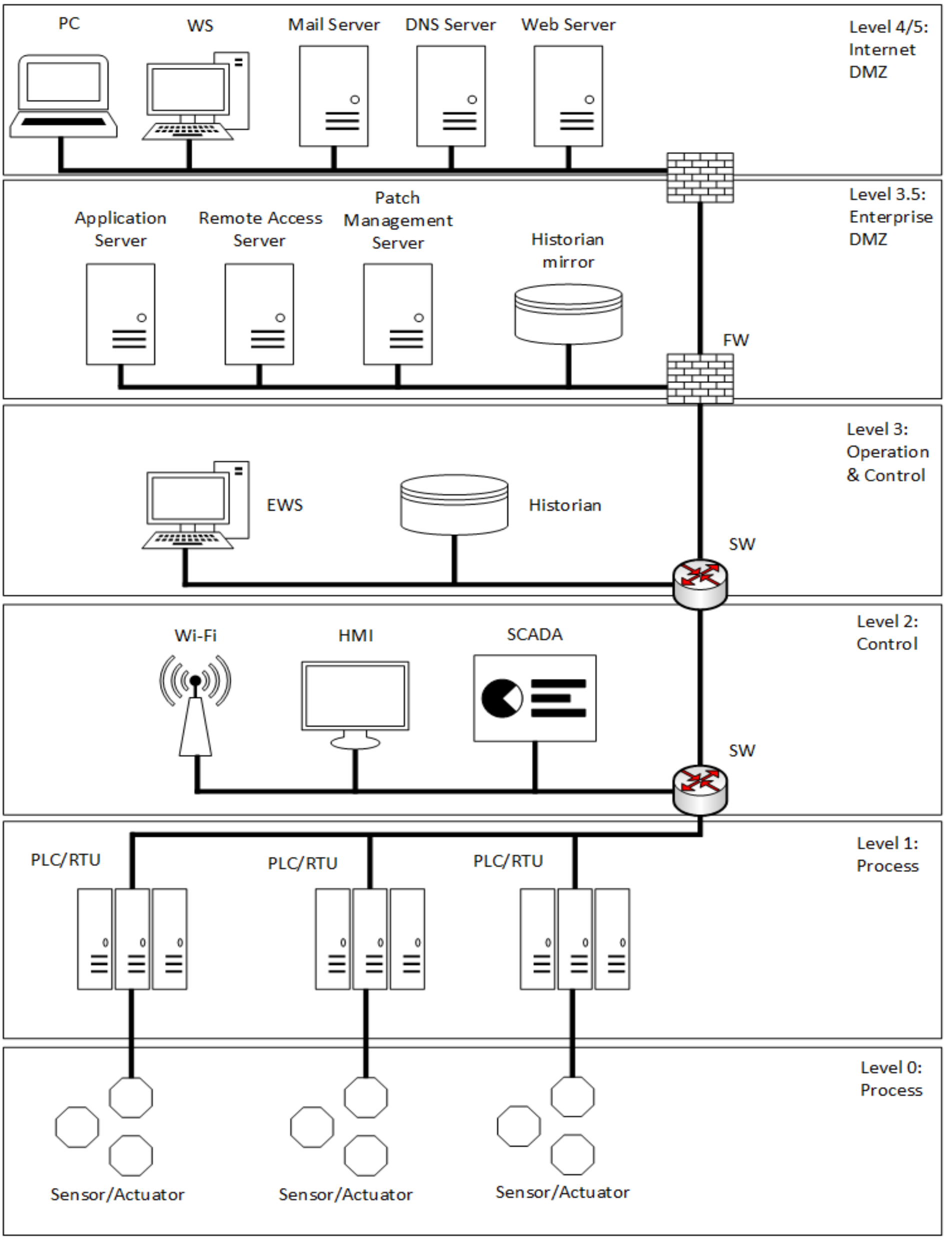


Figure 1.2: The Purdue Model for ICS

Authors in [43] state that common attack vectors can vary from Man-in-the-middle attacks to backdoors and holes in network perimeter, and field devices, to vulnerabilities in common protocols, database attacks, and communication hijacking. A flood of new technologies — especially cloud services and 5G wireless networks — are challenging the foundational, hierarchical approach to designing and operating systems. Traditional systems are being enhanced with new IT solutions that introduce new concepts — the edge and the cloud computing. Edge computing includes traditional OT equipment and an Industrial Internet of Things (IIoT) gateway that performs various operations such as data filtering, aggregation, storage, analytics, and device management. The cloud aggregates data and provides the means for analytics, event processing, process orchestration, and network communications. These new concepts ignore hierarchical levels defined in the Purdue Model and allow direct communication from physical devices to cloud services or through IIoT gateways.

Different attack vectors require that the systems have adequate security controls to mitigate the potential damage that can be made going through the defined level or even cross-levels. This can be done by defining and maintaining the defense in depth [44]. These mechanisms must be set in place to cover all three pillars of organizational transformation-people, process, and technology (to complete the PPT framework). These three pillars have to be regulated through governance, security management, and security controls to achieve the desired level of security. This can be done by employing several techniques mentioned in no particular order of relevance (Stojkov et al. [45]):

- expanding knowledge base through information sharing;
- performing regular vulnerability assessment and hardening security controls;
- practicing different kinds of tabletop exercises;

- conducting regular auditing;
- implementing requirements from relevant standards.

Given the risks these ever-emerging threats present, organizations must share threat information and use it to improve their security posture. This is one of the approaches to building collective knowledge about new trends, increasing experience, and using that information to enrich the defense-in-depth strategy currently set in place. As the National Institute of Standards and Technology (NIST) defines in Special Publication (SP) 800-150 [46], cyber threat information is *any information that can help an organization identify, assess, monitor, and respond to cyber threats. Examples of cyber threat information include indicators (system artifacts or observables associated with an attack), TTPs, security alerts, threat intelligence reports, and recommended security tool configurations.* Gal-Or and Ghose in [47] find that an increase in security information sharing and security technology investment levels leads to higher social welfare than the no-sharing regime. This was recognized at a national level, and today we have communities of different organizations established to improve the resilience and security in the energy and oil and gas sectors by sharing verified information. The examples include national Computer Emergency Response Teams (CERTs), or more specific, the Electricity Information Sharing and Analysis Center (E-ISAC) in the United States, European Energy Information Sharing and Analysis Centre (EE-ISAC), Japan Electricity Information Sharing and Analysis Center (JE-ISAC), Critical Infrastructure Gateway in Canada, or the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). A community consists of more than just local government entities. Randall and Allen [48] find that formal and informal information-sharing networks exist at the meso and macro levels to mitigate uncertainties in the energy sector. Actors involved in information sharing are various: government bodies, private critical infrastructure, business enterprises, IT companies, IT security firms, and security researchers. For example, the Community Cyber Security Maturity Model (CCSMM) was developed by the Center for Infrastructure Assurance and Security at The University of Texas at San Antonio, United States [49], to help communities establish viable and sustainable cyber security programs. An important part of the CCSMM is information sharing, upon which a collaborative framework by Zhao and White is built [50]. Another example would be Microsoft's framework for cybersecurity information sharing and risk reduction [51]. This is a practical way to establish and strengthen that connection between different CI entities. The potential costs of sharing security information can have a negative effect as well, accruing from the resultant loss of market share and stock market value from negative publicity as presented by Campbell et al. in [52] and Cavusoglu et al. in [53].

Holmgren and Molin define vulnerability as *the collection of properties of an infrastructure system that might weaken or limit its ability to maintain its intended function, or provide its intended services when exposed to threats and hazards that originate both within and outside of the boundaries of the system* [54]. Vulnerability assessment is a practice that has to be performed regularly to track an organization's security status continuously. The United States Department of Homeland Security issued national strategy documents that recognize vulnerability assessment as one of the key activities for critical infrastructure protection [55, 56]. These activities are mandatory to demonstrate the maturity of the system's security posture as suggested by the North American Electric Reliability Corporation (NERC) for Critical Infrastructure Protection (CIP) set of requirements [57]. It is suggested not to perform them in a production environment in a manner that can have an adverse impact since they are considered invasive [58]. Benefits of performing regular vulnerability assessments are various: identification of known security exposures before attackers, creation of an inventory of all the devices on the network and their purpose, the definition of the risk level that exists on the network, the establishment of a business risk/benefit curve and optimization of security investments, saving time and costs, complying with industry and regulatory requirements. Given the significance of these activities, different frameworks and methodologies were developed to help in conducting the assessment, notably the works of Holmgren [59], Baker [60], Ten et al. [61], and Ferreira [62]. Allodi and Massacci in [63] leverage data from vulnerability assessments to quantify the likelihood of attacks. By continually practicing these acts correctly, the attack surface should reduce, and the overall maturity of the system and the organization will increase.

The least formal technique for security posture uplift would be passive and active training that simulates cyber and physical attacks through tabletop exercises. In their work, Franchina et al. [64] describe that an effective strategy to protect CI against malicious activities is through the implementation of effective Security Education, Training, and Awareness (SETA) programs. The authors present different active and passive techniques for addressing security challenges, from formal training sessions through seminars and roleplays, to computer-based and web-based training, to red teaming. They insist that hybrid techniques such as tabletop exercises can offer better value since they mix active and passive aspects of the training. Brilingaite et al. [65] follow the European Union Agency for Cybersecurity (ENISA) practice guides on national exercises [66] to make tabletop exercises in a web environment where the topic involves a cyber incident inside a water supply infrastructure. Even though the results were promising for education purposes, the authors state that tabletop exercise in a web environment lacks a social aspect that further limits collaborative activities to provide better solutions. Luiijf and Stolk [67] note that CIP requires good situational awareness to avoid making blind decisions, rapidly assess an incident to see if it was a deliberate attack and start preparations for the worst-case scenarios in time. GridEx [68], organized by NERC, and Cyber Storm [69], organized by Cybersecurity and Infrastructure Security Agency (CISA), are examples of events that are interested to the energy sector. Malicious activities are not the only example where tabletop exercises can be organized. Lo et al. [70] give an example of a tabletop exercise that simulates COVID-19 lockdown in a pandemic and state that after the acquisition of essential resources such as food and daily necessities, the continuation of essential businesses and critical infrastructures is the essential measure that needs to be applied.

Cybersecurity audits can help with assessing compliance against different standards or regulations. They represent a systematic approach — preferably done by the independent party — to examine the security posture of the organization or system. These activities include different checks to validate if proper security mechanisms are in place and ensure that these mechanisms are aligned with security standards, guidelines, and local regulations to avoid cyber threats. The cybersecurity audit can be viewed as a comprehensive review of the PPT. The audit is designed to be more formal than an assessment and includes a carefully curated test case checklist that validates if applied security control mechanisms are in place and work as intended. This approach offers flexibility to accommodate different organizations' heterogenous protection scenarios. There are multiple benefits of performing an audit:

- Risk Assessment — finding weaknesses that represent risks to the organizations is an essential benefit that helps prevent costly and disruptive breaches and prioritize improvements of security;

- Testing controls — existing controls may be put on a challenge to testing the confidence organizations have in their baseline. It represents an excellent opportunity to highlight potential weaknesses in the existing security posture;

- Identifying security gaps — the crucial benefit that appropriately detects further directions of improvement that are not covered in the current security posture. The gaps are the basis organizations can build upon and increase the performance of security controls;

- Improving security posture — by filling the gaps, stakeholders can rest assured that organizations are investing in maintaining the trust amongst all parties. This results in silent growth of the reputation and confidence of the organization in multiple directions;
- Compliance — by proactively practicing regular audits, this often comes as a final confirmation of the work previously done, making the formal evidence for the requirement fulfillment of the arbitrary standard, guideline, or regulation.

Different vectors drive the need for a security audit. Young organizations with low or moderate maturity levels might utilize the audits more often until their procerus and systems do not reach the desired quality target. This is the threshold where more mature organizations start optimizing and doing routine audits bi-annually or even biennial. In turn, cybersecurity audits can be utilized as a preparation for certification or recertification for a specific standard where the certificate's validity plays an important role in the decision process. The third vector covers the remaining irregularities — anything that is not considered a routine audit. Different events can trigger this need:

- Security incident or breach — repercussions these types of events make can be significant, and new, improved security controls emerged from incident response plans should also be audited;
- Existing system upgrade or new system installation — these events represent a milestone that can raise *red flags* since unintentional control overrides can happen;
- Changes to compliance requirements — as offensive techniques utilized by bad actors evolve, so as defensive techniques, and this drives the continual enhancements of the requirements;
- Digital transformation — new directions that Industry 4.0 introduces may reflect on the short- and long-term goals organizations

> set and directly reshape the system's security posture they currently have.

The Information Systems Audit and Control Association (ISACA) and Protiviti, in their report, state that cybersecurity is the top technology challenge for IT audit professionals [71]. The study also states that organizations should continuously review their IT audit plans to address cybersecurity threats and emerging technologies. It also shows that over 50% of organizations in all geographic regions consider conducting audits necessary. Similar results were presented by Slapnicar et al. [72], where internal audits vary between the countries and sectors, with a mean score of 58 on a Cybersecurity Audit Index scale from 0 to 100. Even if it is recognized as necessary, it is still challenging to do the audit since, e.g., the audited infrastructure may not reside only in a private network of the organization or the users are involved in activities that are only partially covered by the business purpose. That is why clear boundaries and objectives must be defined for each audit.

Standards provide a common set of reference points to enable organizations to evaluate whether they have processes, procedures, and other security controls that meet an agreed minimum. The importance of cybersecurity is fortunately recognized across the world, and official and unofficial bodies are developing different legislative procedures, regulations, and recommendation acts to address security issues. One of the first initiatives to certify software products in terms of security has been the Trusted Computer System Evaluation Criteria (TCSEC) in the United States or the Orange Book [73]. The government dictated certification, and it required detailed analysis by security experts and heavy involvement by the buyers in that process. It was a lengthy process that consequently made products under certification fall behind technology development. The Information Technology Security Evaluation Criteria (ITSEC) was introduced in Europe [74]. It later evolved into the Common Criteria that decreased certification costs but excluded the buyers from the certification process and made it less transparent overall [75].

In the past five years, the number of published acts in European countries has dramatically increased [76]. Security standards and recommendations developed by eminent bodies such as the International Organization for Standardization (ISO), National Institute of Standards and Technology, Center for Internet Security (CIS), European Union through the European Programme for Critical Infrastructure Protection (EPCIP) [77] represent the accumulated knowledge about cybersecurity in the form of formal security requirements that have undergone extensive peer review. Some of these standards require formal certification as evidence for compliance. In contrast to TCSEC and ITSEC, newer standards emphasize management notes, best practices, certification, and security governance [78]. This is exactly what security officers and decision-makers require, a security assessment methodology that can systematically present what has to be fulfilled [79, 80]. The security controls defined in these standards can be applied to different types of systems, from software used by small and medium-sized enterprises (SMEs) to robust systems used by large corporations. The use of standards-compliant security controls provides the best assurance of solid security for the organization and conforms to legal requirements. If the organization meets a particular set of security requirements, it gives the customers, suppliers, and partners confidence that the organization can perform on a mature security level. A standards-based approach to information security ensures that all controls are managed in a structured manner, ensuring that people, process, and technology costs are more streamlined and manageable. Security requirements are usually focused on protecting the Confidentiality, Integrity, and Availability of assets. This is also known as the CIA triad:

- Confidentiality — only authorized persons have access to the specific resource;

- Integrity — only authorized persons can change the data making it trustworthy and free from tampering;

- Availability — resources must be accessible to authorized persons whenever they are needed.

Using a standards-based approach can ensure that the CIA triad protection is met. Also, this can improve the reliability, availability, and stability of systems. The United States Government Accountability Office issued the report [81] in which it showed that out of 16 CI sectors, in only three sectors (defense industrial base, government facilities, water and wastewater systems) was determined the adoption of the NIST Framework for Improving Critical Infrastructure Cybersecurity [82]. Energy, food and agriculture, information technology, and transportation systems have taken steps to identify sector-wide improvements from framework use, and the rest nine sectors have not yet implemented these recommendations.

In the last two decades, we witnessed an alarming increase in terrorism and other forms of criminal activities. These malicious actors target critical infrastructure — primarily energy and utility sectors — to disrupt communication, shut down systems and services, and cause chaos. Taking into consideration everything stated in this section, to establish proper CIP and defend from malicious actors, it is necessary to define and follow secure processes and mechanisms that will help with the protection of everything that is considered necessary for public safety, economy, and national security, such as people, physical assets, and critical cyber networks. These initiatives require the involvement of researchers from both academia and industry to win in this warfare. One of the aggravating circumstances for the good actors represents commercial-off-the-shelf product vendors that untruthfully offer inadequate solutions and services to satisfy different security requirements. One example today would be the Zero Trust security model. Zero Trust — the term coined by Stephen Paul Marsh in his Ph.D. thesis [83] and popularized by John Kindervag — advocates that all resources must be continuously inspected and examined at the packet level to limit and strictly enforce access control to verify that everything is legitimate and secure since all network traffic must be considered untrusted [84]. By offering rebranded mature solutions, product vendors are twisting the Zero Trust paradigm, making it difficult for potential customers to choose the correct option. As Anderson states in [85], customers often buy products and services that may be suboptimal or even defective, but customers feel secure as long as they come from big-name suppliers.

When we accumulate the knowledge presented in previous paragraphs, to start the security uplift journey, we can recommend that organizations should begin with:

- assessing the maturity of their current security posture;
- understanding their current business initiatives and security projects;
- documenting where they can reuse existing capabilities;
- setting goals for their future maturity state and time frame to achieve it;
- practicing previously stated techniques for establishing a satisfactory security posture.

1.2 Motivation and Problem Statement

The thing worth noting is that the standards and audits usually complement each other. Internal or external audits usually ask for proof of compliance against a set of requirements. Sometimes, external audits result in formal certification of the product, system, or organization. In his work, Rannenberg [86] states that the idea of security certification was originally initiated by users and procurers hoping to ease the procurement process. Rice recommends mandatory certification of software and services [87]. Holding a certification demonstrates an organization's depth of cybersecurity knowledge, thus creating a competitive advantage. This is beneficial because the certification body can independently validate knowledge and experience. This audit-standards connection can be counterproductive as well. Schierholz and McGrath [88] point out that certification criteria are not publicly accessible and thus unavailable for evaluation by subject matter experts. They also point out that if several certification authorities compete, the certification they can provide can be identical, making the price the only factor that can affect the decision. Anderson [85] addresses perverse incentives for suppliers of security certifications that lead vendors who seek certification to hire auditors who have the laxest reading of a standard. In his work, Edelman states that less trustworthy market participants have more incentives to seek and obtain certification [89].

It is not unusual that organizations implement their security controls without following any formal guidelines by default. They are inherently liable for the risk resulting from insecure systems. Defining security requirements can be considered a complex task that requires engineers to have extensive security experience in security requirements elicitation and analysis. Most of them lack this knowledge [90], leading to an error-prone and insecure system [91]. When they decide to take security more seriously, they start aligning with one primary standard usually recognized worldwide. This often means that initially implemented security controls must be subsequently corrected. These activities also include risk assessments and internal audits to see the implementation status. While preparing for these audits or formal certification, comprehending different standards can be challenging. Different standards defined by different bodies can have similar requirements. This can introduce ambiguity within organizations regarding which standards they should align with and understand their similarities and differences. One approach for solving this problem would be to compare standards side by side to gain a deeper understanding and choose the appropriate one. This includes analyzing tradeoffs between different requirements, which implementation can offer a high level of protection relative to costs and effort needed for their fulfillment [45].

The new challenges arise with the increased number of new publications or new versions of the existing publications that are of utmost interest to the potential clients that must demonstrate compliance in their geographical regions. To display readiness for growing the business, alignment with more than one set of requirements becomes mandatory. We find that this is especially evident in, e.g., Smart Grid. These requirements are very demanding to understand and implement adequately.

Analyzing a handful of publications and their requirements resulted in an idea to construct an extensible model that can represent every new requirement from the arbitrary standard applicable to CI. This model could be used in applications that aim to help security practitioners and decision-makers with reasoning about which standards to comply with. It can also help with tracking and prioritization of requirement implementation. Further, to be able to enhance the security of the system or organization in this way, understanding the risks due to the potential for security failures is a must [92]. Risk assessment is sometimes done separately due to the nature of the organizational structure instead of being an integral part of the security uplift process. Making all these activities complement each other in some manner is another thing that needs to be addressed. These challenges are the main drivers of our research.

Based on this, we define the problem through the following research questions:

(1) *Can an extensible model be developed to represent the requirements from security standards applicable to the Critical Infrastructure?*

(2) *How to obtain information on the maturity of the security infrastructure of an organization or system in relation to the requirements defined in arbitrary security standards while using domain and organizational knowledge to conduct a risk assessment, planning, and tracking of the security improvements?*

The research described in this thesis aims to provide answers to these questions.

1.3 Research Hypotheses and Goals

Based on the research questions presented in Section 1.2, we define the hypotheses that the thesis discusses. They can be summarized as follows:

(**1**) **Hypothesis:** *It is possible to define a model for the representation of the requirements from different security standards, guidelines, and regulations for critical infrastructure. The model should allow the presentation of relevant information common to the requirements of different publications, thus allowing their cross-comparison.*

(**2**) **Hypothesis:** *It is possible to define criteria for prioritization of requirements that, in addition to risk, include the complexity introduced by the dependencies between the different roles of participants in the organizational structure in charge of implementing requirements, the level of importance of the compliance requirements, and the domain affiliation.*

(**3**) **Hypothesis:** *It is possible to extend the model to provide a unique domain-oriented view that allows simultaneous tracking of the implementation of similar requirements selected from different security standards, guidelines, and regulations for critical infrastructure.*

From the previously defined hypotheses, the primary goals of the proposed research are derived, where the expected results include:

(**1**) The definition of a model that uniformly represents the building blocks of security requirements that are defined in different publications. This goal refers to the first research question and is addressed in Chapter 3.

(2) Model extension with components for simultaneous tracking and prioritization of the implementation of similar requirements selected from different security standards, guidelines, and regulations for critical infrastructures. This goal refers to the second research question and is addressed in Chapter 3.

(3) Construction of the framework in accordance with the proposed model and validation that would confirm the practical applicability of the model and identify all its advantages and possible limitations. Details of this goal are discussed in Chapter 4.

1.4 Thesis Structure

Throughout this introductory **Chapter 1**, the problems that this thesis addresses and the necessary background to our work are presented. The rest of the thesis is outlined here.

Chapter 2 presents the literature review, where we first examine different models for security requirements engineering. On top of that, we analyze models that use industry standards as a basis. We further analyze security self-assessment tools and models they use to detect advantages and limitations they possess. This information is valuable for model and framework definition to address both research questions. We further analyze existing maturity models and commonly used risk assessment approaches. We finish the chapter with an analysis of existing prioritization criteria and define the thesis position.

Chapter 3 describes our methodology for model definition and extension. It starts with the description of security standards, guidelines, and regulations selection process. Further, we discuss what outputs of the analysis should be and how they can be used as elements of our model. The requirements information is used for a core model and assurance levels, actor dependency graph, and risk assessment elements as part of the prioritization criteria for the model extension. Finally, the model is presented as a Unified Modeling Language (UML) class diagram for easier readability.

In **Chapter 4**, a framework that uses the proposed model is presented to confirm the practical applicability of the model and to identify its advantages and eventual limitations. For each framework activity, we present security concepts and explain their contribution. Further, we illustrate a case study for framework usage. Finally, we discuss the advantages and limitations of the presented work.

Chapter 5 concludes the work of this thesis. It summarizes the main contributions and presents opportunities for further research and development.

Chapter 2

Research review

This chapter examines different approaches that address the problems defined in Section 1.2. Section 2.1 goes over the existing models and frameworks that can aid our research. Section 2.2 describes the self-assessment tools for cybersecurity resilience and standard compliance found in gray literature that can be used to extract models for requirement representation and catch sight of their limitations that can be addressed in our research. Section 2.3 gives an overview of common maturity models used in practice when assessing the overall state of security of the organization or system. Section 2.4 provides information about different risk assessment approaches that influence our research. In Section 2.5, we describe different techniques for prioritization criteria. Section 2.6 concludes this chapter and gives the position of this thesis compared to research previously reviewed.

2.1 Models for Requirement Representation

Before we can make any analysis of security requirements in security standards, we need to see how security requirements can be defined and elicited in security requirements engineering. Security requirements are considered nonfunctional, quality requirements [93, 94]. Security requirements engineering research the protection of assets from potential threats that may lead to harm, as interpreted by Haley et al. [95]. Nhlabatsi et al. [96] classified approaches to security requirements engineering into four classes:

- Goal-based
- Model-based
- Problem-oriented
- Process-oriented

Goal-based approaches use goals to capture security requirements. Secure Tropos, developed by Mouratidis et al. [97, 98], is one representative of goal-based approaches. It extends software development methods based on the paradigm of agent-oriented software development called Tropos [99] with security concepts such as security constraints, dependencies, goals, and secure entities. Security constraints can be interpreted as security conditions or requirements that users cannot ignore but interpret as an obstacle that restricts the achievement of users' goals. The Anti-Models method defined by van Lamsweerde [100] builds two concurrent models — the desired model of a system and the anti-model with vulnerabilities required for achieving anti-goals — and combines findings to enrich the system with new security requirements. It extends Knowledge Acquisition in automated Specification (KAOS) framework for goal-oriented requirements engineering [101], e.g., with new patterns for formal elicitation of security requirements and duality principle for modeling threats.

Model-based approaches advocate that the models help requirements analysts to understand software problems and identify potential solutions using abstractions. Two prominent representatives are UMLSec and SecureUML. UMLSec is a UML extension that allows users to add security stereotypes and constraints to system design [102]. It can be used to evaluate UML system specifications for vulnerabilities using formal semantics. UMLSec was used as a basis for CARiSMA tool that can enrich the system model with security requirements focusing on confidentiality, integrity, and availability features in order to perform security analysis [103]. Like UMLSec, SecureUML is a UML extension that uses role-based access control (RBAC) policies to define and enforce authorization constraints into UML-based modeled systems [104].

Problem-oriented approaches provide tools for the analysis of software development problems. Lin et al. [105] define anti-requirements and abuse frames as an extension of the problem frames introduced by Jackson [106]. In contrast to problem frames that focus on defensive requirements that must be satisfied, the anti-requirements define malicious users' intentions that must be prevented. Authors integrate anti-requirements into abuse frames to represent security threats and derive requirements from them. Misuse cases are another example of this approach. It represents a negative form of use cases, i.e., use cases that can negatively impact the system [107]. Sindre et al. [108] suggest generic threats and generic security requirements as the two primary reusable artifacts for misuse cases. Haley et al. [95] present the framework that requires defining context for the system using a problem-oriented notation and then validating against the security requirements through the construction of a satisfaction argument.

Process-oriented approaches focus on multi-step processes for security requirements analysis. The System Quality Requirements Engineering (SQUARE) is a nine-step process model developed at Carnegie Mellon University to provide means for eliciting, categorizing, and prioritizing security requirements for information technology systems and applications [109] The idea behind SQUARE is to build security concepts into the early stages of the development life cycle and not as an afterthought. One of the steps requires performing risk assessment as it can help identify the high-priority security exposures. Georg et al. [110] propose a methodology based on aspect-oriented modeling for incorporating security mechanisms in an application using activities such as risk analysis and misuse model generation.

Roudier et al. argue that this classification only represents different perspectives over the same process of security requirement engineering [111]. The authors create ontologies around concepts presented in different previously mentioned approaches and present a meta-model with key concepts that we use in our model. Souag et al. [112] analyze different approaches and cross them with ontologies previously defined in [113] to see how different models reuse them. We found that following only one approach might be more straightforward, but the combination of several approaches can provide us with hidden design vectors worth analyzing. This security requirements engineering analysis provided us with security concepts that need to be included in the further analysis when we shift right and observe requirements defined in security standards. These security concepts, along with their definitions, are:

- Security Requirements — *requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted* as defined in Federal Information Processing Standard (FIPS) 200 [114];

- Assets — *items of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology components) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation)* as defined in NIST SP 800-160 [115];

- Threats — *any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of* *information, and/or denial of service* as defined in NIST SP 800-30 Revision 1 [116];

- Security Goals — *goals that, when met, contribute to meeting some other security goals or ensures that one or more security properties desired by some stakeholder hold* as defined in [117];
- Security Controls — *the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information* as defined in NIST 800-53 revision 5 [118];
- Vulnerabilities — *the collection of properties of an infrastructure system that might weaken or limit its ability to maintain its intended function, or provide its intended services, when exposed to threats and hazards that originate both within and outside of the boundaries of the system* as defined in [54];
- Risks — *measures of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence* as defined in NIST 800-37 [119].

One way to bring only meaningful security requirements into the spotlight would be to standardize specific sets of requirements that can be applied across different domains or, if this is not the case, only in specific sectors. We next focus on security requirements defined in security standards in our analysis. Influenced by the work of Sunyaev [120], who developed the HatSec method for security analysis for the healthcare domain, Beckers et al. defined a conceptual model for security standards that contains concepts and terms from different security standards [121]. The authors created a template based on that model where fields in the template correspond to the concepts defined in the model. This template can be used to make instances for different security standards and compare them field by field. The primary goal of the comparison is to learn about different standards and help with the decision of the suitable standard for certification. The template describes what information the standards present and on which level of detail. Also, the template provides an overview of the security analysis driven by the standards but more on a high level. As input for templates, a small number of similar standards were used (such as International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001 and German IT-Grundschutz). Also, the authors defined uniform terminology used in different standards, but as only a few standards were used as an input, terminology cannot be considered complete.

Hale and Gamble [122] define a process that uses reusable patterns, model templates, and semantic relations to make patterns out of security controls and make a connection to other controls. The process is based on semantic hierarchies that can extract relevant security requirements from control standards using three patterns - impose, perform, and protect. The applicability of the process is demonstrated by the audit domain security requirements of the NIST SP 800-53, Department of Defense Instruction (DoDI) 8500.2, and ISO 15408-2 standards.

The NIST Cybersecurity Framework (CSF) defines one view through which security requirements can be analyzed [82]. The CSF is a risk-based approach to managing cybersecurity risk. It consists of the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core defines activities required to achieve security outcomes. The Framework Implementation Tiers give context on how an organization should interpret and manage security risks. The Framework Profile allows an organization to describe the current or desired state of the security posture in terms of alignment with security requirements. CSF defines 23 domains (i.e., dimensions, categories, or areas of knowledge). The framework is flexible enough to allow users to extend and adjust domains. One example of extension is implemented in Italy [123]. The requirement domains are classified into five functions: identify, protect, detect, respond, and recover. The Framework Core defines these functions to provide a high-level view of the lifecycle of an organization's management of cybersecurity risk. One disadvantage that can be mentioned is that when domains are grouped by functions, it limits the flexibility and scalability of security requirements inside a domain. Requirements that are classified in one domain can be assigned to different functions, not only in one. Also, the degree of dependency on technology, people, and processes varies as we progress through the five functions according to the Cyber Defense Matrix [124].

Leszczyna systematically reviewed the most relevant Smart Grid standards, guidelines, technical reports, special publications, and regulations [125]. The research goal was to provide guidance to security practitioners while making comprehensive security assessments. The study found that six Smart Grid or power systems' standards can be applied to IACS, substations, or all Smart Grid components. While these standards provide general guidance, they can still be used as a reference for implementing security controls. In [126], the authors compare security control coverage between several standards in the energy sector. The security controls that are recognized in this research as important are covered by most of the standards. This is encouraging, but it is interesting to note that personnel qualification is not so important and user training is an almost mandatory requirement by all standards. Similar research focusing on SCADA systems is done by Alcaraz and Zeadally [127] and Sommestad et al. [128].

These papers can be classified as a systematic literature review and do not provide information about security requirement modeling. They still provide guidance on what to look for in security standard analysis and set the right expectations when it comes to information that security standards can give.

2.2 Self-assessment Tools for Cybersecurity Resilience and Standard Compliance

Literature analysis showed that a couple of tools exist for self-assessment for cybersecurity resilience and standards compliance [129]. For example, the Department of Homeland Security (DHS) developed the Cyber Security Evaluation Tool (CSET) [130]. CSET provides a framework for the vulnerability analysis typical for ICS and IT architectures. It can serve as a centralized repository for security requirements. The database has a comprehensive list of requirements from different publicly available standards and commercial ones. To start with the assessment, users must choose the appropriate Security Assurance Level (SAL) that represents the overall criticality rating that is based on the user reviews of security scenarios and estimated consequences. The SAL level — which can be set to low, medium, high, or very high — expects the user to estimate in advance how detailed the assessment will be. Depending on the selected SAL level, the tool will show an increased number of questions that require detailed answers. SAL level is also used as one of the factors to rank questions without answers at the end of the assessment. There are three types of SAL: default (application SAL), SAL based on NIST SP 800-60 [131], and SAL based on FIPS 199 [132]. The tool provides a way to document vulnerabilities by answering the questionnaire that includes questions from standards and custom questions curated by security experts. The tool provides the plugin for graphical modeling of the system architecture. Depending on the components that are drawn, the questionnaire can be further enriched with component-specific questions. Every question has its rank that follows these rules:

- Questions are weighted by subject matter experts with years of experience in information technology and control system cybersecurity relative to other questions;

- Every domain in which the questions were classified was given weight in the same manner;
- Every question is connected to the SAL level that can affect the overall weight of the question only if the SAL is greater than low (e.g., if the SAL level is set to very high for the question, the requirement is quite specific and not so high on the priority list).

The tool can be used in various CI sectors and can be beneficial for organizations since it is open source. It has some limitations, however. CSET puts more focus on individual components but not on the whole solution. The architecture drawing feature provides only high-level questions about the components that add a little value. It does not insist on detailed risk assessment. Cross-standard self-assessment is not provided since every standard is analyzed in isolation without an option to group requirements by similarity. Also, there is a lack of documentation about the ranking and weighting of the questions in the questionnaire. While the only transparent factor is SAL level, other factors include subject matter experts' opinions without clear metrics.

Control System Cyber Security Self-Assessment Tool (CS2SAT) is presented in [133]. The tool was developed by Idaho National Laboratory (INL), and it is the property of the United States Department of Energy. The tool's primary purpose is to enable users to assess the security of the control systems. The tool has a database with a couple of standards, based on which INL created a questionnaire. The idea that the tool propagate is to form a working group whose members would be people from different organizational divisions that have the capability to collect required documentation that can be used to fill in the questionnaire appropriately. As in [130], the tool requires users to define a few SALs that reflect possible consequences after the system was compromised to choose the best mitigation measures for security issues. Also, the tool enables users to draw system architecture. After the users draw the system architecture, questions are classified based on the components that are used on the diagram. Additionally, a set of questions is directly linked with selected standards. Reports can be generated that show where unconformities are detected on the component or standard level. CS2SAT's algorithm prioritizes recommendations based on the criticality of the component, relevance of the requirements, and the gap *size* between where the system is currently at and where the requirements expect it to be. These three factors form the basis for further mitigation suggestions. Also, results in the report can be categorized based on PPT and then decomposed in a more fine-grained manner for further analysis.

The Cyber Resilience Review Self-Assessment Package (CRR) is presented in [134]. The tool is one Portable Document Format (PDF) file with 299 questions classified into ten groups. The questionnaire aims to assess security practices in CI and their operational resilience. The focus is put on areas that will bring better security and resilience measures during normal and stressful operations. The questions are based on a couple of standards (e.g., NIST SP 800-18 [135], NIST SP 800-30 [116], NERC CIP [57], Federal Information System Controls Audit Manual (FISCAM) [136], FIPS 102 [137] but the tool does not check for compliance against them but only gives the overall score. Each question focuses on assets classified into four categories: people, information, technology, and facilities. The user has to mark how each of the four assets is affected for each question. The overall impression is that the high-level questionnaire represents a form of quick audit since it is projected to be delivered during the six-hour workshop. The Center for Internet Security developed its self-assessment tool around CIS controls [138]. It is a web application that enables users to track and prioritize their implementations of the CIS Controls. It also includes knowledge extracted from a couple of standards, such as NIST SP 800-53 [118] and Payment Card Industry Data Security Standard (PCI DSS) [139]. The users can also see how their systems are positioned against the industry average. Other self-assessment tools that we found are omitted from detailed analysis due to their lower complexity that would not bring anything new to the discussion.

The Open Security Controls Assessment Language (OSCAL) was developed as a collaborative effort by the NIST and The Federal Risk and Authorization Management Program (FedRAMP) [140] OSCAL provides a machine-readable meta schema for different compliance and risk management frameworks expressed in eXtensible Markup Language (XML), JavaScript Object Notation (JSON), and YAML Ain't Markup Language (YAML). It is also used for sharing system security plans, security assessment plans, and reports. The main goal is to enable organizations to exchange information via automation and provide interoperability. It consists of several layers:

- *Controls Layer* is the lowest layer with two models — *Catalog Model* and *Profile Model.* The *Catalog Model*represents a collection of security controls in standardized, machine-readable formats such as XML. This is suitable for easier information search and conversion between formats. The *Profile Model* represents a baseline that consists of selected controls from catalogs. It can provide a set of controls required to achieve a certain level of security. Besides the information imported from catalogs, it also provides placeholders for describing what to import, merge or modify from the *Catalog Model.* The OSCAL is viewed as an ongoing development, so there are only a few examples of future usage of these merging and modifying features that aim to link and modify similar security controls.

- *Implementation Layer* consists of the *Component Definition Model* and *System Security Plan Model.* The maintainers of the hardware, software, or services develop the*Component Definition Model* to describe in detail the controls that are supported for this specific hardware, software, or service. *System Security Plan Model* — as the name suggests — enables the modeling of highly granular system security plan content, including points of contact, system characteristics, and control compliance descriptions.

- *Assessment Layer* consists of an *Assessment Plan*, *Assessment Results Model*, and *Plan of Actions and Milestones Model*. The *Assessment Plan* contains information on how to perform an assessment or continuous monitoring activities. The *Assessment Results Model* collects information produced from a set of assessment activities, and the *Plan of Actions and Milestones Model* provides placeholders for addressing the findings.

We find OSCAL a promising initiative led by respected organizations that can be built upon. The idea of interoperability and easier exchange of standards in clearly defined form is a step towards the renovation of the topic. However, since it can be considered a new initiative in the early stage of development, the adoption rate amongst the organizations is yet to be determined. For our research, we try to define a model that will be compatible with foundational parts of the OSCAL.

All these tools were analyzed to collect information that would be beneficial for the model that we aim to define. They also pointed out which standards would be interesting for detailed analysis. While these tools are built to support security practitioners in their decisions, their documentation lacks the details that are of utmost interest to our research, such as approaches for requirements mapping, a weighting system for the requirement prioritization, or a clear connection between the requirements and risk assessment.

2.3 Maturity Models

Capability Maturity Model Integration (CMMI) describes best practices that can help organizations improve their processes. Specifically, CMMI for Development provides guidance for the efficient development of products and services [141]. Even though CMMI focuses on processes, the maturity levels that it defines can be applied to other segments of organizations or the systems they develop. CMMI defines two paths using levels. One path defines that organizations have to improve processes in selected areas (capability levels) incrementally, and the other enables organizations to improve the overall state of their processes by incrementally addressing sets of process areas (maturity levels). There are four capability levels:

- Level 0 — Incomplete — the process is either not performed or is partially performed;
- Level 1 — Performed — process satisfies defined work to produce expected products;
- Level 2 — Managed — process is planned and executed in accordance with policy;
- Level 3 — Defined — process is accommodated to an organization's specific needs and based on the organization's set of processes.

There are five maturity levels:

- Level 1 — Initial — process is ad hoc;
- Level 2 — Managed — process is planned and executed in accordance with policy;
- Level 3 — Defined — process is well defined, accommodated to specific organization's needs, and improved over time;
- Level 4 — Quantitatively Managed — quantitative objectives per customer and organization's needs are defined and followed for better process performance;
- Level 5 — Optimizing — processes are continuously improved based on the quantitative understanding of business objectives.

Gilsinn and Schierholz introduced the concept of a vector of Security Assurance Levels (SALs) to describe the protection factor needed to ensure the system's security [142]. The SALs aim to help standard developers, users, and vendors to understand the protection factor without going into details about each standard individually. They represent a qualitative approach to addressing the security of a system split into zones. SALs can be broken down into four different types that can be used in different phases of the security life cycle:

- Target SAL — represents the desired level of security for a system;
- Design SAL — represents the planned level of security for a system;
- Achieved SAL — represents the actual level of security for a system;
- Capability SAL — represents the security level that a system can reach if appropriately configured.

These SALs are based on the seven foundational requirements that are defined in International Electrotechnical Commission (IEC) 62443 standards:

- Access control;
- Use control;
- Data integrity;
- Data confidentiality;
- Restrict data flow;
- Timely response to an event;
- Resource availability.

Here, SALs are not expressed as a single number but as a vector of values that match seven foundational requirements. SALs are defined in four levels, where each level increases the security posture:

- SAL 1 — describes protection against casual or coincidental violation. These violations — usually loose policies and procedures — can come both from employees and outside attackers;
- SAL 2 — describes protection against intentional violation using simple means. These means do not require many details about the security of the system;
- SAL 3 — describes protection against intentional violation using sophisticated means. Here, attackers require advanced knowledge about a specific system's security to craft custom attacks;
- SAL 4 — describes protection against intentional violation using sophisticated means with extended resources. The difference between SAL 3 and SAL 4 is in the resources that the attackers have at their disposal.

The Cybersecurity Capability Maturity Model (C2M2) was developed by several bodies in the United States, mainly oriented toward the electricity, oil, and gas sectors [143]. It is descriptive guidance that proposes practices applicable to information technology and operations technology assets. It is designed for organizations to measure and improve their cybersecurity programs. The guideline defines the maturity model as *a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline* [143]. The maturity model that C2M2 proposes is a benchmark against which organizations can evaluate the current level of capability of their practices, processes, and security controls. Measuring current posture can be beneficial to organizations since they can evolve and transition into a more mature state. The model defines four maturity indicator levels (MILs):

- MIL 0 — practices are not performed;
- MIL 1 — practices are performed but mostly ad hoc;
- MIL 2 — practices are documented and more advanced than at MIL 1;
- MIL 3 — policies are set in place, and personnel has proper training and skills.

These MILs can be applied independently to each group of security practices. C2M2 also states that evaluation quality depends on who performs the practice, when, and with which tools and techniques. The maturity may be good even if this is done ad hoc. The main problem is that this approach cannot repeatedly give the same satisfactory results. Thus, documenting steps and defining policies that must be followed are crucial parts of the security uplift journey.

By looking at the three mentioned models, we can see a level of similarity among them. CMMI gives two views and provides choices to organizations. Even though maturity levels are more fine-grained than capability levels, the capability levels seem to provide more flexibility since the organization can focus only on those areas where improvement aligns with business objectives. The SAL levels are pure security levels that are oriented toward systems. We would agree with the authors [142] and extend SAL with level 0 — much like Level 0 in C2M2 — to label systems with zero controls to satisfy security requirements. C2M2 is more process-oriented but remains within cybersecurity boundaries. The critical observation is that no matter how good resources an organization has, the quality would not be consistent over time if the work is not done systematically.

2.4 Risk Assessment Methods

Risk assessment is a necessary process that must be practiced in the organization. It is used to identify, estimate, and prioritize risks to the organization in terms of assets, operations, employees, and other organizations when some action is performed or some system is used. This is recognized as an important point in NIST Cybersecurity Framework. Implementation Tiers suggest having risk management practices set in place to implement CSF successfully. The framework defines four tiers that support organizational decision-making about how to manage security risks: partial, risk-informed, repeatable, and adaptive. CSF explicitly states that these tiers are not maturity levels and that progression to higher tiers is only encouraged when feasible and aligned with the organization's upper management decisions. A proper risk assessment methodology is critical for a successful CIP program. Various standards and enterprise models describe how risk assessment should be practiced [144, 145]. The methodologies for conducting risk assessment might be different regarding the applicability domain and the audience, but they all use common elements that are recognized in Section 2.1 — threats and vulnerabilities that have to be identified, classified, and their impact evaluated.

The two standardized approaches are NIST SP 800-30 Revision 1 [116] and ISO/IEC 27005:2011 [146]. Al Fikri et al. [147] even proposed a methodology that combines these two approaches. NIST SP 800-30 provides guidance for conducting risk assessments of federal information systems and organizations. It identifies three levels on which risk assessment can be conducted – organization level, mission/business process level, and information system level. The risk assessment process is done in four steps:

(1) Assessment preparation — required to define the scope of the assessment, including gathering all inputs, assumptions, and constraints that are relevant;

(2) Performing assessment — aims to detect all risks by analyzing threats and vulnerabilities, impacts and likelihoods of exploitations;

(3) Results communication — required to provide the decision-makers with necessary information about detected risks to guide them in further decisions;

(4) Assessment maintenance — required to keep relevant information about the risks up to date if the situation changes.

Each step consists of several tasks and supplemental guidance on how to perform them successfully. NIST SP 800-30 has comprehensive tables of threats, vulnerabilities, impacts, and likelihoods of threat events occurring. This can be a good source of information even for other risk assessment methodologies. NIST SP 800-30 suggests using the following formula for calculating risks:

$$Risk = Likelihood \times Impact \tag{2.1}$$

The likelihood of the risk can be further expressed as:

$$Likelihood = Threat \times Vulnerabilities \tag{2.2}$$

For example, if the software or library used in the system has a known vulnerability, there is a threat of malicious actors exploiting that vulnerability to compromise the system. The threat can be eliminated if the software is regularly updated to fix known issues. On the other hand, the impact expresses the level of consequences the organization or system will have if the threat occurs. The risk expressed as the product of likelihood and impact is a widely accepted formula, even though alternatives exist [148, 149, 150]. With a combination of likelihood and impact, the risk level can be determined on a qualitative scale of *very low to very high* or a semi-quantitative scale of 0–10, as presented in Table 2.1.

Likelihood	**Level of Impact**				
	Very Low (0)	**Low (2)**	**Moderate (5)**	**High (8)**	**Very High (10)**
Very High (10)	Very Low	Low	Moderate	High	Very High
High (8)	Very Low	Low	Moderate	High	Very High
Moderate (5)	Very Low	Low	Moderate	Moderate	High
Low (2)	Very Low	Low	Low	Low	Moderate
Very Low (0)	Very Low	Very Low	Very Low	Low	Low

Table 2.1: NIST SP 800-30 Level of Risk Assessment Scale

ISO/IEC 27005:2011 gives guidelines for the risk management process for information and security in organizations that support ISMS following ISO/IEC 27001. It describes both high-level and detailed approaches for performing a risk assessment. The risk assessment process is done in six steps:

(1) Context establishment — required to determine the scope and purpose of risk assessment;

(2) Performing risk assessment — consists of risk identification, estimation, and evaluation. These are required steps to define what could cause a loss to an organization, which estimation methodology to use, and how to compare risks with evaluation criteria;

(3) Risk treatment — provides different guidance options on how to address identified risks;

(4) Risk acceptance — provides details on how to meet acceptance criteria;

(5) Risk communication — gives guidance on how information about risks is communicated between decision-makers and other stakeholders;

(6) Risk monitoring and review — points out key guidance that should be continuously monitored and improved.

ISO/IEC 27005:2011 also uses matrices similar to NIST SP 800-30 to express risks in a qualitative and quantitative manner, considering different likelihoods and consequences on business and organization assets. As in NIST SP 800-30, ISO/IEC 27005:2011 gives a comprehensive collection of threats and vulnerabilities.

One representative of enterprise models for risk assessment is the Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro (OCTAVE Allegro) methodology. It is a security risk evaluation methodology developed by the Software Engineering Institute at Carnegie Mellon University [151]. It was designed to allow users to assess risk without extensive organizational knowledge, expertise, or input. It consists of eight steps grouped into four phases. In the first phase, the organization must develop risk measurement criteria. During the second phase, information assets are profiled to identify which assets are used and how. In the third phase, the organization must identify threats to the information assets. In the final phase, risks are identified, analyzed, and mitigated.

Another example is the Factor Analysis of Information Risk (FAIR) [152]. A security consultant Jack Jones designed FAIR to help organizations understand, analyze and measure information risk. Like other methodologies, FAIR follows a formal framework that has four stages. In the first stage, assets and threats to them must be identified. During the second stage, it is necessary to collect information to make an estimation of how threats can harm the assets that will result in losses, both direct and indirect. In stage three, it is calculated how much loss the organization can expect. In the final stage, risks are derived and articulated qualitatively.

Filippini et al. [153] reviewed over 20 more approaches that can be applied to critical infrastructures. Cherdantseva et al. [154] presented 24 risk assessment methods applicable to SCADA systems. They find that methods can be roughly classified based on their details (guidelines, activity-specific methods, and elaborated guidelines) and their expressiveness (model-based and formula-based). This is the proper classification for all approaches mentioned in this section. We can notice that a significant number of risk assessment methodologies exist, thus making it difficult to choose one. Hence, organizations usually go with standardized ones like NIST SP 800-30 and ISO/IEC 27005. Whichever risk assessment is used, the primary focus must be put on the fact that this is an important activity that must be regularly exercised. Thus, it is one of the essential parts of our model and framework.

2.5 Techniques for Requirement Prioritization

A significant number of methods for requirements prioritization have been proposed in the literature [155]. These methods face different challenges such as budget, time, resources, and technical constraints. They also depend on the opinion of the subject matter experts and stakeholders' expectations. Achimugu et al. [156] find many error-prone, with scalability issues, and lack the social actors' aspect. This makes the choice of the suitable method more difficult. The priority for any decision is usually determined by examining multiple factors. Different authors [157, 158] among the most popular methods for multi-criteria decision-making problems emphasize Analytical Hierarchy Process (AHP) [159], Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS) [160], and Simple Additive Weighting (SAW) [161]. Detecting criteria and assigning weights to them is common for all three techniques.

AHP is a model that aims to simplify the assessment of all criteria related to decision-making by organizing them into a hierarchy, evaluating pairwise comparisons between relevant elements in a hierarchy, and finally gathering weighted results from the process. It can be time-consuming and not scalable for a more significant number of requirements [162]. TOPSIS aims to obtain the farthest and shortest distance from the negative and positive ideal solutions, respectively. It also adds weights to each criterion and calculates the geometric distance between each alternative and the alternative that has the best score in each criterion. Compared to AHP, it lacks the ability to organize requirements hierarchically, and scores can be difficult to update if irrelevant requirement is introduced [163]. In SAW, the final score of each alternative for ranking is calculated by summing the weighted criteria. It is easy to use, but the limitation is that the larger rank always makes that decision alternative better. This puts greater responsibility on the decision-maker to choose the proper weights for all requirements.

Karlsson et al. [164] state that a prioritizing session could consist of three consecutive stages:

- The preparation stage — a team is assembled for the session and supplied with available information used to structure the requirements;
- The execution stage — using the inputs from the previous stage, the decision-makers define the requirements prioritization;
- The presentation stage — in this stage, results are presented to the persons of interest.

Most of the proposed methods in [155] can be applied to security requirements. Tariq et al. presented an exciting approach to prioritizing the information security controls in cloud computing and wireless sensor networks using a fuzzy analytical hierarchy process [165]. The authors consulted decision-makers and defined seven main criteria for security controls selection: implementation time, effectiveness, risk, budgetary constraints, exploitation time, maintenance cost, and mitigation time. The controls were assigned weight for each criterion, and the best control was the one with the highest score. The proposed approach was applied to ISO/IEC 27001 security controls. In [166], the authors propose an extension to threat modeling with the goal of allowing the prioritization of security requirements via a valuation graph that includes assets, threats, and countermeasures. Some authors propose utilizing data mining and machine learning techniques to automate the prioritization of the requirements [167], though the used algorithms limit effectiveness, and efforts from the stakeholders are still needed.

Literature analysis showed us that different factors have to be included in defining appropriate prioritization criteria for requirement implementation. These factors include, e.g., how easy the criteria can be used, the level of involvement of the users (primarily stakeholders), how accurate the final result should be, and how risk assessment can affect the priority.

2.6 Thesis Position

The previous sections described different aspects of our research, interesting concepts, and implementations.

Looking at the literature review, we can conclude that similar standards were analyzed. In this thesis, we want to provide more width to the analysis of security publications by introducing more variety, from organizational standards to horizontally applicable system standards to guidelines and respected local regulatory documents.

Further, we want to provide a model as one solution to some limitations pointed out in previous sections and be flexible to complement existing solutions such as OSCAL.

Instead of traditional isolated standard analysis, we want to provide a framework that would simultaneously lead the users through a cross-comparison of multiple standards and make compliance preparation easier in terms of accommodation to organization structure, risk assessment, and implementation.

Chapter 3

Model for Requirement Representation

This chapter presents the core of the thesis that addresses the research questions defined in Chapter 1. The proposed model for security requirement representation is described in detail, from the analysis of relevant standards that influenced model creation to addressing some limitations of existing solutions described in Chapter 2 to setting the screen for model validation. Proposing a plain model for security requirements purely based on the entities extracted from the security standards is not sufficient. This thesis aims to extend the base model of the security requirements with elements that surround the implementation process, which can bring value if they are documented.

Our research has used a three-stage methodology, as presented in Figure 3.1.

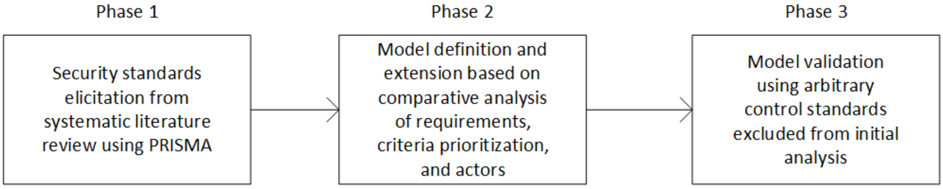

Phase 1
Security standards elicitation from systematic literature review using PRISMA
Phase 2
Model definition and extension based on comparative analysis of requirements, criteria prioritization, and actors
Phase 3
Model validation using arbitrary control standards excluded from initial analysis

Figure 3.1: Three-stage research methodology

Section 3.1 presents the first stage that focuses on security publication elicitation from the systematic literature review. The outputs from this stage are relevant standards, guidelines, and regulations that are further used for information extraction and pattern detection. Section 3.2 presents how selected publications and their requirements are used to form appropriate classification that will be the foundation for requirements grouping by similarity. Sections 3.3, 3.4, and 3.5 further explain components that have to be included as an extension of the initial model to allow cross-standard compliance tracking and requirement prioritization: assurance model definition, actors' involvement, and prioritization criteria, respectively. Section 3.6 presents the second phase, i.e., the model definition that uses the outputs of phase one. The third and final stage, model validation, is described separately in Chapter 4.

3.1 Publication Selection

The first part of the first phase is a systematic literature review and analysis of relevant security standards, guidelines, and regulations for critical infrastructure. The literature review was done using the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) methodology [168]. Thome et al. [169] and Cooper [170] use similar concepts, but due to the wide acceptance of PRISMA as a *de facto* standard for meta-synthesis and meta-analysis not bounded by specific research designs, we decided to follow this methodology [171].

The rationale for conducting a systematic literature review lies in the fact that from these results, we can detect which publications are worth considering for further analysis due to their structure and applicability. Many publications exist today — especially those applicable to a specific country or region — and they are heavily influenced by more mature standards [76]. For example, German IT-Grundschutz [172] is quite similar to ISO/IEC 27001 [173], and the United Kingdom's Cyber Assessment Framework (CAF) [174] references ISO/IEC 27001, ISO/IEC 27002 [175] and IEC 62443 [176] in almost every chapter. The main objective of the analysis is to find the publications that have the most occurrences in scientific papers, books, and technical reports that are mentioned in the context of the protection of critical infrastructures. The occurrence numbers will be a good indicator that a particular publication must be analyzed in more detail due to their relevance in the scientific papers. Hunter [177], Kuglowski [178], and Gazis [179] presented qualitative approaches for standard evaluation by domain, structure, and maturity. Also, a quantitative approach is described in the works of Sommestad et al. [128], that base their evaluation on the number of occurrences of specific keywords in the text. The publication identification phase was initially based on the quantitative approach in our research. This often regenerates much noise in the initial record set. Hence, we introduced some qualitative requirements during the screening process for more fine-grained results.

The eligibility criteria for the relevant publications we previously defined in [45] are as follows:

- The publication has a published version in English;
- A standardization body or government institution published the publication;
- The publication has to specify security requirements that can be used for similarity and compliance testing. This means that the requirements are well structured and classified and not defined in the form of, e.g., an essay;

- The publication is primarily security and not privacy-oriented. Nonetheless, publications may have privacy-related requirements.

Additional criteria that were applied followed these rules:

- At least one publication had to be general and not too domain-specific so that it can be adapted to the different critical infrastructure sectors;

- Standards had priorities over guidelines, and guidelines had priorities over regulations. The reason for this is that certifications are done against specific standards. On the other hand, guidelines are not obligatory for full compliance, and regulations are usually applied only at a national level not having extensive geographical coverage;

- The adoption level had to be high, and this was confirmed with occurrence numbers and consulting grey literature.

The aggregative databases were used in the search, concretely Google Scholar and Semantic Scholar that contained papers of numerous publishers and recognized publishers such as the Institute of Electrical and Electronics Engineers (IEEE), Springer, and Association for Computing Machinery (ACM). Search keywords were *cybersecurity standards*, *security standard*, *critical infrastructure standard*, and *security requirements*, but this resulted in more than 40,000 results. The additional keywords *oil and gas*, *smart grid*, *power grid*, *electrical grid*, *water*, *nuclear*, *food and agriculture*, *transportation*, *finance*, *dams*, and *healthcare* were distinctively added in combination with the first four to get more narrow results. Even though these search engines can do Boolean searches, in this case, they looked at each of the keywords individually or all of them at once, so the initial results had to be refined further by looking at the titles, keywords, abstracts, and eliminating duplicate and irrelevant studies, as well as employing backward and forward reference *snowballing* strategy.

This approach significantly decreased the initial records count, and 62 papers were further analyzed. After reviewing the selected papers, 34 only mentioned relevant publications in other contexts, and only a few presented the research more comprehensively. The occurrence of the most mentioned publications in relevant context is presented in Table 3.1.

Publication	**Type of Publication**	**Occurrence**
NERC CIP	Regulation	16
IEC 62351	Standard	14
ISO/IEC 27001/27002	Standard	11
NISTIR 7628	Standard	11
HIPAA	Regulation	9
NIST SP 800-53	Guideline	9
IEC 62443 (ISA 99)	Standard	8
NIST SP 800-82	Guideline	6
IEC 61850	Standard	4
PCI DSS	Standard	3
GB/T 22239	Standard	3
DHS Catalog	Guideline	2

Table 3.1: Publication occurrences in the study

The publications with only one occurrence were omitted from the tabular representation as less relevant for further analysis. By looking at Table 3.1, we can conclude that one of the highest numbers of occurrences have general-purpose standards and guidelines such as ISO/IEC 27001/27002 and NIST SP 800-53. Also, smart grid publications have a dominant number of occurrences making this sector, solely on the occurrence numbers, very interesting from the security regulatory standpoint. Some sectors, such as nuclear, food and agriculture, had one or zero occurrences, making them less relevant to the security scientific community. Most of the publications are globally recognized, and the majority were developed by organizations in the United States, but the Chinese GB/T 22239 information security technology standard [180] can be emphasized as an honorable mention.

As with any literature review, the limitations of our review process must be noted. The analysis was done based only on our interpretation of the papers. Also, we cannot rule out the possibility that other relevant standards exist and are used only in some geographic regions. Some publications may not have found their place in the review due to different reasons, such as terminology used by authors which did not bring a paper to the attention of our analysis, a paper not being listed on the databases examined, or not consulting the gray literature that might have more relevant information. The literature search method adopted still helped ensure an acceptable level of completeness of our literature review, considering the limitations previously mentioned. Hence, we believe that the papers analyzed are representative, and the analysis results may be generalized for different critical infrastructure domains.

The final set of publications that were used for further analysis was the following:

- IEC 62443
- ISO/IEC 27001 and 27002
- NIST SP 800-53
- NERC CIP

3.1.1 Selected Standards

3.1.1.1 IEC 62443-3-3:2013 (ISA 99)

IEC 62443 are international series of standards developed by IEC and the International Society of Automation (ISA99). These standards were developed to systematically address the need to identify vulnerabilities in IACS environments and mitigate them. Series cover organizational and technical aspects of security throughout the whole system's life cycle. The standards are designated as *horizontal*, meaning that they are proven to be applicable to a wide range of different industries. Standards are grouped into four groups to cover all aspects, from general security concepts to technical requirements to secure development life cycle requirements. To be precise, four groups are as follows:

- General concepts
    - ∗ IEC/TS 62443-1-1 defines general terminology used in these series and puts focus on seven foundation requirements;
    - ∗ IEC/TS 62443-1-2 describes the terms and acronyms used in IEC 62443 standards.
- Policies and procedures
    - ∗ IEC 62443-2-1 presents guidance on how to develop a security program;
    - ∗ IEC/IS 62443-2-2 presents a framework and methodology for evaluation of the protection of IACS systems;
    - ∗ IEC/TR 62443-2-3 presents patch management in IACS systems;
    - ∗ IEC 62443-2-4 presents security requirements for IACS service providers that they can offer to the asset owners in the integration and maintenance phases of project delivery.
- System security
    - ∗ IEC/TR 62443-3-1 describes assessments of different cybersecurity tools, techniques, and mitigation measures that can be applied to IACS environments;
    - ∗ IEC 62443-3-2 describes requirements for risk assessment for splitting IACS into zones;

  - ∗ IEC 62443-3-3 describes control system requirements related to the seven requirements defined in IEC/TS 62443-1-1.

- Component security
  - ∗ IEC/TR 62443-4-1 presents process requirements for establishing a secure development life cycle of IACS products;
  - ∗ IEC/TR 62443-4-2 presents security requirements for different components such as networks, software applications, and embedded devices.

While all parts of these series are relevant, *IEC 62443-3-3:2013 System security requirements and security levels* standard has become the most utilized standard [181]. It defines four security levels that provide proper granulation of all security requirements, covering everything from protection from coincidental violations to intentional violations using sophisticated approaches. Besides description, requirements have a rationale and supplemental guidance section to describe the intentions more closely. In our analysis, this standard was selected since it represents the system-level standards that cover all relevant security aspects of the system. Also, this type of standard can add diversity to the overall results.

3.1.1.2 ISO/IEC 27001 and 27002

The *ISO/IEC 27001:2013; Information technology – Security techniques – Information security management systems – Requirements* is published by ISO together with IEC, and it represents the leading international information security standard. It provides a framework for systematical information protection by adopting an Information Security Management System (ISMS). ISMS represents a set of rules that must be defined and followed in the form of policies and processes. It involves identifying stakeholders and their expectations and risks, defining and implementing security controls that mitigate these risks, and continuously measuring and improving processes. The goal of ISO

27001 is to protect all three parts of the CIA triad. This can be done by conducting risk assessments and implementing mitigations. The standard consists of two parts:

- Part 1 — 11 clauses that introduce the standard terms and definitions, as well as the requirements that have to be satisfied if the company wants to be certified;
- Part 2 — Annex A only states 114 control objectives and assigned controls.

ISO 27001 only states what needs to be implemented, not how to do it. Its supplementary standard, ISO 27002, provides guidance on how each security control listed in Annex A of ISO 27001 works, its objective, and how to implement it. The complete title of the ISO/IEC 27002 standard is ISO/IEC 27002:2013; Information security, cybersecurity and privacy protection - Information security controls. It only provides a specific aspect of an ISMS, and organizations cannot certify against this standard, unlike ISO 27001. ISO 27000 family of standards consists of over 40 standards. Besides ISO 27001 and ISO 27002, the following standards are used frequently:

- ISO/IEC 27005 — defines guidelines for information security risk management;
- ISO/IEC 27017 — defines guidelines for information security in cloud environments;
- ISO/IEC 27018 — defines guidelines for protecting privacy in cloud environments.

These two standards were selected as the representatives of general-purpose security standards that have the requirements that can be applied to different sectors. They often go together with additional security standards more specific to the systems in use.

3.1.1.3 NIST SP 800-53

NIST 800-53 is a security compliance guideline created by the United States Department of Commerce and the National Institute of Standards and Technology. The fifth revision is entitled *Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*. Since it is a technology-neutral guideline, various sectors can adopt it. It is mandatory for all United States federal information systems, organizations, and agencies except those related to national security. The organizations that work with the federal government are also required to comply with this guideline. In North America, NIST SP 800-53 is widely used in the private sector. It provides guidance for all types of information systems. These systems include:

- Healthcare systems;
- Cloud computing systems;
- Mobile systems;
- Internet of Things systems;
- Industrial control systems and networks.

NIST 800-53 consists of countermeasures, techniques, and processes to respond to security and privacy risks. It is designed to provide guidance to organizations in identifying a set of security and privacy controls that are needed to manage risks and primarily satisfy requirements defined in the Federal Information Security Modernization Act (FISMA) [182], the Privacy Act of 1974 [183], and Federal Information Processing Standards [184].

NIST SP 800-53 undergoes regular revisions to be up to date with emerging security threats. Each control that is described contains base control and control enhancements. Each base control has a discussion section that gives more details about the control. Control enhancements are used where there is an increased risk of system exploitation.

A prerequisite for control enhancement implementation is successfully implemented base control. For example, in the *Identification and Authentication* family of controls, base control *IA-2* covers the identification and authentication of organizational users. A series of connected enhanced controls provide more specific guidance, such as multi-factor authentication, single sign-on, and the distinction of privileged and non-privileged account authentication.

This publication is selected as a top guideline representative according to Table 3.1. Even if initially aimed at systems that reside in the US, it is well recognized and applied worldwide.

3.1.1.4 NERC CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection is a NERC movement that provides a suite of regulations that define how the bulk electric systems (BES) prepare for cyber and physical threats that can affect the system's reliability. BES includes transmission elements that operate at 100 kV or higher voltages and real power and reactive power resources connected at 100 kV or higher [185].

NERC is subject to oversight by the United States Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada [57]. NERC requires all North American bulk power system owners, operators, and users to comply with these regulations. The unique NERC program tracks and assesses an organization's compliance. NERC event defines monetary and non-monetary penalties for non-compliance [186]. Due to rigorous requirements, many countries outside of North America require compliance or partial compliance with NERC CIP to uplift their security. Currently, there are twelve publications, with six more that are subject to future enforcement. The requirements are focused on performance, risk management, and entity capabilities. Each requirement has information about applicable systems to define further the scope of systems and measures section that provides examples of evidence to demonstrate the implementation. They cover different areas of critical infrastructure systems such as:

- asset identification;
- the Electronic Security Perimeter (ESP);
- management of system security;
- sabotage reporting;
- physical security of cyber assets.

NERC CIP was selected as the publication with the most occurrences during the literature review. It has requirements that can be applied to other sectors. Also, it represents the regulatory type of publication that gives diversity to our analysis.

3.1.1.5 Excluded Publications

IEC 62351 is the current standard for security in energy management systems. Its primary focus is on securing data communication and processing through confidentiality, data integrity, authentication, and non-repudiation [187]. The requirements are quite technical and can be considered highly specific since they include security technologies for specific communication protocols. That violates our eligibility criteria, and hence even though this standard has a high occurrence number, it was excluded from further analysis.

The Health Insurance Portability and Accountability Act (HIPAA) was created by the United States Department of Health and Human Services' Office for Civil Rights [188]. It was created to modernize and protect healthcare information and Personally Identifiable Information maintained by the healthcare and healthcare insurance industries. It consists of different rulesets covering privacy, security, and reaction to breaches. Even though technology-neutral, this regulatory publication is excluded from the final set for further analysis since it is region-specific, and one such representative (NERC CIP) was already included.

The National Institute of Standards and Technology Internal or Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cybersecurity represents the three-volume framework that can be used to develop cybersecurity strategies that apply to Smart Grid [189]. It is considered to be a de facto standard for Smart Grid. This standard was excluded from the initial analysis since it is oriented towards one domain, but it was used as a control standard for model validation in Chapter 4. NIST SP 800-82 specifies guidance on improving the security in ICS, DCS, SCADA systems, and PLCs [190]. The publication gives a summary of typical implementation architectures with associated risks, vulnerabilities, and mitigations to these systems. This standard includes recommendations from the IEC 62443 set of standards and NIST SP 800-53. Since they were included in the analysis, this standard was omitted.

IEC 61850 is the international standard that defines communication protocols used among different equipment located in a substation, such as different protection, control, and measurement equipment [191]. As with IEC 62351, this standard was excluded from further analysis due to a violation of our eligibility criteria in terms of specific levels of details it provides.

The Payment Card Industry Data Security Standard (PCI DSS) that describes requirements for companies that process, store, or transmit credit card information [139], Chinese GB/T 22239 that proposes general security requirements, and DHS Catalog that provides practices for various ICS [192] had low occurrence numbers to be further included in the analysis. As we mentioned previously, the occurrence numbers in our eligibility criteria provide information about the usage frequency and applicability of the standard among different sectors. The numbers indicate that the direct applicability of these standards is lower among sectors. Their structure might introduce noise into our model, and hence we marked them as less relevant for our analysis.

The final set of publications consisted of one system security standard, one general security information standard, one globally recognized guideline, and one geographically specific regulation. This set gave us enough diversity to cover different aspects of security requirements and detect patterns that repeat. The excluded publications were too domain-specific with a high level of details that would not benefit our classification, or they reference selected publications to some extent. Most of the requirements from excluded publications would be classified into only a few security control categories from the selected publications, and we would not gain much on the similarity note.

3.2 Security Controls Classification

As the next step, the defined set of publications underwent an in-depth analysis of each security requirement. This was done to find similarities that could give us building elements of the model. Simultaneous comparison of security requirements one by one from four different publications can be quite challenging and time-consuming. For example, if we would only compare ISO/IEC 27001 against NIST SP 800-53 or NIST SP 800-53 against ISO/IEC 27001 and tried to directly map one security control onto a similar one from the other publication, we would have some controls that do not fully satisfy the intent of the controls defined in other publication [193]. If we followed this approach and repeated it for more than two publications, the results would be even more inconsistent. With a more significant number of publications, this does not scale well. With the assumption that the requirements from different publications are similar by the intents they define, compliance with only one of them would result in the equivalent security posture no matter which security standard we choose to certify against.

One solution for this problem is to define a common view through which all security requirements can be analyzed. One approach is provided by the United States Department of Homeland Security. They issued a control system security report that classifies security controls that security requirements describe into roughly two categories [194, 192]:

- Organizational sub controls — cover physical and cyber organizational management controls such as security policies and personnel security;
- Operational sub controls — cover controls such as configuration management and service acquisition that allow the system to operate securely.

Another approach is provided by the NIST Cybersecurity Framework (CSF), as explained in Section 2.1. CSF sees each security requirement through one of five functions:

- identify — covers activities that will help an organization to understand how to manage security risks regarding all assets;
- protect — covers implementation of different measures to ensure delivery of critical services;
- detect — covers activities that will detect security events;
- respond — covers all activities that are necessary to respond to detected security incidents;
- recover — covers activities necessary to restore any capability or service affected by a security incident.

The security requirements are not grouped directly to the functions but over cybersecurity categories. When we look at the selected publications, the CSF category is a synonym for a domain, dimension, or area of knowledge that is used in this thesis interchangeably. The categories consist of security requirements that are similar in terms of what aspect of the assets should be protected when security control is implemented. CSF has the flexibility to expand the number of categories above the existing 23. The categories can have subcategories to determine requirements further. Classifying requirements deny flexibility for more fine-grained grouping. As we pointed out in [45], there are several examples of why this can be considered a limitation. CSF category *supply chain risk management* is assigned to function *identify*. If we analyze NIST 800-53, it has the domain with the same name, but the requirements in that domain can be assigned differently to functions, e.g., the requirement *SR-10 Inspection of systems or components* can be assigned to function *detect*, *SR-2 Supply chain risk management plan* to *identify*, or the requirement *SR-9 Tamper resistance and detection* to *protect*. Further, some requirements can be assigned to domains that do not exist in CSF. For instance, in NIST 800-53 *CA-2 Control assessments* and ISO/IEC 27001 *9.1 Monitoring, measurement, analysis, and evaluation* can be assigned to *detect* function, and ISO/IEC 27001 *9.2 Internal audit* and NERC CIP *014-2 R2* to *identify* the function, and all of them can be related to compliance capabilities. Also, CSF, in some cases, introduces ambiguity in its classification. For example, *ID.RA-1* is grouped under *identify* function, but *DE.CM-8* is grouped under *detect* function, but both activities involve the identification of vulnerabilities. The functions can be seen as a good feature but not as primary since standards define requirements that cover the whole lifecycle of the systems, from policies and procedures to design and implementation, to decommission. Focusing only on the domains that have the majority of the requirements seen as protective and ignoring the ones marked with detect function may introduce significant gaps in the security posture of an organization or system.

If we look at the selected publications, requirements are naturally grouped into the domains as the top-level hierarchy. More approaches define different domains for security requirements classification. Different authors [130, 192, 195, 196, 197] define 26, 18, 18, 17, and 10 domains, respectively, as presented in Table 3.2.

CSET	DHS Catalog	Sabillon et al.	CMMC	Carias et al.
Access Control	Organizational Security	Nation States	Access Control	Asset Management
Account Management	Personnel Security	Government and Strategy	Asset Management	Business Continuity Management
Audit and Accountability	Physical and Environmental Security	Legal and Compliance	Audit and Accountability	Detection Processes and Continuous Monitoring
Communication Protection	System and Services Acquisition	Cyber Assets	Awareness and Training	Governance
Configuration Management	Configuration Management	Cyber Risks	Configuration Management	Incident Analysis
Continuity	Strategic Planning	Frameworks and Regulations	Identification and Authentication	Information Security
Environmental Security	System and Communication Protection	Architecture and Networks	Incident Response	Information Sharing and Communication
Incident Response	Information and Document Management	Information, Systems and Applications	Maintenance	Risk Management
Information Protection	System Development and Maintenance	Vulnerability Identification	Media Protection	Security Awareness and Training
Information and Document Management	Security Awareness and Training	Threat Intelligence	Personnel Security	Threat and Vulnerability Management
Maintenance	Incident Response	Incident Management	Physical Protection	
Monitoring and Malware	Media Protection	Digital Forensics	Recovery	
Organizational	System and Information Integrity	Awareness Education	Risk Management	

Table 3.2 continued from previous page

CSET	DHS Catalog	Sabillon et al.	CMMC	Carias et al.
Personnel	Access Control	Cyber Assurance	Security Assessment	
Physical Security	Audit and Accountability	Active Cyber Defense	Situational Awareness	
Plans	Monitoring and Reviewing Control System Security Policy	Evolving Technologies	System and Communications Protection	
Policies	Risk Management and Assessment	Disaster Recovery	System and Information Integrity	
Policies and Procedures General	Security Program Management	Personnel		
Portable/Mobile/ Wireless				
Procedures				
Remote Access Control				
Risk Management and Assessment				
System and Services Acquisition				
System Integrity				
System Protection				
Training				

Table 3.2: List of domains by different authors

Our selected publications, IEC 62443 3-3, ISO/IEC 27001, NIST800-53, and NERC CIP, define another 7, 14, 20, and 12, respectively, as presented in Table 3.3.

CSF	IEC 62443 3-3	ISO 27001/27002	NIST 800-53	NERC CIP
Asset Management	Identification and Authentication Control	Information Security Policies	Access Control	BES Cyber System Categorization
Business Environment	Use Control	Organization of Information Security	Awareness and Training	Security Management Controls
Governance	System Integrity	Human Resource Security	Audit and Accountability	Personnel and Training
Risk Assessment	Data Confidentiality	Asset Management	Assessment, Authorization, and Monitoring	Electronic Security Perimeter(s)
Risk Management Strategy	Restricted Data Flow	Access Control	Configuration Management	Physical Security of BES Cyber Systems
Supply Chain Risk Management	Timely Response to Events	Cryptography	Contingency Planning	System Security Management
Identity Management and Access Control	Resource Availability	Physical and Environmental Security	Identification and Authentication	Incident Reporting and Response Planning
Awareness and Training		Operations Security	Incident Response	Recovery Plans for BES Cyber Systems
Data Security		Communications Security	Maintenance	Configuration Change Management and Vulnerability Assessments
Information Protection Processes and Procedures		System Acquisition, Development and Maintenance	Media Protection	Information Protection

Table 3.3 continued from previous page

CSF	IEC 62443 3-3	ISO 27001/27002	NIST 800-53	NERC CIP
Maintenance		Supplier Relationships	Physical and Environmental Protection	Supply Chain Risk Management
Protective Technology		Information Security Incident Management	Planning	Physical Security
Anomalies and Events		Information Security Aspects of Business Continuity Management	Program Management	
Security Continuous Monitoring		Compliance	Personnel Security	
Detection Processes			PII Processing and Transparency	
Response Planning			Risk Assessment	
Communications			System and Services Acquisition	
Analysis			System and Communications Protection	
Mitigation			System and Information Integrity	
Improvements (Respond)			Supply Chain Risk Management	
Recovery Planning				
Improvements (Recover)				
Communications				

Table 3.3: List of domains in selected publications

Given the limitations in existing approaches previously mentioned, we concluded that using category-oriented requirements grouping will provide a more fine-grained classification. Also, the initial list of the domains, for example, in CSF, needed to be redefined to cover more aspects that security controls might enable. We analyzed requirements from selected publications, extracted keywords that are potential candidates for the domains, and cross-compared domains from Tables 3.2 and 3.3 to define a new set. As described in [45], the result contains 24 domains presented in Table 3.4.

Domain	Objective	Score
Business Continuity and Disaster Recovery	Define and practice backup and recovery procedures to recuperate in case of an incident.	4
Data Handling	Define data classification and analyze usage in the organization.	4
Identity Management and Access Control	Apply security controls for the identification, authentication, and access to the systems by complying with principles of least privilege and separation of duties.	4
Network Security	Apply security controls to protect network architecture and maintain defense-in-depth.	4
Secure Design, Implementation, and Validation	Practice secure design analysis, implementation, and validation to ensure the developed system is secure.	4
Security Monitoring	Employ security controls for the collection of security-related information.	4
Asset Management	Manage all technology assets throughout the whole lifecycle from the procurement until disposal.	3
Change Management	Employ and follow procedures to ensure only authorized changes can occur.	3
Compliance Capability	Employ regular assessments and internal audits to maintain targeted compliance.	3
Configuration Management	Establish and maintain consistency of the system's configuration within its lifecycle.	3
Endpoint Security	Apply security controls to protect endpoint devices and maintain defense-in-depth.	3
Incident Response	Define and maintain procedures for incident response.	3
Personnel Security	Practice background and psychological checks during the hiring process for a specific role.	3
Physical and Environmental Security	Apply physical and environmental controls to ensure that technology assets cannot be compromised.	3
Risk Management and Assessment	Detect, analyze, and assess all security risks affecting human or technology assets.	3

Table 3.4 continued from previous page

Domain	Objective	Score
Security Awareness and Training	Employ continuous personnel development by raising security awareness and culture within the organization and offering specialized training.	3
Security Operations	Employ mechanisms to implement operational security controls.	3
Security and Privacy Governance	Define an organization's systematic program to address security.	3
System, Data, and Communication Protection	Utilize well-known industry-recognized controls for securing data in transit and at rest.	3
System and Services Acquisition	Perform all needed examinations to ensure that all acquired systems and services comply with the organization's policies and do not introduce additional risk.	3
Vulnerability and Patch Management	Establish controls and processes to help identify vulnerabilities within the infrastructure and provide appropriate protection against threats that could adversely affect the system's security.	3
Maintenance	Properly maintain all technology assets by applying vendor recommended configuration and industry best practices.	2
Portable Device Security	Apply security controls to protect portable devices and maintain defense-in-depth.	2
Resource Management	Properly allocate and efficiently manage human and technology resources required for each new or existing project.	2

Table 3.4: List of defined domains with scores

We grouped all requirements from the selected publications to their respective domains in the following step. Similar requirements were also subjectively grouped into clusters inside a domain during this step. Throughout this process, we noticed that NIST SP 800-53 has a significant number of requirement enhancements that could be classified into different domains and not necessarily into the original domain where, by guideline definition, all requirements reside. Some of the examples were noted in our previous work [45]: *IR-4 Incident Handling (4) Information Correlation*, *SI-4 System Monitoring (23) Correlate Monitoring Information*, and *AU-6 Audit Record Review, Analysis, and Reporting (3) Correlate Audit Record Repositories* can be grouped even though they originally belong to other domains. Similarly, IEC 62443-3-3:2013 has requirement enhancements that can be interpreted as the natural enhancements of the base requirement that can go together, unlike NIST SP 800-53. Also, requirements and requirement enhancements are bounded by so-called security levels. The base requirement is mandatory to be satisfied to be compliant with any security level above one. The difference in the certification process makes the requirement enhancements that are usually defined for security levels two and above. Looking only at these two publications, we concluded that for the requirement classification, requirement enhancements have to be considered as the first order requirements, i.e., for most cases, equally important as the base requirements, with a few additions being that they have ancestors, and they might be more demanding to achieve.

As already mentioned, CSF security functions are a nice feature to have to balance between different security controls that focus on different phases of an organization or system lifecycle. That is why we labeled each requirement with one of the five functions. This gives more mobility for security experts to reprioritize decisions in case of additional constraints such as limited budget and to focus more on security events prevention (identify, protect, detect) or on what to do after a security incident occurs (respond and recover). This vector is not included in the prioritization criteria described in Section 3.5 because the degree of dependency on technology, people, and processes varies in terms of devices, networks, applications, data, and users, as stated by Yu [124].

We quantified domains to provide additional information for the prioritization criteria described in Section 3.5. The prioritization criteria will allow us to sort non-compliant requirements by importance for implementation, similar to some of the tools described in Section 2.2. Unlike these tools that lack a clear explanation of the methodology used, how many experts were interviewed, and what professional background qualifies them to construct the scoring system, we used a quantitative approach based on the information extracted from publications. These scores will play a minor role in overall priority score calculation since we will focus on more critical elements in further sections, but they can bear enough value to present nuances between the requirements. Due to their minor role in the overall score, the threshold values were roughly defined.

As defined in [45], the following rules were used to calculate scores in Table 3.4:

- All 24 domains have an initial score of two on a scale of 1–2 based on the occurrence during the systematic literature review and domain definition. The scale has two values to support the domain list extension in the future. The expectations are that updated versions of existing standards and new standards will arise, and they will have new requirements specific to the new technologies such as cloud security, edge security, or the Internet of Things. These newly introduced domains will get an initial score of one on a scale of 1–2 due to their novelty and domain immaturity;

- If the domain had over 50 requirements in all four publications combined, it gets an additional one point because of the assumption that the domain is versatile and can express its requirements in a fine-grained manner. This limits an arbitrary interpretation of the requirement depending on the organization. The threshold number is high since NIST SP 800-53 has many requirement enhancements, and we interpret them as the first order requirements;

- If three or more security requirements from the same domain in three distinct publications are labeled as similar, the domain gets an additional one point because of the assumption that the majority of analyzed publications recognize the importance of that control. Similar requirements were subjectively grouped into subcategories inside a domain by the intention requirements try to achieve. For example, the domain *Identity Management and Access Control* can have the subcategory *Access Control Management* where we can put IEC 62443-3-3:2013 *SR 2.1 Authorization enforcement*, ISO 27001 Appendix A *9.1.1 Access control policy*, NIST SP 800-53 *AC-1 Access control policy and procedures*, and NERC CIP *004-6 R4 Access Management program.* That is sufficient for the domain to gain one additional point. On the other hand, the domain *Endpoint Security* can have a subcategory *Mobile Code* where we can put IEC 62443-3-3:2013 *SR 2.4 Mobile code* and NIST SP 800-53 *SC-18 Mobile code* that is insufficient for the domain to improve score based on this subcategory.

Looking at Table 3.4, we can conclude that all publications emphasize providing business continuity, securing data and users, and thinking about security from the beginning of the software development lifecycle. On the other hand, there are fewer requirements when we approach the end of the project delivery and enter the maintenance phase. Also, these publications focus more on traditional systems with less portable devices as the primary source of information. With the expansion of IoT and edge computing, this will undoubtedly change. Resource management is an important category but often overlooked, and this analysis proved this once again.

3.3 Assurance Model

The model has to be extended to gain all the required information to address all research questions. We already stated that publications have base requirements that are usually obligatory to be satisfied and serve as a mandatory prerequisite for requirement enhancements. Also, we noted that some requirements might be harder to achieve than others. Therefore, the requirements have to be observed with an additional vector in mind. This vector we call the assurance level inside a domain. The assurance levels use a qualitative approach to express how sophisticated security controls are used to satisfy security requirements. Each advanced requirement that is successfully satisfied requires more sophisticated means to make an exploit. For example, all base requirements regarding user authentication assume at least password-based authentication. The advanced controls involve implementing multi-factor authentication, a more sophisticated control that is harder to exploit. This information can be used to track the maturity of the security posture. Different maturity levels influential to our work are presented in Section 2.3 [142, 143, 141].

Our proposed assurance level model is two-dimensional. The first dimension reflects the essence level and the second the maturity of implementation, i.e., the implementation level. The essence level represents the priority of the implementation of the requirements. In previous work [45], we proposed numerical nomenclature for this:

- *3* – the requirement is mandatory and must be satisfied for the final solution to be acceptable;
- *2* – the requirement has a high priority and should be included, if possible, within the delivery time frame with a lower priority;
- *1* – the requirement is desirable, but the priority is the lowest;
- *0* – the requirement is not obligatory to be addressed.

The numerical scale is descending to accommodate the prioritization criteria described in Section 3.5 of this chapter. The values can be assigned driven by different goals. For example, if the goal for the organization is to prepare for IEC 62443-3-3:2013 security level 1 certification, only requirement *SR 3.8 Session integrity* would be assigned the essence level 3, and all SR 3.8 requirement enhancements would be assigned the essence level 0, 1, or 2 since they are not necessary for the goal to be accomplished. Also, if the system does not allow wireless access to portable devices, in NIST SP 800-53, *AC-18 Wireless Access enhancement 5 (Antennas and transmission power levels)* be assigned level 0.

The implementation level is a qualitative measure representing the overall maturity of security control implementation defined in the requirement. The proposed implementation levels are guided by the scale defined in CMMI [141]. Even though CMMI levels are process-oriented, they can be applied to all three pillars of the PPT framework since all of them can implement controls described in the requirements as stated in NIST SP 800-53 [118]. One of the main drivers for our research is the needs of product providers, and since the CMMI model contributes to the performance of the product providers [198], the proposed implementation levels reshaped the existing scale to fit our needs. The implementation levels are as follows [45]:

- *Not Applicable* — security controls are not implemented since the security requirement is not applicable to a specific security context where the organization or system operate;

- *None* — security controls are not implemented;

- *Initial* — security controls introduced through requirement are implemented *ad hoc* with a low level of maturity and traceability;

- *Managed* — security controls are implemented and documented to comply with the requirement as a bare minimum; there is no clear plan for further improvement in case of an organizational or system change; Requirement enhancements, if any, are not implemented;

- *Defined* — security controls are improved compared to the previous level by implementing requirement enhancements if they exist; Process and technology invariants are defined where possible;
- *Quantitatively Managed* — security controls are quantitatively analyzed to identify deviations and implement further improvements;
- *Optimizing* — security controls are continually improved through innovative technological improvements and lessons learned.

The implementation levels can express the organization's overall maturity against the selected standards. For example, as we pointed out in [45], the report can be generated based on the implementation levels assigned to requirements to provide statistical information about the percentage in which domain requirements' implementation achieved a *Defined* or *Quantitatively Managed* level of maturity.

Payne [199] states that a straightforward security metrics program must be defined for goals and objectives. When it comes to standard alignment, security assessment, and certification preparedness, this is related to the assurance levels we defined. The goal definition by NIST SP 800-53 is presented in Section 2.1. The actors who define goals only express the main intentions for achieving the goal but not the means to accomplish it. The involvement of other actors that will delegate, track, and implement security controls is necessary to achieve those goals. Since achieving goals is something that takes time, tracking the whole process is essential. Key performance indicators (KPIs) should be defined to measure the effectiveness of the implementation. KPIs represent a measure of performance over time for a specific objective. They provide targets and milestones to which teams aspire and give insights to the upper management to make better decisions. KPIs can be necessary to keep the teams involved in requirements implementation aligned with the organization's goals, hold them accountable, and make necessary adjustments. One example of the security goal would be that the system must be aligned with the IEC 62443-3-3:2013 set of SAL level 3 requirements. This means that 90 out of 100 requirements and requirement enhancements must be implemented. This goal can be interpreted as a standalone project involving different people in the organization and making them cooperate. With the assumption that the organization follows agile development practices [200] to track progress, one KPI can be the weekly or monthly burndown trend of fulfilled requirements per seven domains. Security goals and KPIs are elements defined and interpreted by human actors. Regarding the model we develop, KPIs are not the essential extension but natural addition that goes well with another extension element described in the next section — actors.

3.4 Actors

If we wanted to extract our security requirements driven by the business needs, we have different techniques that have the capability to do that, as described in Section 2.1. Since our focus is on security standards and guidelines, the elicitation process is more straightforward. Standards and guidelines have well-defined requirements that are proven to work in practice. In the previous section, we defined an assurance model that can align with business needs. The model we want to create is primarily aimed at security practitioners in companies who should be able to track the implementation process. In this process, naturally, other relevant entities from the organizational structure must be involved since the organization is a complex pattern of communication and relationships among human beings [201]. Hence, the question *what are the requirements that need to be addressed?* is extended with *and who will implement them?* This section discusses the relationships among the social actors involved in the implementation process.

Boehm states that an error not identified and corrected in the requirements phase can cost a lot more to correct in subsequent phases [202]. Therefore, security requirements should not be an afterthought. Ideally, the organization would have implemented the information security management system (ISMS) and security development lifecycle (SDL) on a system level such as one designed by Microsoft [203] or IEC 62443-4-1 [204]. However, in practice, this is not always the case. A survey done by Errata Security shows that, out of 46 organizations, 30% use a formal SDL, while 43% do not use any SDL methodology [205]. Mohamed et al. [206] conducted a study that shows that employees are getting aware of how much security is essential, but SDL practices are still in the early stages, and there is a lack of security-related training. On the other hand, Said et al. [207] showed that top-level management and organizational structure support make the most significant impact on information security knowledge management implementation. These results influence the definition of the social component of our model.

The idea for modeling social actors can be used from the $i*$ (iStar) framework, a basis for several goal-oriented models described in Section 2.1 [208]. The $i*$ framework enables the construction of a model that represents an organization or socio-technical system. It identifies stakeholders and models them as actors who depend on each other to achieve goals. It requires creating an actor diagram, a graph whose nodes represent actors while edges represent dependencies among them. Since our model aims to track requirement implementation to lift security posture to a more mature level or prepare a system or organization for certification against an arbitrary standard, the $i*$ framework has conceptual elements that we need. The framework defines actors as active entities collaborating with other actors to achieve their goals by exercising their know-how [208]. These actors can be categorized into two types [209]:

- *Role* — abstract characterization of the behavior of a social actor within a domain, e.g., security advisor or software engineer;

- *Agent* — concrete actor, e.g., person or organization.

Actors are connected with actor links:

- *plays* — links an agent to a role, e.g., a person plays the role of security advisor;
- *is-part-of*— links actors of the same type, e.g., the software engineer is part of one team in the organization;
- *is-a* — specialization construct where one actor of any type specializes another actor of the same type, e.g., programmer role has junior, intermediate, and senior roles;

Actors define their intentional elements:

- *Goal* — represents a state that the actor wants to achieve;
- *Soft goal* — represents an ambiguously defined goal without clear criteria for its fulfillment;
- *Resource* — represents an entity that is produced or provided by the actor;
- *Task* — represents an activity defined by some procedure that explains how something can be done.

Intentional elements are then connected using intentional element links to express intentions in a structured way:

- *Means-end* — offers alternative approaches to achieve goals;
- *Contribution* — expresses how intentional elements contribute to the satisfaction of soft goals;
- *Decomposition* — enables decomposition of complex elements into smaller ones of the same type.

Besides actor links, actors are connected through dependencies. A dependency represents a link between two actors where one actor (the depender) depends on another (the dependee) to fulfill a goal or soft goal, perform a task, or deliver a resource (the dependum).

One of the problems that the *i** has is scalability [210]. Scalability issues can be mitigated by using model views that depict only essential parts of the model to the problem being solved, i.e., strategic dependency. Strategic dependency is a network of dependency relationships that show who depends on whom for what. Therefore, we did not want to include every element that the *i** defines, only those necessary to connect between social actor entities. The adjusted elements to fit our model are presented in Table 3.5.

i* element	**Our model element**
Actor (depender and dependee)	Actor involved in the implementation
Role	Role in which actor acts
Resource (dependum)	Security control that is to be implemented to satisfy the security requirement
Resource dependency	Relationship between social actors (depender and dependee) and security requirements through security control
Goal	Goal to be achieved

Table 3.5: Mapping of the i* elements to our model

We can track all dependencies between actors and security controls that need to be implemented to satisfy security requirements using these elements. For example, as part of achieving compliance with an arbitrary standard (goal), if the requirement is to define Security Information and Event Management (SIEM) rules for security monitoring of a system that should be added as a part of the offering (dependum), the security advisor (depender) needs to report the progress to the upper management in the form of the number of rules that will be part of the portfolio or the percent of the false positives that the ruleset creates (KPI). The security advisor depends on the security engineer (dependee) to design and implement the rules, and the security engineer (depender) depends on the infrastructure engineer (dependee) that needs to set up the system for testing. This forms a dependency graph of all involved social actors where on each level, we can have more than one actor depending on the others. Complex graphs signal that compliance with a particular requirement can take more time, making them a priority for the analysis. Therefore, it is vital to get familiar with the organizational structure and identify all actors to track the requirement implementation dependency graph precisely.

3.5 Prioritization Criteria

In previous sections, we presented a couple of elements that are important to analyze in more detail to extract relevant information that can help the organization improve its security posture. Also, these elements are closely related to security requirements that have to be satisfied. Now, we can combine this knowledge to make a distinction between the requirements when preparing for their implementation. To do that, we must form prioritization criteria that will help us with the decision in which order to proceed with the implementation.

Section 2.5, described existing approaches for defining prioritization criteria. They all have their advantages and limitations. We must take into consideration that the same requirements can have different priorities in different organizations. For example, suppose an organization or its systems operate in an area where the likelihood of earthquakes, tornadoes, or tsunamis is increased. In that case, data and systems recovery requirements will have a bigger priority for these organizations than others residing in geographically safer areas. Also, organizations that have an obligation to comply with a broader number of standards, guidelines, and regulations will have to work with a more significant number of requirements in total. Using some techniques described earlier that require complex calculations on a considerable amount of data is not scalable.

Further automation of the prioritization of requirement implementation can be more difficult. That is why we focused on determining the proper criteria instead of proposing a new technique for prioritization calculation. Our criteria for choosing one technique are as follows:

(1) The technique has to allow each criterion can be weighted. This is necessary to distinguish more important criteria for the overall score.

(2) The technique has to be simple enough to be used even without extensive software automation. This means that anyone from the organization involved in the security posture uplift process would easily understand and use this technique.

(3) The technique has to have wide acceptance in practice. This is evidence that it is a proven technique.

Among the existing techniques from Section 2.5, most were derived from AHP, TOPSIS, and SAW, which served as a basis. While AHP and TOPSIS satisfy criteria 1 and 3, they are slightly more complicated in terms of calculations than SAW, making them fall on criterion 2. The Simple Additive Weighting (SAW) method or weighted summing method satisfies our criteria. Nonetheless, all three techniques work with weighted criteria so that SAW can be easily substituted with another technique in future work.

Considering analysis results from previous sections, four elements of prioritization criteria are:

- Risk level score (RL)
- Essence level score (EL)
- Actor dependency graph score (ADG)
- Domain affiliation score (DA)

These elements can be used as a criterion for requirement grouping by similarity. By introducing multiple criteria, prioritization gets less prone to errors and less dependent on the decision-makers and security experts involved in the calculation. DA score is driven by standards, EL by the business decision on which compliance level an organization or system certifies for, and ADG by organizational structure. The room for error can be inaccurate risk assessment, but the error space can be reduced by utilizing comprehensive risk, threat, and vulnerability registers.

In Section 2.4, we explained representative risk assessment approaches. These approaches are usually tailored to the organization's needs, primarily regarding possible applicable threats and vulnerabilities. We can make a coarse-grained classification based on qualitative and quantitative approaches for risk assessment. Both types have their limitations. The qualitative approaches rely on subjective data and much simplifying assumptions. The quantitative approaches use probabilistic methods where risk estimation is never complete in the mathematical sense. Nonetheless, the key element that organizations need to focus on is the definition of a security risk register. Each security risk must be identified, and the owner must be assigned.

This is usually someone from the management. By looking at the risk assessment formula 2.1, we can see a close relationship between risk and threats and vulnerabilities. The connection between them is made over assets or resources. The asset of value may have a vulnerability that the threat actor can exploit. Security controls must be implemented to secure the assets. Security controls are mechanisms that can be used to satisfy security requirements. These are necessary links that we have when assessing risks. Risk assessment is the most crucial criterion among all four since the consequences of wrong assessment can be catastrophic in terms of fines, damaged reputation, customer dissatisfaction, or even business failure.

When we have defined our criteria, now SAW steps must be followed. The SAW has the following steps:

(1) Define the criteria that will be used as a reference in decision making, namely C_i.

(2) Determine the suitability rating of each alternative on each criterion.

(3) Make a decision matrix D based on the criteria (C_i), then normalize the matrix based on the equation adjusted to the type of attribute (benefit attribute or cost attribute). The equation is as follows:

$$R_{ij} = \begin{cases} \frac{x_{ij}}{\max x_{ij}} & \text{if } j \text{ is the benefit attribute} \\ \frac{\min x_{ij}}{x_{ij}} & \text{if } j \text{ is the cost attribute} \end{cases} \tag{3.1}$$

where:

- R_{ij} is a normalized performance rating of alternatives
- x_{ij} is the attribute value of each criterion
- $max\ x_{ij}$ is the maximum value of each criterion
- $min\ x_{ij}$ is the minimum value of each criterion
- for benefits, the maximum value is the best; for costs, the minimum value is the best

(4) The final result is obtained from the ranking process, i.e., the addition of the normalized matrix multiplication with the weight vector so that the highest value is chosen as the best alternative (A_i). The preference value for each alternative (V_i) is given as:

$$V_i = \sum_{j=1}^{n} w_j R_{ij} \tag{3.2}$$

where:

- V_i is the ranking for each alternative
- w_j is the weighted value of each criterion

- R_{ij} is the normalized performance rating value

We have already defined prioritization criteria for the first step. Next, suitability ratings required by the second step are given. We already mentioned that each criterion could affect the final ranking of the requirement differently. The most impact on the ranking must have the risk assessment score, namely half of the overall score. The risk level score can be calculated for each identified risk separately, and they all can be included in the calculation of the priorities or, for simplicity, only the risk level score with the maximum value can be observed. The essence level is the second criterion that affects the overall score. Since it covers all types of publications, some of which are not mandatory to be compliant with, the weight should be smaller than for risk assessment. Actor dependency criterion depends on the organizational structure, which can be different from case to case, and domain affiliation is a criterion that should provide better granularity. This order of precedence applies if multiple requirements have the same overall score.

We will use scaled quantitative scores from Table 2.1 calculated with the formula 2.1 for the risk assessment score. This is presented in Table 3.6.

Risk Level - C_1	**Score**	**Weight**
Very High	5	50%
High	4	
Moderate	3	
Low	2	
Very Low	1	

Table 3.6: Risk Level Criterion

For the essence level, we will use the proposed nomenclature in Section 3.3. Naturally, the requirements that are not necessary are not scored. This is presented in Table 3.7.

Essence Level – C_2	**Score**	**Weight**
Mandatory	3	30%
High Priority	2	
Low Priority	1	

Table 3.7: Essence Level Criterion

For actor dependency graph complexity explained in Section 3.4, we will use scores presented in Table 3.8. There are always a minimum of two actors, one depender and one dependee. Complexity can be adjusted per actual organizational structure.

Actor Dependency Graph – C_3	**Score**	**Weight**
Extreme (10+ actors)	4	15%
High (6-10 actors)	3	
Medium (4-6 actors)	2	
Low (2-4 actors)	1	

Table 3.8: Actor Dependency Graph Criterion

For domain affiliation scores, we will use scaled scores assigned in Table 3.4 in Section 3.2. This is presented in Table 3.9.

Domain Affiliation – C_4	**Score**	**Weight**
High (score 4)	3	5%
Medium (score 3)	2	
Low (score 1-2)	1	

Table 3.9: Domain Affiliation Criterion

We will assume that four requirements from arbitrary standards will be alternatives for prioritization – A_1, A_2, A_3, and A_4. Since this is only a demonstration of how the SAW method works, we assume that the suitability ratings were already determined. Also, to demonstrate how the SAW method works, we will assume that only risk with maximum value for each alternative is used for further calculations. For our criteria, we treat every criterion but *ADG* as a benefit. The risk reduction naturally gives more benefits than it would cost in the long term. If the goal is to achieve a certain level of security defined in some arbitrary standard, the essence level can also be treated as a beneficial criterion. The domain affiliation has the lowest impact on the final score, but in the long term, compliance with the requirement from a specific domain can affect the qualitative component of the implementation levels defined in Section 3.3. Hence, we can consider domain affiliation as a beneficial criterion. The only criterion that can be considered as a cost is the actor dependency graph. The complexity that organizational structure can bring in terms of the number of employees from different teams that must be involved in implementation can negatively affect the achievement of other non-security-related goals.

Next, we have to determine the suitability rating for each requirement based on the scores defined in the first step. This is presented in Table 3.10.

Requirement	$\boldsymbol{C_1}$	$\boldsymbol{C_2}$	$\boldsymbol{C_3}$	$\boldsymbol{C_4}$
A_1	4	3	3	3
A_2	3	2	2	2
A_3	2	1	2	1
A_4	3	3	3	3

Table 3.10: Suitability Rating Matrix

Next, we have to create normalized matrix.

$$R_{11} = \frac{4}{\max\{4,3,2,3\}} = 1$$

$$R_{12} = \frac{3}{\max\{4,3,2,3\}} = 0.75$$

$$R_{13} = \frac{2}{\max\{4, 3, 2, 3\}} = 0.5$$

$$R_{14} = \frac{3}{\max\{4, 3, 2, 3\}} = 0.75$$

$$R_{21} = \frac{3}{\max\{3, 2, 1, 3\}} = 1$$

$$R_{22} = \frac{2}{\max\{3, 2, 1, 3\}} = 0.67$$

$$R_{23} = \frac{1}{\max\{3, 2, 1, 3\}} = 0.33$$

$$R_{24} = \frac{3}{\max\{3, 2, 1, 3\}} = 1$$

$$R_{31} = \frac{\min\{3, 2, 2, 3\}}{3} = 0.67$$

$$R_{32} = \frac{\min\{3, 2, 2, 3\}}{2} = 1$$

$$R_{33} = \frac{\min\{3, 2, 2, 3\}}{2} = 1$$

$$R_{34} = \frac{\min\{3, 2, 2, 3\}}{3} = 0.67$$

$$R_{41} = \frac{3}{\max\{3, 2, 1, 3\}} = 1$$

$$R_{42} = \frac{2}{\max\{3, 2, 1, 3\}} = 0.67$$

$$R_{43} = \frac{1}{\max\{3, 2, 1, 3\}} = 0.33$$

$$R_{44} = \frac{3}{\max\{3, 2, 1, 3\}} = 1$$

$$D = \begin{bmatrix} 1 & 1 & 0.67 & 1 \\ 0.75 & 0.67 & 1 & 0.67 \\ 0.5 & 0.33 & 1 & 0.33 \\ 0.75 & 1 & 0.67 & 1 \end{bmatrix}$$

In the end, rankings are calculated based on the weights previously defined in tables and the normalized matrix.

$$V_1 = 1 \times 0.5 + 1 \times 0.3 + 0.67 \times 0.15 + 1 \times 0.05 = 0.9505$$

$$V_2 = 0.75 \times 0.5 + 0.67 \times 0.3 + 1 \times 0.15 + 0.67 \times 0.05 = 0.7595$$

$$V_3 = 0.5 \times 0.5 + 0.33 \times 0.3 + 1 \times 0.15 + 0.33 \times 0.05 = 0.5155$$

$$V_4 = 0.75 \times 0.5 + 1 \times 0.3 + 0.67 \times 0.15 + 1 \times 0.05 = 0.8255$$

Table 3.11 shows the final rankings.

Requirement	**Score**	**Ranking**
A_1	0.9505	1
A_4	0.8255	2
A_2	0.7595	3
A_3	0.5155	4

Table 3.11: Final requirements priorities

Using the SAW method, requirement A_1 got the best score and, consequently, the best ranking for implementation. This would be the process for calculating ratings for all selected requirements.

3.6 Model

To create the model, we went from eliciting relevant publications to analyzing their requirements to expanding the analysis with the assurance model, social actors' aspects, and prioritization criteria. Now we have all the required elements to construct the model. For better readability, the conceptual model is presented in the form of a UML class diagram in Figures 3.2 and 3.3.

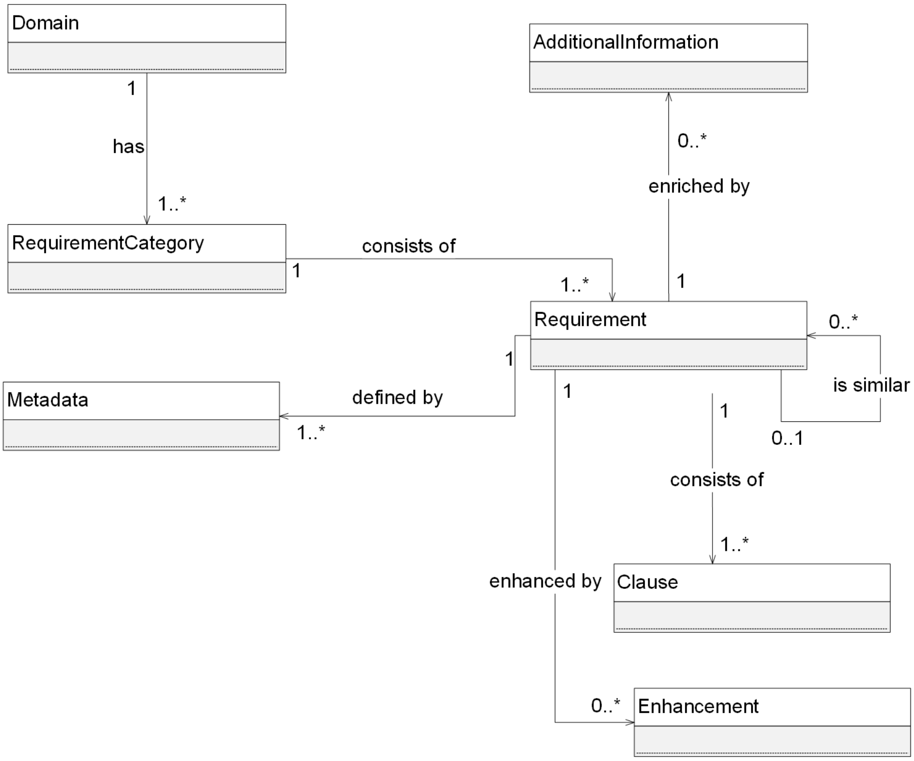


Figure 3.2: UML class diagram of the core model elements

The core model representing the requirement is straightforward to follow, as shown in Figure 3.2. Different publications define their requirements in different forms. Therefore, we first have to detect the relevant building entities of each requirement. The form which can apply to all publications is defined by analyzing the structure of the requirements defined in four selected standards. It consists of the following elements:

- *Domain* — represents a domain, category, or area of knowledge through which all requirements are interpreted. Each standard classifies the requirements into specific domains as discussed in Section 3.2; thus, it is an inevitable part of the model;
- *Requirement Category* — subcategory that can be used to further group the requirements based on similarity. This component is omitted from most of the standards. Only ISO/IEC 27002 and CSF define some granulation, while others have a flat structure inside a domain. The existence of this component is essential for fine granulation of the requirements and the basis for future classification recalibration if necessary;
- *Requirement* — the central entity that contains information about the requirement itself. It also has a recursive association that indicates the connection between similar requirements from different publications or requirement enhancements from the same publication;
- *Clause* — requirements can be flat, as in IEC 62443-3-3:2013, or can consist of multiple clauses, such as requirements defined in NIST SP 800-53 or NERC CIP. This dynamic nature of the requirement definition is covered with this component;
- *Enhancement* — often, a requirement has additional improvements that are not enough to construct an entirely new requirement. This entity can be used for extending the base requirement with controls defined in different publications that are missing in the observed ones. This can also be evidence for reaching the higher implementation levels;

- *Metadata* and *Additional Information* — keep information such as publication name, author, version, type, the rationale for implementation, supplemental guidance, links, and other attachments.

Figure 3.3 shows the model extension with elements described in this Chapter and Section 2.1.

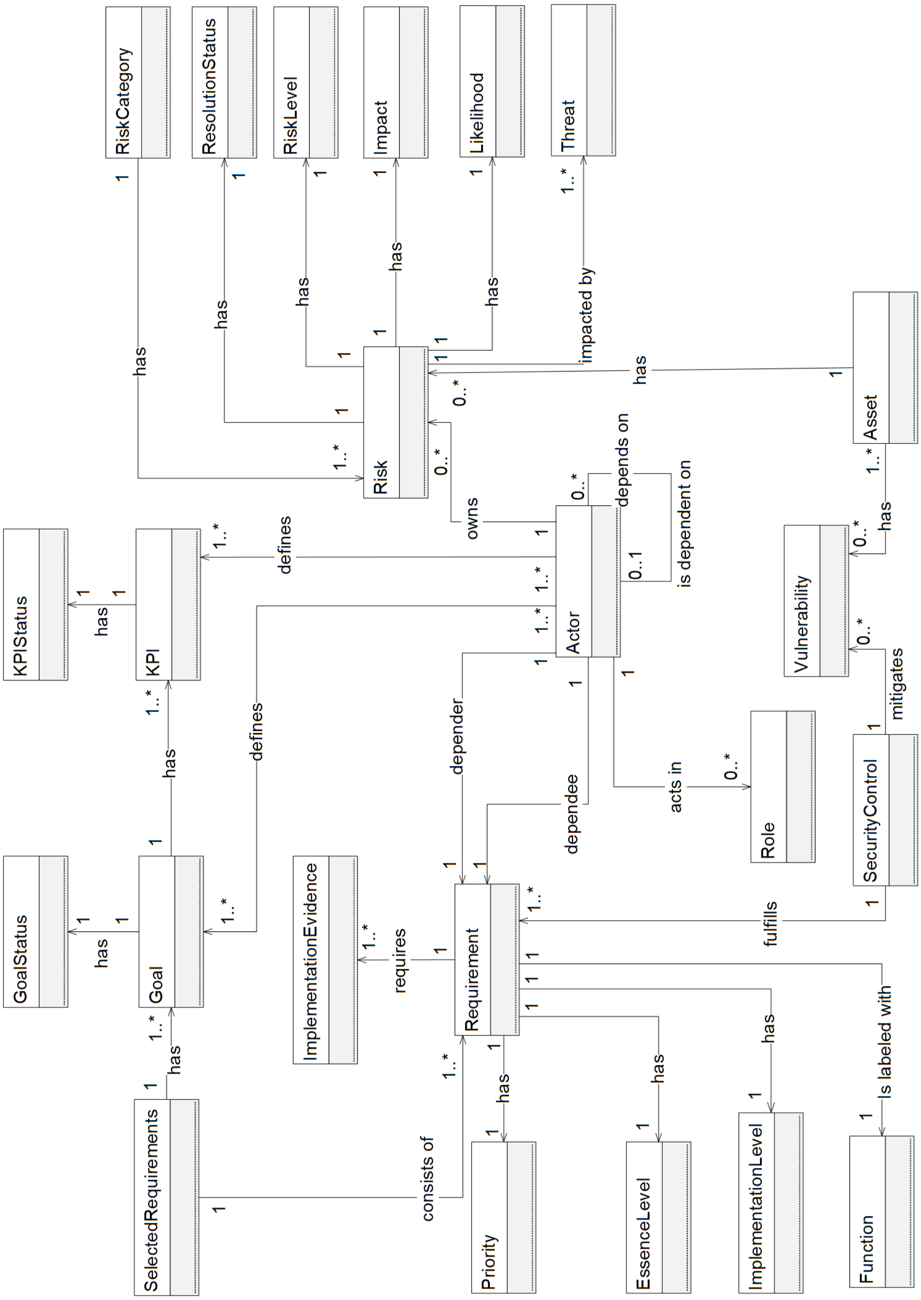


Figure 3.3: UML class diagram of the proposed model

The entities that constitute the base requirement are omitted for better readability since they can be found in Figure 3.2. The remaining parts of the model are summarized as follows:

- *Selected Requirements* — consists of the selected requirements for tracking and analysis. The requirements selection is heavily impacted by the project goals that have to be defined from the start. This is represented with *Goal(s)* and *Goal Status* entities that are tracked through *KPI(s)* that are defined by the *Actor(s)* acting in a specific *Role(s)*.

- *Risk* — represents the main component regarding prioritization criteria described in Section 3.5. This element is associated with the *Asset(s)* that can be affected by the requirement implementation. Further, risks are connected with the *Threat(s)* and their *Impact(s)* and *Likelihood*, *Risk Level*, and *Resolution Status* set after the risk analysis. Finally, every risk is owned by the *Actor*.

- *Requirement* — it is extended to give additional information essential for the implementation, such as *Essence Level* of the requirement extracted from the standard, *Implementation Level* to mark the maturity of the security control, *Implementation Evidence* to support the claims about the implementation, and *Function* (identify, protect, detect, respond, recover). Every *Requirement* has the *Priority* calculated based on the equations in Section 3.5.

- *Actor* — it is defined as a recursive association to support the creation of actors' dependency graph that can be complex.

- *Asset* — every asset can have its associated *Risk(s)* and *Vulnerabilities* that are mitigated by implementing *Security Control(s)* to satisfy *Requirement(s)*.

A few not self-explanatory connections need to be explained in more detail by looking at the model in Figures 3.2 and 3.3. Table 3.12 summarizes key dependencies.

Dependency	Explanation
Domain - Requirement Category	Domains can have multiple subcategories but at least one. Having multiple subcategories can enable more fine-grained grouping of similar requirements. Categories must be assigned to exactly one domain.
Requirement - Clause	Depending on the publication, a requirement might not have clauses. We assume that if the requirement does not have explicitly stated clauses, the base requirement consists only of one clause.
Requirement – Enhancement	We treat each requirement enhancement as a first-order requirement. Here, enhancement can be an additional phrase that is not complete to be a standalone clause, but that can, in some contexts, enrich the existing requirement as the standards evolve.
Selected Requirements – Goal	With the implementation of the selected set of requirements, multiple goals can be achieved, e.g., compliance with two standards simultaneously.
Requirement – Implementation Evidence	Each successfully implemented requirement must have evidence that can demonstrate compliance, e.g., design document, procedure, test suite, etc.
Actor – Role	The actor does not have to have an assigned role, i.e., it can be a general actor that currently does not reflect any role in the organizational structure.
Requirement – Actor	The requirement must have one directly connected depender and dependee, while the rest of the actors can form a graph. It is easier to track the main dependencies between the requirement implementation and the chain of responsibility.
Risk – Threat	Each risk is impacted by at least one threat.
Requirement – Asset	Requirements and assets are indirectly connected with security controls. Security controls fulfill security requirements and eliminate or reduce vulnerabilities to assets.

Table 3.12: Explanation of connections

This extended model has all the necessary elements to collect relevant information while tracking security requirements implementation. It is a basis for a framework that will validate the model. In the next chapter, we present the final phase of the methodology — the model validation.

Chapter 4

Model Validation

In the final step of our methodology, the model validation is performed. First, we construct a framework that uses the proposed model to confirm the practical applicability of the model and to identify its advantages and eventual limitations. This allows us to execute coordinated activities that touch upon every model element. For each activity, we present security concepts and explain their contribution to the framework in Section 4.1. In Section 4.2, we illustrate a case study for framework usage. Finally, Section 4.3 discusses the advantages and limitations of the presented work.

4.1 Security Assessment Framework for Critical Infrastructure

The proposed security assessment framework for critical infrastructure serves as a guide with activities designed to analyze security requirements, prioritize and track their implementation, and assess the overall maturity of an entity's security posture. It represents a systematic approach to connecting relevant elements of the presented model: assets, security goals, KPIs, threats, vulnerabilities, social actors, risk assessment information, and selected security requirements. The framework has multiple iterative activities grouped into three phases:

(1) The seeding phase

(2) The assessment phase

(3) The implementation tracking phase

Each phase is explained in detail in separate sections. The summary of all activities is presented in Table 4.1.

Phase	Activity	Inputs	Techniques	Outputs
The Seeding Phase	Asset inventory definition	Architecture, generic list of assets	Use cases, sessions with experts	Asset inventory
	Threat inventory definition	A generic list of threats, inventory of assets	Sessions with experts	Threat inventory
	Vulnerability inventory definition	A generic list of vulnerabilities, inventory of threats	Vulnerability scanning tools, security testing, penetration testing, code reviews	Vulnerability inventory
	Requirement inventory definition	Standards, guidelines, regulations	Expert analysis according to defined flow	Requirement inventory
The Assessment Phase	Compliance assessment	Requirements set, business and security goals	A questionnaire, providing evidence for each requirement compliance	Compliance scores, set of non-compliant requirements
The Implementation Tracking Phase	Goals definition	A generic list of goals	Sessions with stakeholders, security advisors	Goal collection
	KPIs definition	A generic list of KPIs	Sessions with stakeholders, security advisors	KPI collection
	Actor dependency graph creation	Organizational structure	Sessions with product owners, team leads	Actor dependency graph
	Risk assessment	Collections of assets, threats, vulnerabilities	Available techniques from Section 2.4	Risk collection

Table 4.1: Framework activities

We also implemented a proof-of-concept tool that follows all framework activities for the purpose of model validation.

4.1.1 The Seeding Phase

The first phase, called the seeding phase, requires users to populate knowledge bases with relevant elements. It consists of four activities:

- Asset inventory definition
- Threat inventory definition
- Vulnerability inventory definition
- Requirements inventory definition

As we already mentioned, assets and security requirements are indirectly connected with security controls. An asset can be anything that brings value to the organization, e.g., business functions, trade secrets, software, hardware, confidential documents, or people. If it gets compromised by a malicious user, the organization or system might suffer a loss. The goal of the first activity is to define an asset inventory. This collection can identify operating systems or proprietary software as an asset. Also, different hardware devices such as firewalls, sensors, and cameras can be added to the asset collection. Assets that end up in the collection might have different values so that additional classification can be done. For example, we can consider intellectual property such as, e.g. the algorithm for optimization of energy distribution to be more expensive than a web server. Here, assets can be assigned scores that reflect their value or importance to the organization or the customers. This will help in prioritizing risks in the following phases. Analysts with domain knowledge and familiarity with the organizational use cases have to curate the list of assets. Generic examples of assets that can help can be found in ISO/IEC 27005:2011 and the work of Herzog et al. [211].

It should be noted that it is desirable to have a defined inventory management process to maintain asset inventory. Also, assets would benefit from a tool dedicated to asset management. Stakeholders or security experts can perform asset checklist verification and avoid possible mistakes with these resources.

Similarly, threat inventory has to be defined during the second activity. Two broad categories of threats can be detected — natural and man-made threats. Natural threats can include wildfires, earthquakes, tornadoes, extreme cold, etc. Man-made threats can include terrorism and armed attacks, dysfunctional management practices, hacking and other cybersecurity crimes, etc. A threat can harm the system in the form of physical damage or through malware. If a threat is realized, assets can be compromised. Sessions with experts in the organization need to be made to recognize potential attackers, their capabilities, and motivations to impact assets negatively. Generic examples of threats that can help can be found in NIST SP 800-30, ISO/IEC 27005:2011, and the German BSI catalog [212].

The collection of potential vulnerabilities has to be defined during the third activity. The vulnerabilities are the threat's entry point to harm the assets. There is a hand full of methods that can be used to detect vulnerabilities ranging from basic code reviews to automated vulnerability scanning tools to penetration testing. Generic examples of vulnerabilities can be found in ISO/IEC 27005:2011.

The fourth activity requires that the database be populated with the requirements from all desired standards, guidelines, and regulations. The database can be a simple spreadsheet or a bespoke application. The activity diagram that represents the steps necessary for populating the database with new requirements based on the model is presented in Figure 4.1.

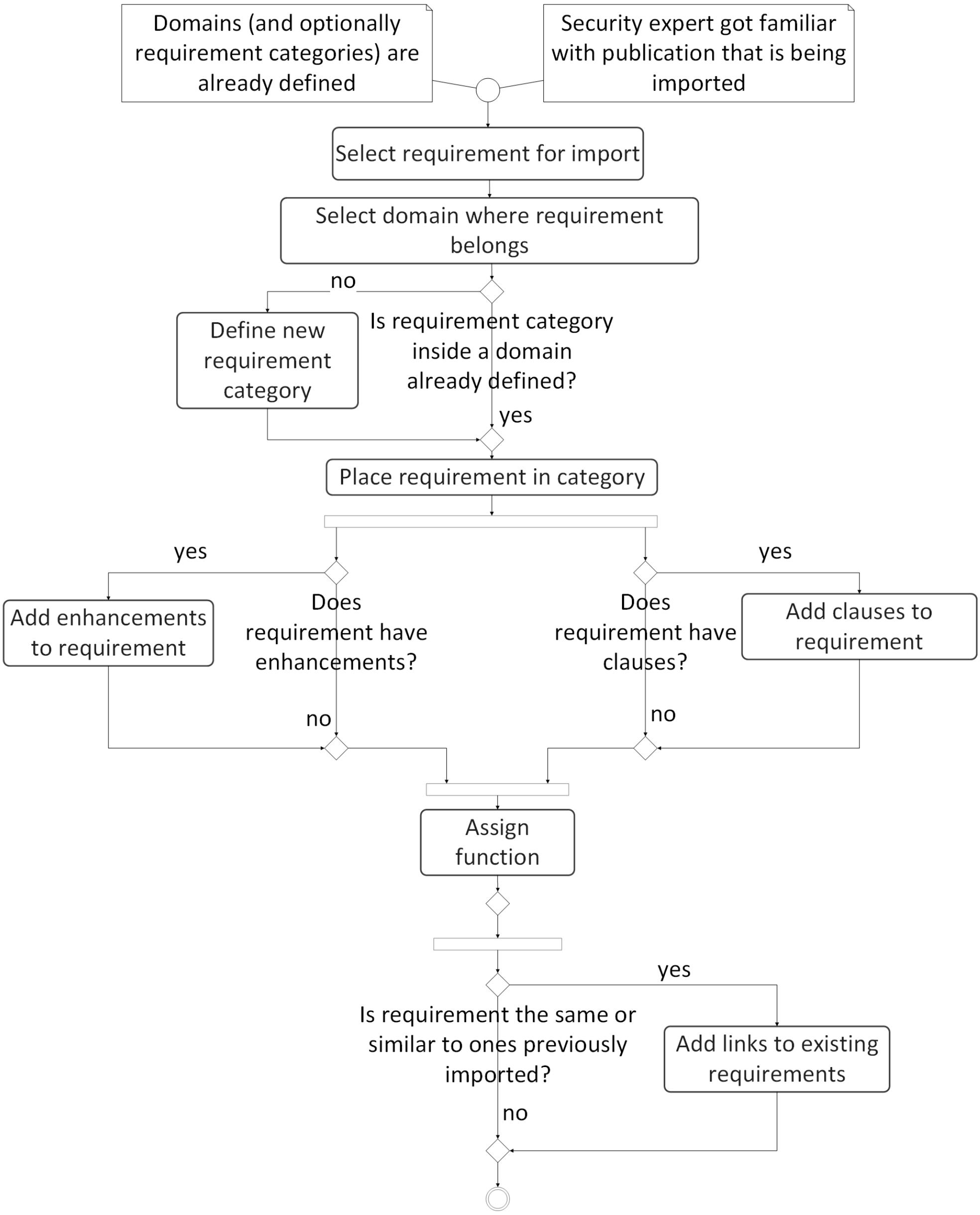

Domains (and optionally requirement categories) are already defined
Security expert got familiar with publication that is being imported
Select requirement for import
Select domain where requirement belongs
no
Is requirement category inside a domain already defined?
Define new requirement category
yes
Place requirement in category
yes
yes
Add enhancements to requirement
Does requirement have enhancements?
Does requirement have clauses?
Add clauses to requirement
no
no
Assign function
yes
Is requirement the same or similar to ones previously imported?
Add links to existing requirements
no

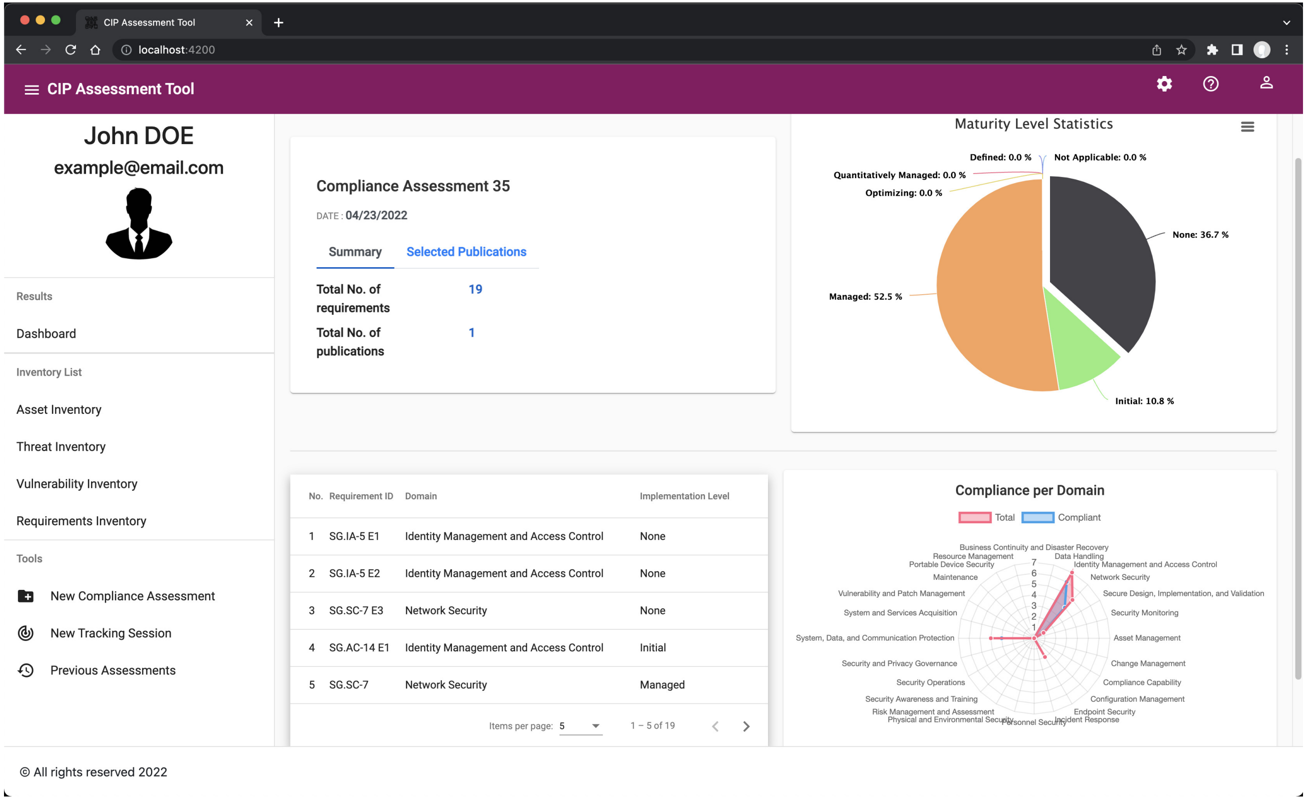
Figure 4.1: Process for import of new requirements

Every requirement is analyzed individually. The assumption is that the 24 domains are already defined as we did in Section 3.2. Also, an analyst or security expert has already got familiar with the publication structure that is being added to the collection. The process starts by populating relevant information about the requirement, metadata, and additional information. Next, the requirement is placed in one of the domains. Here, the subcategories can help in a fine-grained grouping. If the requirement is similar to other requirements from other publications that are already imported, it will be assigned to the existing subcategory. If not, a new subcategory that describes the nature of the requirement must be defined, and a new requirement must be added there. This analysis is beneficial for the next steps where the main parts of the requirement — clauses and enhancements — are imported. This decomposition can help determine what function and the essence level to assign and make a connection with similar requirements from other standards during the import. This can be an approach for building a knowledge database about similarities between different publications. Outputs of the activities in the seeding phase are required to set up the assessment in the second phase.

4.1.2 The Assessment Phase

The second phase, called the assessment phase, requires users to do the initial assessment. It consists of single activity — compliance assessment. For this activity, based on the business and security goals set by the stakeholders, compliance with the requirements from the selected standards is being assessed. This usually means that specific compliance level requirements need to be analyzed. The compliance assessment requires users to mark the requirement with one of the implementation levels from a scale provided in Section 3.3 (*Not Applicable, None, Initial, Managed, Defined, Quantitatively Managed, Optimizing*). This is required to gain information about the maturity of the security posture against the selected set of requirements. In the initial score, the partial compliance should be marked with implementation level *None* since in an actual audit, that would be treated as a nonconformance.

Nonetheless, the partial compliance information can be submitted as implementation evidence. This will be helpful for the last phase of our framework since it can significantly simplify the quantification of prioritization criteria. If the organization or system is compliant with the requirement, evidence materials must be provided in documents or links to other artifacts. When the assessment is done, results should contain relevant data such as requirement compliance and maturity based on the implementation levels scale for each requirement. An example from our tool is presented in Figure 4.2.



Compliance Assessment 35

DATE : 04/23/2022

Summary | Selected Publications

Total No. of requirements	19
Total No. of publications	1

No.	Requirement ID	Domain	Implementation Level
1	SG.IA-5 E1	Identity Management and Access Control	None
2	SG.IA-5 E2	Identity Management and Access Control	None
3	SG.SC-7 E3	Network Security	None
4	SG.AC-14 E1	Identity Management and Access Control	Initial
5	SG.SC-7	Network Security	Managed

Figure 4.2: Results of the compliance assessment phase

The most valuable output for the next phase is the set of non-compliant requirements.

4.1.3 The Implementation Tracking Phase

The final phase, the implementation tracking phase, requires users to prepare information for requirement implementation prioritization. It consists of four activities:

- Goals definition
- KPIs definition
- Actor dependency graph creation
- Risk assessment

Security goals represent objectives that, if achieved, would lift the security to a satisfactory level. They are influenced by business goals and stakeholders' views of a secure system, making them different for every organization. They usually refer to the CIA triad, authentication, authorization, and nonrepudiation with the idea of protecting the system against threats and vulnerabilities. Also, these individual goals can be fulfilled if compliance with a particular standard is reached. Sessions with stakeholders and security advisors can help in defining these goals. The same applies to key performance indicators because we need them to track goal completeness. As mentioned in Section 3.3, KPIs can be important to keep the teams involved in requirements implementation, aligned with security goals, and holding them accountable. Defining trackable KPIs can be difficult. Therefore, the KPIs definition requires brainstorming sessions with actors familiar with security goals, processes, and procedures used in the organization and the teams involved in reaching these goals.

The creation of an actor dependency graph requires good knowledge of the organizational structure or proper mapping of actors to the business roles in the organization. The formation of the actor dependency graph is explained in detail in Section 3.4.

The purpose of risk assessment is to evaluate the level of risk to the organization or system. Here, for each asset, associated threats and vulnerabilities are analyzed. Any methodology that suits the organization best can be used. Some of the proposed methodologies are presented in Section 2.4. The risk assessment results are inputs for the risk register, where every risk has to have an owner. This is usually someone from the management. The risk register is essential to decide which security risks must be addressed by implementing security controls and complying with security requirements and which can be accepted or mitigated. The activity diagram that represents the initial setup for tracking the implementation of the requirements is given in Figure 4.3.

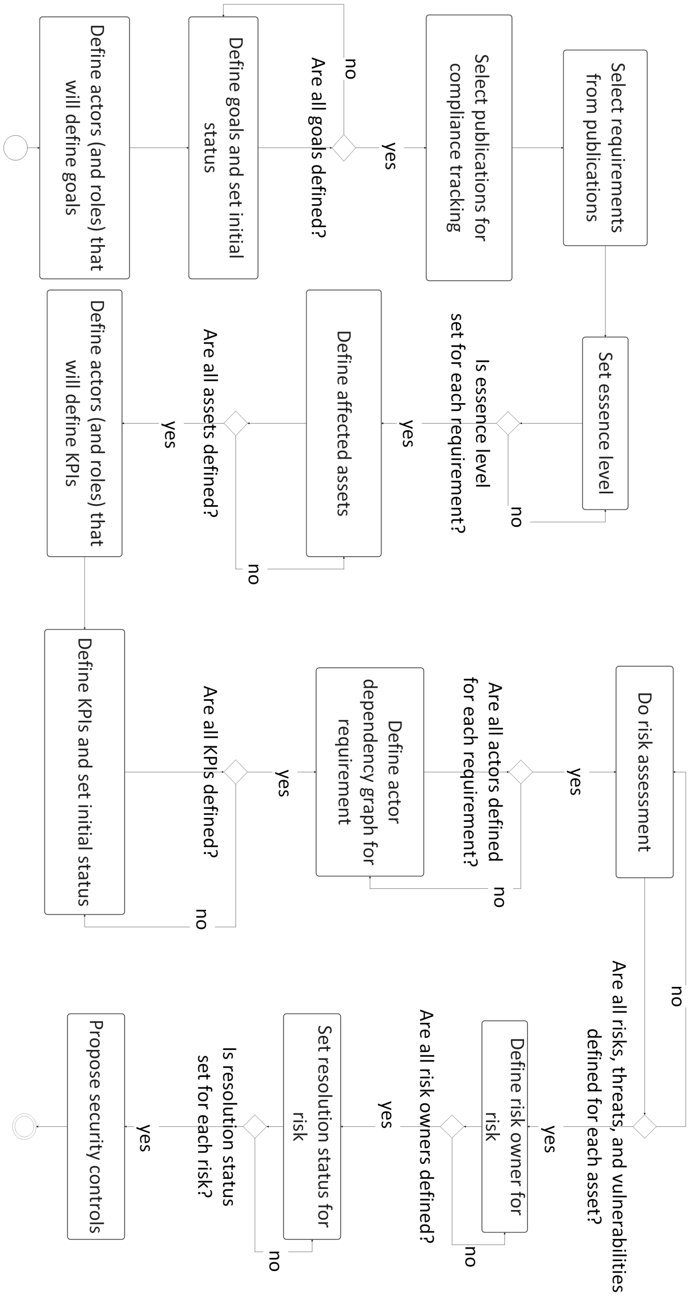

Define actors (and roles) that will define goals
Define goals and set initial status
Are all goals defined?
no
yes
Select publications for compliance tracking
Select requirements from publications
Set essence level
Is essence level set for each requirement?
no
yes
Define affected assets
Are all assets defined?
no
yes
Define actors (and roles) that will define KPIs
Define KPIs and set initial status
Are all KPIs defined?
no
yes
Define actor dependency graph for requirement
Are all actors defined for each requirement?
no
yes
Do risk assessment
no
Are all risks, threats, and vulnerabilities defined for each asset?
yes
Define risk owner for risk
Are all risk owners defined?
no
yes
Set resolution status for risk
Is resolution status set for each risk?
no
yes
Propose security controls

Figure 4.3: Initial setup for requirement implementation tracking

The process starts with selecting actors or stakeholders who define goals that directly determine the set of relevant requirements. This set can contain all non-compliant requirements that were the output of the previous phase or just their subset. If they were labeled partially compliant in the previous phase, relevant information about risks, threats, actor dependency graph, and partial evidence materials might already be familiar. This can speed up the overall analysis. Further, we define an asset list and actors that will define KPIs for tracking. Then, individual requirement analysis starts by defining the actor dependency graph and doing the risk assessment. The setup continues with the assignment of the risk owner and the risk resolution status. The setup ends with the proposal of the security controls that will fulfill the requirement. Now, we have all information that can be used to calculate the implementation priorities. This can be done using the SAW method we explained in Section 3.5 or any other multi-criteria decision-making method that can utilize provided information.

Since our prioritization criteria consist of four parts, it is worth noting that each of them can be used individually to group non-compliant requirements by similarity. This can give different views to our analyses. By regularly practicing these iterative activities and updating the implementation details of each requirement, we can track overall maturity against that set of requirements. Progress of implementation is tracked through KPIs statuses and overall goals statuses.

4.2 Case Study – Smart Grid Industrial Control System

In this section, we describe the scenario for using the framework by Vendor A, a company that produces software for an industrial control system for utilities worldwide. Vendor A has a workforce of around 300 software engineers of different seniority organized into agile teams.

Additionally, Vendor A has a dedicated security team that covers a broad spectrum of security-related activities. Also, Vendor A has established a security development lifecycle based on IEC 62443-4-1 standard.

Vendor A produces a set of software products for the utility companies. The software is customized for each customer and is deployed on the premises of the utility company, where the customer's personnel is responsible for secure operation. The software is not directly accessible from the Internet. It is configured and maintained by system administrators, used by utility controllers, and integrated with several other systems (e.g., remote terminal units in the field, customer's internal information systems, geographic information systems). This business model requires Vendor A to comply with various standards recognized worldwide. Furthermore, to enable customers to prove their regulatory compliance concerning the purchased software, Vendor A must provide the implementation evidence for each requirement fulfillment.

As a mature organization, Vendor A is already familiar with different standards. It is assumed that the sizeable mature organization has its system at least partially compliant with IEC 62443-3-3 and NIST SP 800-53. Hence, we will assume that the asset inventory definition, threat inventory definition, and vulnerability inventory definition activities are already practiced, and the knowledge base can be considered comprehensive enough for our exercise.

One publication that utility companies ask for compliance proof is the National Institute of Standards and Technology (NIST) Internal or Interagency Report (IR) 7628 Guidelines for Smart Grid Cybersecurity, a *de facto* standard for Smart Grid. It is worth to be noted that this publication was not in the set of analyzed standards, but it was the highly positioned publication in Table 3.1 in Section 3.1. NISTIR 7628 represents the three-volume report that describes an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their combinations of Smart Grid-related characteristics, risks, and vulnerabilities [189]. We can do the remaining activity from the seeding phase - requirements inventory definition.

Every requirement in NISTIR 7628 has a well-defined structure where information of interest that can be used in our model are as follows:

- *Name* and *Unique identifier* → can be mapped directly to *Metadata*
- *Requirement* base text → can be mapped directly to *Requirement*
- *Requirement clauses* → can be mapped directly to *Clause*
- *Supplemental guidance* → can be mapped to *Additional Information*
- *Requirement enhancements* → can be mapped directly to *Enhancement*
- *Additional considerations* → can be mapped to *Additional Information*

Supplemental guidance and *Additional considerations* do not map directly to the model elements. This is understandable since this type of information in different publications comes in different forms. For these purposes, *Additional Information* will contain this information. NISTIR 7628 has more information for requirements that are not directly mapped into our model:

- *Category* — identifies whether the security requirement is a governance, risk, and compliance, common technical, or unique technical requirement. This information can be helpful during the initial mapping process to determine in which requirement subcategory an observed requirement should be placed based on the similarity.

- *Impact Level Allocation* — represents impact levels for confidentiality, integrity, and availability objectives expressed on a low, moderate, and high scale. Security experts can use this information for calculating prioritization criteria.

Based on the mappings, we can conclude that the most valuable information in requirements from NISTIR 7628 can be mapped to the elements of our model.

To use NISTIR 7628 requirements with others from different publications, following the activity flow in Figure 4.1, we must try to classify these requirements into one of the 24 defined domains. This will demonstrate if the domain definition in previous research was done correctly. NISTIR 7628 has 197 requirements with 50 requirement enhancements classified initially into 19 domains. The mapping of the requirements to the proposed domains is already done in our previous work [45] and given in Table 4.2 The requirement enhancements are mapped to the same domain as the original requirements but omitted from Table 4.2 for better readability.

Domain	**Objective**
Business Continuity and Disaster Recovery	SG.CP-1, SG.CP-2, SG.CP-3, SG.CP-4, SG.CP-5, SG.CP-6, SG.CP-7, SG.CP-8, SG.CP-9, SG.CP-10, SG.IR-10
Data Handling	SG.AC-20, SG.CM-9, SG.ID-1, SG.ID-2, SG.ID-3, SG.ID-4, SG.ID-5, SG.MP-1, SG.MP-2, SG.MP-3, SG.MP-4, SG.MP-5, SG.MP-6
Identity Management and Access Control	SV.AC-1, SG.AC-2, SG.AC-3, SG.AC-4, SG.AC-6, SG.AC-7, SG.AC-8, SG.AC-11, SG.AC-12, SG.AC-13, SG.AC-14, SG.AC-15, SG.AC-16, SG.AC-17, SG.AC-18, SG.AC-19, SG.AC-21, SG.CM-5, SG.IA-1, SG.IA-2, SG.IA-3, SG.IA-4, SG.IA-5, SG.SC-19
Network Security	SG.AC-5, SG.CA-4, SG.SC-2, SG.SC-5, SG.SC-7, SG.SC-18, SG.SC-21
Secure Design, Implementation, and Validation	SG.AC-9, SG.AC-10, SG.CP-11, SG.IA-6, SG.IR-9, SG.PL-2, SG.SA-8, SG.SA-10, SG.SC-3, SG.SC-4, SG.SC-6, SG.SC-22, SG.SC-24, SG.SC-25, SG.SC-27, SG.SC-28, SG.SC-29, SG.SC-30, SG.SI-6, SG.SI-8, SG.SI-9
Security Monitoring	SG.AU-1, SG.AU-2, SG.AU-3, SG.AU-4, SG.AU-5, SG.AU-6, SG.AU-7, SG.AU-8, SG.AU-9, SG.AU-10, SG.AU-13, SG.AU-15, SG.AU-16, SG.CA-6, SG.SI-4
Asset Management	SG.CM-8
Change Management	SG.CM-3, SG.CM-4
Compliance Capability	SG.AU-11, SG.AU-14, SG.CA-1, SG.CA-2
Configuration Management	SG.CM-1, SG.CM-2, SG.CM-6, SG.CM-7, SG.CM-10, SG.CM-11, SG.SA-6, SG.SA-7, SG.SA-9
Endpoint Security	SG.SC-13, SG.SC-16, SG.SC-23, SG.SI-3, SG.SI-7
Incident Response	SG.IR-1, SG.IR-2, SG.IR-3, SG.IR-4, SG.IR-5, SG.IR-6, SG.IR-7, SG.IR-8, SG.IR-11
Personnel Security	SG.PL-3, SG.PS-1, SG.PS-2, SG.PS-3, SG.PS-4, SG.PS-5, SG.PS-6, SG.PS-7, SG.PS-8, SG.PS-9, SG.SA-2
Physical and Environmental Security	SG.PE-1, SG.PE-2, SG.PE-3, SG.PE-4, SG.PE-5, SG.PE-6, SG.PE-7, SG.PE-8, SG.PE-9, SG.PE-10, SG.PE-11, SG.PE-12
Risk Management and Assessment	SG.PL-4, SG.PM-5, SG.RA-1, SG.RA-2, SG.RA-3, SG.RA-4, SG.RA-5
Security Awareness and Training	SG.AT-1, SG.AT-2, SG.AT-3, SG.AT-4, SG.AT-6, SG.AT-7
Security Operations	/
Security and Privacy Governance	SG.AT-5, SG.CA-3, SG.CA-5, SG.PM-1, SG.PM-2, SG.PM-3, SG.PM-4, SG.PM-6, SG.PM-8, SG.PL-5, SG.SI-1, SG.SI-5
System, Data, and Communication Protection	SG.SC-1, SG.SC-8, SG.SC-9, SG.SC-10, SG.SC-11, SG.SC-12, SG.SC-14, SG.SC-15, SG.SC-17, SG.SC-20, SG.SC-26
System and Services Acquisition	SG.SA-1, SG.SA-4, SG.SA-5, SG.SA-11
Vulnerability and Patch Management	SG.RA-6, SG.SI-2
Maintenance	SG.MA-1, SG.MA-2, SG.MA-3, SG.MA-4, SG.MA-5, SG.MA-6, SG.MA-7
Portable Device Security	/
Resource Management	SG.PL-1, SG.PM-7, SG.SA-3, SG.AU-12

Table 4.2: NISTIR 7628 requirements mapping to domains

Let us compare the original classification of the requirements in the standard and our proposed classification. We can notice that not every requirement originally classified into original NISTIR 7628 domains belongs in that domain when a different approach for domain definition is introduced. Guided by different sets of domains, some of the requirements could be classified differently than those represented in Table 4.2. This is done subjectively, driven by security practitioners' knowledge earlier developed. All 197 requirements were classified into our existing domains. Out of 19 domains, 13 can have their requirements mapped to one of 24 domains we introduced earlier in this paper. *Media Protection (SG.MP)* and *Information and Document Management (SG.ID)* are the two domains with most requirements mapped onto the domain *Data Handling*. The same situation is with *Identification and Authentication (SG.IA)* and *Access Control (SG.AC)*, which are mapped to the *Identity Management and Access Control* domain. The requirements from only six original domains had to be reclassified to different domains: *Planning (SG.PL)*, *Security Assessment and Authorization (SG.CA)*, *Security Program Management (SG.PM)*, *mart Grid Information System and Information Integrity (SG.SI)*, *Smart Grid Information System and Communication Protection (SG.SC)* and *Smart Grid Information System and Services Acquisition (SG.SA)*. Out of 24 domains, 22 have at least one requirement assigned, while only two have none. These two are *Security Operations* and *Portable Device Security*. Figure 4.4 summarizes the mapping results.

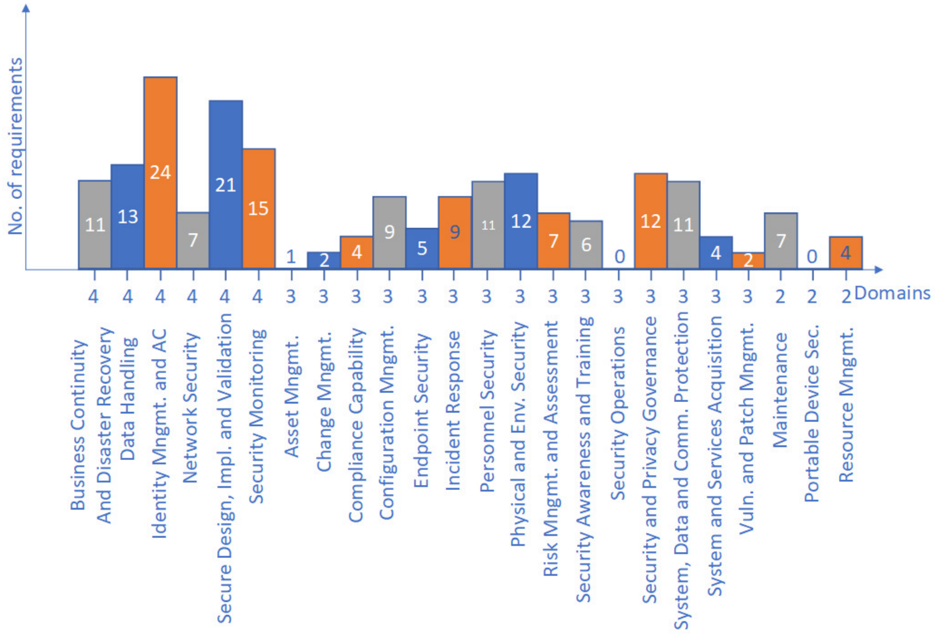


Figure 4.4: NISTIR 7628 summary numbers per domain

From the results, we can conclude that NISTIR 7628 covers similar requirements as previously analyzed publications. This confirms that the initial domain scores defined in Table 3.4 are valid. The only exceptions are *Asset Management* and *Change Management*, which lack more requirements, and the *Maintenance* domain records the increased number of requirements due to the existence of the dedicated domain in the original classification in the standard.

Following the steps from the activity diagram presented in Figure 4.1, simplified information for the *SG.IA-5 Device Identification and Authentication Enhancement 1* is provided as one model instance in Figure 4.5. Here, we present the connection with similar requirements from relevant standards based on the assumption about Vendor A's standards familiarity described earlier.

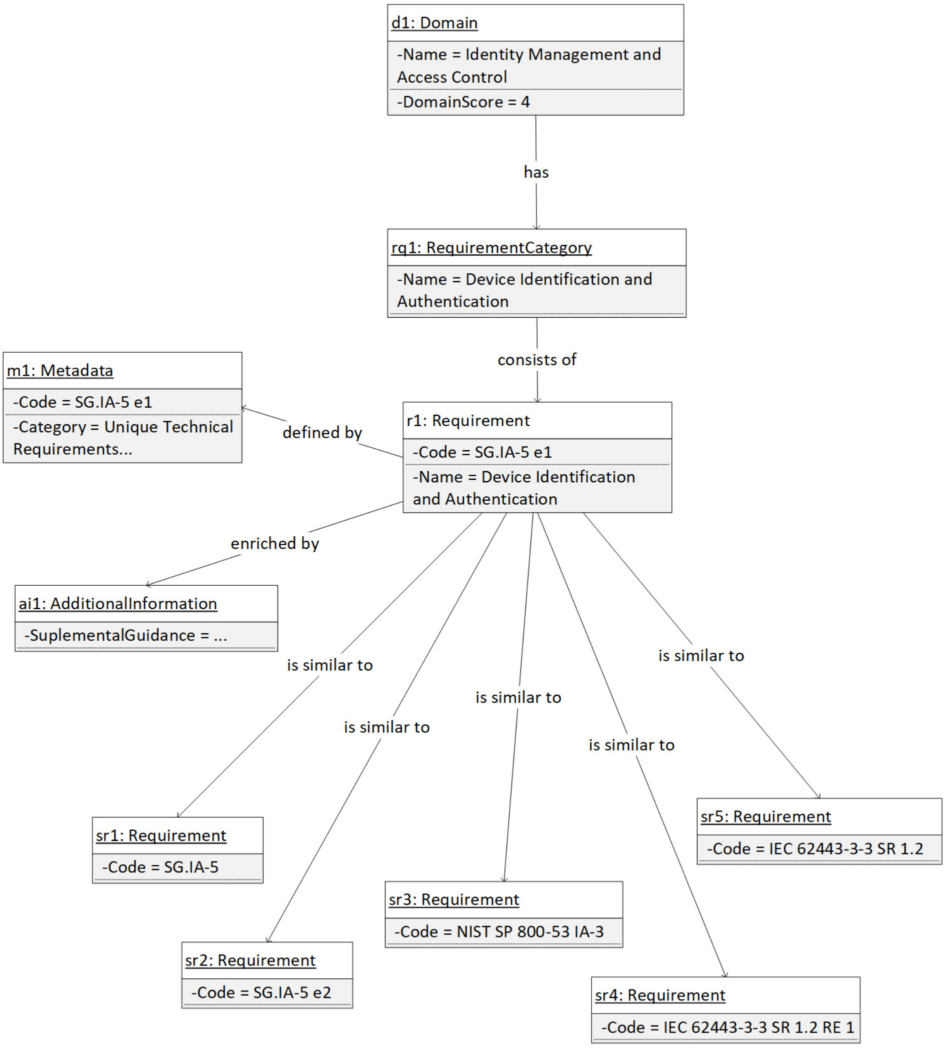

d1: Domain
-Name = Identity Management and Access Control
-DomainScore = 4
has
rq1: RequirementCategory
-Name = Device Identification and Authentication
consists of
m1: Metadata
-Code = SG.IA-5 e1
-Category = Unique Technical Requirements...
defined by
r1: Requirement
-Code = SG.IA-5 e1
-Name = Device Identification and Authentication
enriched by
ai1: AdditionalInformation
-SuplementalGuidance = ...
is similar to
is similar to
is similar to
is similar to
is similar to
sr1: Requirement
-Code = SG.IA-5
sr2: Requirement
-Code = SG.IA-5 e2
sr3: Requirement
-Code = NIST SP 800-53 IA-3
sr4: Requirement
-Code = IEC 62443-3-3 SR 1.2 RE 1
sr5: Requirement
-Code = IEC 62443-3-3 SR 1.2

Figure 4.5: SG.IA-5 Device Identification and Authentication Enhancement 1 as a model instance

NISTIR 7628 defines typical logical interface categories and architectural diagrams used in production with security requirements to help vendors and integrators during the design and development of security controls. For demonstration purposes for the compliance assessment phase, we have chosen interface category 4. This category defines the interface between control systems and equipment without high availability and computational and/or bandwidth constraints such as SCADA systems. This interface category suggests the fulfillment of the following requirements: *SG.AC-14*, *SG.IA-4*, *SG.IA-5*, *SG.IA-6*, *SG.SC-3*, *SG.SC-5*, *SG.SC-7*, *SG.SC-8*, *SG.SC-17*, *SG.SC-29* and *SG.SI-7*. These 11 requirements have additional eight requirement enhancements. The security goal in front of us is to have all 19 requirements fulfilled. The results are presented in Table 4.3.

Requirement ID	**Compliance**	**Implementation Level**
SG.AC-14	Compliant	Initial
SG.AC-14 E1	Compliant	Initial
SG.IA-4	Compliant	Managed
SG.IA-5	Compliant	Managed
SG.IA-5 E1	Partially Compliant	None
SG.IA-5 E2	Not Compliant	None
SG.IA-6	Compliant	Managed
SG.SC-3	Compliant	Managed
SG.SC-5	Compliant	Managed
SG.SC-7	Compliant	Managed
SG.SC-7 E1	Compliant	Managed
SG.SC-7 E2	Compliant	Managed
SG.SC-7 E3	Not Compliant	None
SG.SC-8	Compliant	Managed
SG.SC-8 E1	Partially Compliant	None
SG.SC-17	Not Applicable	None
SG.SC-29	Compliant	Managed
SG.SI-7	Not Compliant	None
SG.SI-7 E1	Not Compliant	None

Table 4.3: Compliance Assessment Results

Table 4.3 shows that out of 19 requirements, two are marked as partially compliant, four as non-compliant, and one as not applicable. The implementation level for compliant requirements is mainly in a managed state.

In the final phase of the framework, six requirements previously marked as not compliant and partially compliant with the implementation level *None* are assessed. Following the activity flow defined in Figure 4.3, six requirements were assigned necessary information. The example for *SG.IA-5 E1* requirement is given in Figure 4.6. The number of assets, risks, and security controls in Figure 4.6 is reduced and simplified for better readability. Also, only risks with maximum value were included in further calculating the risk level score. Risk assessment was done following the NIST SP 800-30 guidance.

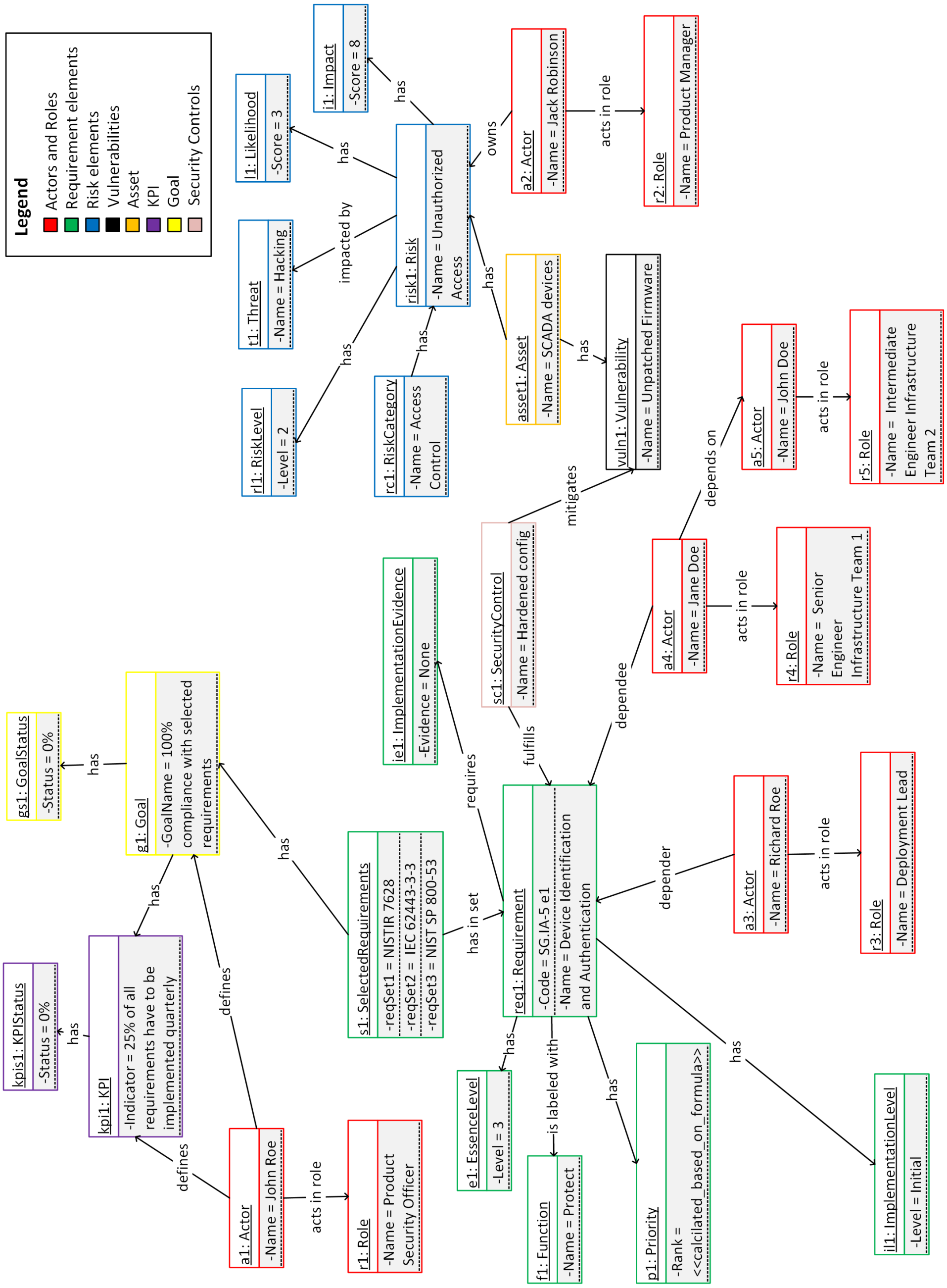


Figure 4.6: SG.IA-5 Enhancement 1 – complete initial setup

At this stage, the users have enough information to see the exercise's goal, how it is measured, which assets and actors are involved, their dependency graph, and associated risks. By repeating these steps for each remaining requirement, using the SAW method as described in Section 3.5, the suitability rating matrix is defined and presented in Table 4.4.

Requirement	C_1	C_2	C_3	C_4
SG.IA-5 E1	2	2	1	3
SG.IA-5 E2	2	2	1	3
SG.SC-7 E3	2	1	1	3
SG.SC-8 E1	3	2	2	2
SG.SI-7	2	3	2	2
SG.SI-7 E1	2	1	1	2

Table 4.4: Suitability Rating Matrix for Vendor A assessment

Finally, implementation priority is calculated and presented in Table 4.5.

Requirement	**Score**	**Ranking**
SG.SC-8 E1	0.8095	1
SG.SI-7	0.7435	2
SG.IA-5 E1	0.736	3
SG.IA-5 E2	0.736	4
SG.SC-7 E3	0.634	5
SG.SI-7 E1	0.6175	6

Table 4.5: Final requirement priorities for Vendor A

Looking at the results, we can see that the requirement *SG.SC-8 E1*, which requires having cryptography mechanisms employed to ensure communication integrity, got the highest priority for implementation. This is reasonable since the suitability rating matrix shows the highest scores for all criteria. The following requirement is a mandatory requirement *SG.SI-7*, but since the risk assessment criterion has the highest weight, *SG.SC-8 E1*, even though it is an enhancement, has a higher priority. If the risk assessment for the *SG.SI-8 E1* had been calculated differently, the score might have been lower, and the mandatory requirement SG.SI-7 would come on top. The following two requirements, *SG.IA-5 E1* and *SG.IA-5 E2* are related to the authentication of devices. They got the same score as expected since both requirements are enhancements of the same base requirement. The nuance that separates the last two requirements is the domain affiliation score, which in our opinion, makes a valid difference since implementing proper boundary protection can provide protection against a more significant number of remote threats.

4.3 Discussion

We mentioned that countries and standardization bodies form working groups to publish new, improved guidelines, directives, and standards to enforce better security. The organizations are obligated to align with these standards, guidelines, and directives. Having a model that can be used to map every new security requirement that arises would benefit a significant number of organizations. This can be a sound basis for further automation. That is why we presented a set of activities in the form of a framework that aims to map the individual model component to check its applicability. We presented a detailed analysis of the NISTIR 7628 standard and how it fits into our model. The results can be considered satisfactory. During the analysis, we have seen that NISTIR 7628 requirements are structured in a way that the most important elements can be mapped to our model. The NISTIR 7628 and our domain definition similarity helped with faster requirement classification. This confirmed that our initial selection of publications from which we defined our model was adequate.

During the definition of the model and later during the validation process, we confirmed that many standards that have narrower applicability in terms of the CI sectors or geographical region are similar to the most influential standards, security guidelines, and regulations, especially the ones we selected for our analysis. This is encouraging as the cost of aligning with every next standard is significantly reduced since the requirements and the analysis steps are already familiar. The same applies to risks, threats, vulnerabilities, and actors. The NISTIR 7628 offers real-world scenarios where the requirement elicitation is already provided. In the scenario where interface category 4 set of requirements was assessed, we have seen that risks dictate the prioritization for the implementation. However, the rest of the criteria give the finer granulation between the requirements, giving the importance even to the least impactful criterion - domain affiliation. Risk assessment can be done by following any methodology as long as the risks can be quantified. Since the risk score bears half of the total weight, it must be done carefully. This can be time-consuming, but the timing can be improved by adequately doing the activities from the seeding phase of the framework. Having the tool that follows the framework can improve the assessment even further.

This kind of framework represents a sound basis for further improvement of existing processes in companies, such as system security plans. To the best of our knowledge, the approach for model construction described in this thesis that considers the social actor aspect in the form of a dependency graph was not made previously. The organization's personnel works on compliance preparations, so this part can be beneficial for providing the details about who and why has done a specific action to improve security posture. Further, the model has the necessary components to connect with a risk assessment. This is done through the requirement prioritization criteria to allow usage of an arbitrary risk assessment framework and put emphasis on the requirement implementation rather than on a purely numeric estimation of risk without any action items. More insights and tracking details of the implemented requirements can be given by having the requirements and associated risks more coupled. The data that can be extracted from the assessment results can provide sufficient information about the implementation status, such as the number or percentage of fulfilled requirements, implementation priority, risks accepted or mitigated, and actors involved.

The model is compatible with the OSCAL document format for requirements exchange. Even if it is in the early stage of development, projected to be a *de facto* standard, and thus our model can be ready for its early adoption. The mappings of relevant elements between the two models are presented in Figure 4.7.

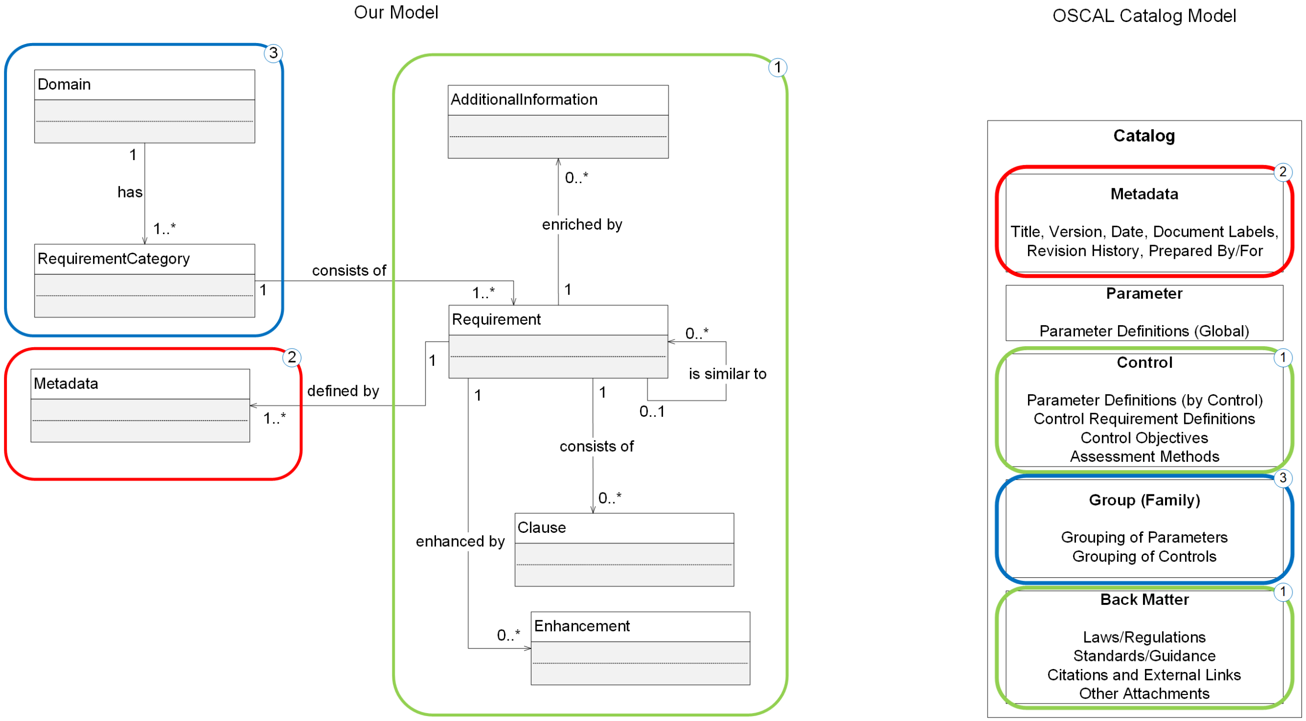


Figure 4.7: Requirement Model to OSCAL Catalog Model mapping

Applications that use this model can also use OSCAL documents as an exchange data format. It is only necessary to remove sufficient data that OSCAL documents require and insert additional parameters introduced with our model. This can also be applicable to our proof-of-concept tool implemented for the model validation.

Further, compared to others mentioned in Section 2.2, our framework gives the users the advantage of having one means that enables the comparison of multiple standards at once. It gives insights into the quantitative and qualitative nature of the requirement implementation through the assurance model and maintains the complexity of all involved social parties in the form of a dependency graph. All components are based on the proven methods and appropriately adjusted to fit the model's needs. In our model, we removed the CSF's limitation in terms of grouping by functions but kept that information to help security practitioners during the requirement analysis providing more flexibility per the Cyber Defense Matrix. The tools such as CSET, CS2SAT, or CRR utilize security requirements from different security publications to form a questionnaire that would allow for a quick self-assessment of the current security posture. Our framework goes into more detail and focuses on the requirements from the security publications. In this way, a more precise analysis can be done, with enough details to proceed with the security posture uplift.

One limitation can be our prioritization criteria. The primary vector is focused on the risk assessment, which has its drawbacks. We aimed to support a numeric estimation of risks that can impact the priority of the requirement implementation regardless of a large number of proposed risk methodologies. This would enable the security decision-makers to understand the current security posture of an organization or system and help them allocate security funds to improve it. We believe that the model can be easily extended to use a suitable risk methodology that might converge in the future if the current model is not adequate. Also, the cost-benefit analysis considers only the actor dependency graph as an actual cost. The reasoning behind it is that if more people are involved in implementation, more time will use for the security activities, which may negatively impact the planning and development of new features. Expanding prioritization criteria with additional criterion, e.g., a budget, may produce results that are better aligned with business goals.

Another limitation of the proposed solution is more oriented toward the current nature of the defined domains. Even though the domains that we defined as a basis for the requirements classification are expandable, every new domain introduced afterward can potentially desynchronize the initial mappings of the requirements. As an example, if the organization is heavily reliant on cloud technologies, introducing a new cloud security domain would be a suitable extension. This would require reclassifying some existing requirements, e.g., NIST 800-53 SA-9 External system services could be transferred from the asset management domain to the new cloud security domain. This dynamic recalibration of the requirements classification without strong manual interference by the experts may introduce problems. A possible solution would be to expand the requirements with new similarity factors to help with the automation. This is considered to be future work.

Chapter 5

Conclusion

An increasing number of exploits of software and hardware solutions vulnerabilities are making daily headlines in mass media. The critical infrastructure sectors are not spared. This positions the security of organizations and their systems as one of the top priorities.

Throughout this work, we have focused on the measures that can be taken to uplift the security posture by following guidance presented in different security standards, guidelines, and regulations. We found that following many requirements from different publications can be challenging and time-consuming. We found that many requirements are pretty similar by comparing publications side by side. It is not surprising that organizations can be confused and indecisive on which standards to follow. An increasing number of standards and local regulations put even more pressure on organizations that want a presence in different parts of the world. They are required to be compliant with a hand full of requirements simultaneously. Even though some requirements can be similar, some are not, and they must be implemented accordingly. This requires a good strategy on how to approach and track the implementation. In the existing literature, some initiatives can be found that try to solve some of the issues presented here but usually focus on one issue at a time without connecting with others.

We aimed to connect and address all practical issues through one comprehensive study.

Based on this research, we defined the following research questions:

(1) *Can an extensible model be developed to represent the requirements from security standards applicable to the Critical Infrastructure?*

(2) *How to obtain information on the maturity of the security infrastructure of an organization or system in relation to the requirements defined in arbitrary security standards while using domain and organizational knowledge to conduct a risk assessment, planning, and tracking of the security improvements?*

From there, we formulated hypotheses that guided our work:

(1) **Hypothesis:** *It is possible to define a model for the representation of the requirements from different security standards, guidelines, and regulations for critical infrastructure. The model should allow the presentation of relevant information common to the requirements of different publications, thus allowing their cross-comparison.*

(2) **Hypothesis:** *It is possible to define criteria for prioritization of requirements that, in addition to risk, include the complexity introduced by the dependencies between the different roles of participants in the organizational structure in charge of implementing requirements, the level of importance of the compliance requirements, and the domain affiliation.*

(3) **Hypothesis:** *It is possible to extend the model to provide a unique domain-oriented view that allows simultaneous tracking of the implementation of similar requirements selected from different security standards, guidelines, and regulations for critical infrastructure.*

Section 5.1 highlights the contributions of this thesis, which can be grouped around the model, prioritization criteria, and evaluation framework. Section 5.2 presents future research and development opportunities.

5.1 Contributions of the Thesis

To address the first research question, we inspected various models for security requirements representation in Sections 2.1 and 2.2 to learn about elements that are necessary building units for our model. Section 2.1 contains a glossary of these elements.

To define our model, we first conducted a systematic literature review to extract relevant publications for further structural analysis in Section 3.1. We established eligibility criteria for the final set of publications that resulted in four publications of interest:

- IEC 62443
- ISO/IEC 27001 and 27002
- NIST SP 800-53
- NERC CIP

The information gained from these publications was beneficial for model creation presented in Section 3.6.

During the analysis of different standards, guidelines, and regulations, we found that one of the key challenges after understanding the requirements is to provide a way to measure how they are implemented and in which order. To address the second research question, this required us to define prioritization criteria to describe key features that need to be determined when planning the implementation. Through Sections 2.3, 2.4, and 2.5, we examined various concepts closely connected with security requirements. These analyses provided us with enough information to construct the prioritization criteria in Sections 3.2, 3.3, 3.4, and 3.5, that has four essential criteria:

- Risk level — reflects the results of the risk assessment that can be done using any suitable methodology that is able to quantify risks. This is the most influential criterion for the overall priority score;
- Essence level — information driven by the nature of the requirements in the publication that the organization needs to be compliant with;
- Actor dependency graph complexity — provides information about necessary dependencies between users involved in the implementation of incompliant requirements;
- Domain affiliation — adds qualitative information about the requirements that can reflect nuances between requirements classified into different domains.

To validate the applicability of our model, in Chapter 4, we constructed the framework and provided guidance for the collection of all relevant information that the model requires. We used knowledge from Chapters 2 and 3 to define the set of activities required to assess the maturity of the security posture of an arbitrary organization or system. We evaluated our framework and model on a case study implementation with one domain-specific standard.

To summarize, the contributions of this thesis include:

- The definition of a model for security requirement representation that can be used for tracking implementation and compliance with multiple security standards, guidelines, and regulations simultaneously in a uniform manner;
- The definition of the prioritization criteria that is relevant for the implementation of incompliant security requirements; the

prioritization criteria rely on four factors: risk assessment results, essence levels of the requirements set that is analyzed, dependency graph of the social actors involved in the implementation, and the domain affiliation of the requirement;

- The definition of the framework for model usage, including guidance for its execution and tailoring; the framework guides users through all activities, from importing new requirements to quantitatively expressing prioritization criteria to assessing the maturity of the security posture of an organization or system.

Considering these contributions, we confirm the stated hypotheses and meet all the introduced goals and expected results of this research.

5.2 Future Work

The contributions we presented in this thesis do not solve all security issues that can arise. They can help in the security uplift journey, but the connections with different security lifecycle development practices must be strengthened. Every new artifact produced during the design, implementation or verification phase of the system development can be used as a valuable evidence resource for our framework. Depending on how security is practiced in the organization, this connection could be formalized through strictly defined processes and further automatized with bespoke applications.

One of the steps that can be done is expanding the knowledge base of available standards, primarily focusing on relatively new concepts and technologies such as cloud computing, edge computing, and the Internet of Things. This would keep our systematization of knowledge about security requirements up to date and relevant in the future. Also, the framework can be expanded with additional activities such as enforcing different kinds of tabletop exercises that would help detect new threats and vulnerabilities.

As we already mentioned, new technologies will require new standards that may open an issue related to the static nature of the proposed framework. Once the requirement is assigned to a specific domain, it should not be reclassified in the current proposal. New technologies will undoubtedly require other security aspects to be tackled that might introduce new domains that would naturally group some existing requirements. This would mean that some steps from the framework would need to be triggered again to recalibrate the existing setup. Dynamic recalibration without strong manual interference by the experts in this situation would save much time.

Further, our analysis focuses on the security requirements, omitting the regulations that cover privacy aspects. Since many of the privacy requirements are related to data handling, our proposed domains can be expanded with new subcategories that would describe these aspects. This would also extend the applicability of the model and framework to non-critical infrastructure sectors.

Even though our prioritization criteria are colored with budgetary constraints in the background, we did not explicitly tackle this segment in our cost-benefit analysis. Expanding the prioritization criteria with this criterion might bring additional value to the stakeholders in redistributing the budget in the organizational structure.

The framework can be used as a tool for auditing purposes. Our proof-of-concept application can be enhanced with proposed features and offered as an open-source tool. It might be used in combination with modern concepts such as blockchain to enable transparency of the results and improve the performance of the certification process.

Bibliography

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review (2008).

[2] V. Buterin, Ethereum: A next-generation smart contract and decentralized application platformhttps://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf (Accessed February 7, 2022).

[3] A. B. L. de Sousa Jabbour, C. J. C. Jabbour, C. Foropon, M. Godinho Filho, When titans meet – Can industry 4.0 revolutionise the environmentally-sustainable manufacturing wave? The role of critical success factors, Technological Forecasting and Social Change 132 (C) (2018) 18–25. doi:10.1016/j.techfore.2018.0.

[4] A. Jamwal, R. Agrawal, M. Sharma, A. Giallanza, Industry 4.0 technologies for manufacturing sustainability: A systematic review and future research directions, Applied Sciences 11 (12) (2021). doi:10.3390/app11125725.

[5] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, Q. Li, Y. C. Hu, Make web3.0 connected, IEEE Transactions on Dependable and Secure ComputingPublisher Copyright: IEEE (2021). doi:10.1109/TDSC.2021.3079315.

[6] C. Foundations, Protecting america's infrastructures, The Report of the (1997).

[7] P. Act, Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001, Public Law 107 (2001) 56.

[8] W. House, Presidential policy directive/ppd 21–critical infrastructure security and resilience, Washington, DC (2013).

[9] E. Commission, Critical infrastructure, Tech. rep., https://ec.europa.eu/home-affairs/pages/page/critical-infrastructure_en (Accessed February 2, 2022).

[10] S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE control systems magazine 21 (6) (2001) 11–25.

[11] E. Martinez-Hernandez, M. Leach, A. Yang, Understanding water-energy-food and ecosystem interactions using the nexus simulation tool nexsym, Applied Energy 206 (2017) 1009–1021.

[12] X. Zhang, V. V. Vesselinov, Integrated modeling approach for optimal management of water, energy and food security nexus, Advances in Water Resources 101 (2017) 1–10.

[13] L. Wu, A. Elshorbagy, S. Pande, L. Zhuo, Trade-offs and synergies in the water-energy-food nexus: The case of saskatchewan, canada, Resources, Conservation and Recycling 164 (2021) 105192. doi:https://doi.org/10.1016/j.resconrec.2020.105192.

[14] M. Bazilian, H. Rogner, M. Howells, S. Hermann, D. Arent, D. Gielen, P. Steduto, A. Mueller, P. Komor, R. S. Tol, et al., Considering the energy, water and food nexus: Towards an integrated modelling approach, Energy policy 39 (12) (2011) 7896–7906.

[15] G. M. Gold, M. E. Webber, The energy-water nexus: an analysis and comparison of various configurations integrating desalination with renewable power, Resources 4 (2) (2015) 227–276.

[16] A. Dubreuil, E. Assoumou, S. Bouckaert, S. Selosse, N. Maı, et al., Water modeling in an energy optimization framework–the water-scarce middle east context, Applied energy 101 (2013) 268–279.

[17] D. Energy, The water-energy nexus: Challenges and opportunities, US Department of Energy (2014).

[18] A. Laugé, J. Hernantes, J. M. Sarriegi, Critical infrastructure dependencies: A holistic, dynamic and quantitative approach, International Journal of Critical Infrastructure Protection 8 (2015) 16–23.

[19] L. Strezoski, I. Stefani, Utility derms for active management of emerging distribution grids with high penetration of renewable ders, Electronics 10 (16) (2021) 2027.

[20] L. A. Rossman, R. E. Dickinson, T. Schade, C. C. Chan, E. Burgess, D. Sullivan, F.-H. Lai, Swmm 5-the next generation of epa's storm water management model, Journal of Water Management Modeling (2004).

[21] R. Schierholz, B. de Wijs, Cybersecurity in power plants: Still an underestimated problem-how end users and vendors are or should be facing it, in: PowerGen Europe, 2011.

[22] D. Dzung, M. Naedele, T. P. Von Hoff, M. Crevatin, Security for industrial communication systems, Proceedings of the IEEE 93 (6) (2005) 1152–1177.

[23] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, B. Green, Looking back to look forward: Lessons learnt from cyber-attacks

on industrial control systems, International Journal of Critical Infrastructure Protection 35 (2021) 100464.

[24] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security & Privacy 9 (3) (2011) 49–51.

[25] K. Zetter, Everything we know about ukraine's power plant hack, Wiredhttps://web.archive.org/web/20220316203035/https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (Accessed on 3 September 2021).

[26] K. E. Hemsley, E. Fisher, et al., History of industrial control system cyber incidents, Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States) (2018).

[27] N. Perlroth, Hackers are targeting nuclear facilities, homeland security dept. and fbi say, The New York Timeshttps://web.archive.org/web/20220316215753/https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html (Accessed on 3 September 2021).

[28] A. Di Pinto, Y. Dragoni, A. Carcano, Triton: The first ics cyber attack on safety instrument systems, in: Proc. Black Hat USA, Vol. 2018, 2018, pp. 1–26.

[29] R. Dudley, D. Golden, The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms, Tech. rep., https://energyrights.info/sites/default/files/artifacts/media/pdf/the_colonial_pipeline_ransomware_hackers_had_a_secret_weapon_self-promoting_cybersecurity_firms_-_propublica.pdf (Accessed on 3 September 2021).

[30] S. Duncan, R. Carneiro, J. Braley, M. Hersh, F. Ramsey, R. Murch, Beyond ransomware: Securing the digital food chain, Tech. rep., https://web.archive.org/web/20220301090045/https://www.ift.org/news-and-publications/food-technology-magazine/issues/2021/october/features/digital-food-chain (Accessed on 3 September 2021).

[31] E. Luiijf, M. Klaver, Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set, International Journal of Critical Infrastructure Protection 35 (2021) 100471.

[32] S. Ruffle, É. Leverett, A. Coburn, S. Kelly, T. Evan, Cyber risk: Business blackout the insurance implicatons of a cyber attack on the us power grid (2020).

[33] C. Directive, 114/ec of 8 december 2008 on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union 23 (2008) (2008) 74–82.

[34] J. Lopez, R. Setola, S. D. Wolthusen, Overview of critical information infrastructure protection, in: Critical Infrastructure Protection, Springer, 2012, pp. 1–14.

[35] W. J. Tolone, D. Wilson, A. Raja, W.-n. Xiang, H. Hao, S. Phelps, E. W. Johnson, Critical infrastructure integration modeling and simulation, in: International conference on intelligence and security informatics, Springer, 2004, pp. 214–225.

[36] M. Dunn Cavelty, M. Suter, The art of ciip strategy: tacking stock of content and processes, in: Critical Infrastructure Protection, Springer, 2012, pp. 15–38.

[37] U. S. O. of Homeland Security, National strategy for homeland security, DIANE Publishing, 2002.

[38] N. C. for Counterterrorism, M. o. J. Security, Security, National security strategy 2019, Tech. rep., https://english.nctv.nl/topics/national-security-strategy/documents/publications/2019/09/19/national-security-strategy (Accessed on 3 September 2021).

[39] U. S. D. of Homeland Security, National Infrastructure Protection Plan, Partnering to enhance protection and resiliency, US Department of Homeland Security, 2009.

[40] C. Governments, National strategy for critical infrastructure, Her Majesty the Queen in Right of Canada, Canada (2009).

[41] K. M. Kolevar, Energy critical infrastructure and key resources sector-specific plan as input to the national infrastructure protection plan (redacted) (2007).

[42] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on scada systems, in: 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing, IEEE, 2011, pp. 380–388.

[43] T. J. Williams, The purdue enterprise reference architecture, Computers in industry 24 (2-3) (1994) 141–158.

[44] D. Kuipers, M. Fabro, Control systems cyber security: Defense in depth strategies, Tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States) (2006).

[45] M. Stojkov, N. Dalčeković, B. Markoski, B. Milosavljević, G. Sladić, Towards cross-standard compliance readiness: Security requirements model for smart grid, Energies 14 (21) (2021) 6862.

[46] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, Nist special publication 800-150: guide to cyber threat information sharing, NIST, Tech. Rep (2016).

[47] E. Gal-Or, A. Ghose, The economic consequences of sharing security information, in: Economics of information security, Springer, 2004, pp. 95–104.

[48] R. G. Randall, S. Allen, Cybersecurity professionals information sharing sources and networks in the us electrical power industry, International Journal of Critical Infrastructure Protection 34 (2021) 100454.

[49] N. Sjelin, G. White, The community cyber security maturity model, in: Cyber-Physical Security, Springer, 2017, pp. 161–183.

[50] W. Zhao, G. White, A collaborative information sharing framework for community cyber security, in: 2012 IEEE Conference on Technologies for Homeland Security (HST), IEEE, 2012, pp. 457–462.

[51] C. Goodwin, J. P. Nicholas, J. Bryant, K. Ciglic, A. Kleiner, C. Kutterer, A. Massagli, A. Mckay, P. Mckitrick, J. Neutze, et al., A framework for cybersecurity information sharing and risk reduction, Microsoft (2015).

[52] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, International Journal of Electronic Commerce 9 (1) (2004) 70–104.

[53] K. Campbell, L. A. Gordon, M. P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer security 11 (3) (2003) 431–448.

[54] Å. J. Holmgren, S. Molin, Using disturbance data to assess vulnerability of electric power delivery systems, Journal of Infrastructure Systems 12 (4) (2006) 243–251.

[55] G. W. Bush, National strategy for the physical protection of critical infrastructures and key assets, Department of Homeland Security, 2003.

[56] K. T. Schwalm, National strategy to secure cyberspace, Tech. rep., DNK LLC ALBUQUERQUE NM (2006).

[57] N. A. E. R. C. (NERC), Cip standards, Tech. rep., https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (Accessed February 7, 2022).

[58] N. A. E. R. C. (NERC), Frequently asked questions cip version 5 standards consolidated comments, Tech. rep., https://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPV5_FAQs_May_Posting_Consolidated_Comments_June_17_2015.pdf (Accessed February 7, 2022).

[59] Å. J. Holmgren, A framework for vulnerability assessment of electric power systems, in: Critical Infrastructure, Springer, 2007, pp. 31–55.

[60] G. H. Baker, A vulnerability assessment methodology for critical infrastructure sites, in: DHS symposium: R and D partnerships in homeland security, 2005.

[61] C.-W. Ten, C.-C. Liu, G. Manimaran, Vulnerability assessment of cybersecurity for scada systems, IEEE Transactions on Power Systems 23 (4) (2008) 1836–1846.

[62] A. Ferreira, Vulnerability analysis in critical infrastructures: A methodology, Security and Defence Quarterly 24 (2) (2019) 65–86.

[63] L. Allodi, F. Massacci, Security events and vulnerability data for cybersecurity risk estimation, Risk Analysis 37 (8) (2017) 1606–1627.

[64] L. Franchina, G. Inzerilli, E. Scatto, A. Calabrese, A. Lucariello, G. Brutti, P. Roscioli, Passive and active training approaches for critical infrastructure protection, International Journal of Disaster Risk Reduction 63 (2021) 102461.

[65] A. Brilingaitė, L. Bukauskas, V. Krinickij, E. Kutka, Environment for cybersecurity tabletop exercises, in: ECGBL 2017 11th European Conference on Game-Based Learning, Academic Conferences and publishing limited, 2017, pp. 47–55.

[66] P. S. Evangelos Ouzounis, Panagiotis Trimintzios, National exercise - good practice guide, Tech. rep., https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide (Accessed on 16 February 2022).

[67] H. Luiijf, D. Stolk, An international tabletop exercise on critical infrastructure protection: the lessons identified, International journal of critical infrastructures 6 (3) (2010) 293–303.

[68] N. A. E. R. C. (NERC), Gridex, Tech. rep., https://www.nerc.com/pa/CI/ESISAC/Pages/GridEx.aspx (Accessed on 16 February 2022).

[69] Cybersecurity, I. S. Agency, Cyber storm: Securing cyber space, Tech. rep., https://www.cisa.gov/cyber-storm-securing-cyber-space (Accessed on 16 February 2022).

[70] I.-T. Lo, C.-Y. Lin, M.-T. Cheng, A covid-19 lockdown tabletop exercise in new taipei city, taiwan, Disaster Medicine and Public Health Preparedness (2021) 1–7.

[71] ISACA, 2019 report: Annual isaca/protiviti survey - today's toughest challenges in it audit: Tech partnerships, talent, transformation, Tech. rep., https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpgl (Accessed on 16 February 2022).

[72] S. Slapničar, T. Vuko, M. Čular, M. Drašček, Effectiveness of cybersecurity audit, International Journal of Accounting Information Systems 44 (2022) 100548. doi:https://doi.org/10.1016/j.accinf.2021.100548.

[73] D. C. Latham, Department of defense trusted computer system evaluation criteria, Department of Defense (1986).

[74] E. Commission, D.-G. for the Information Society, Media, Information Technology Security Evaluation Criteria (ITSEC) : Provisional evaluation criteria: Document COM(90) 314, Publications Office, 1992.

[75] Common criteria for information technology security evaluation, Tech. rep., https://www.commoncriteriaportal.org/cc/ (Accessed on 3 February 2022).

[76] T. F. of German Industries (BDI), Cyber-landscape i: Cyber security laws, Tech. rep., https://web.archive.org/web/20210109145510/https://english.bdi.eu/article/news/cyber-security-laws/ (Archived on 9 January 2021).

[77] E. Commission, et al., Communication from the commission on a european programme for critical infrastructure protection, COM (2006) 786 (2006).

[78] Y. Barlette, V. V. Fomin, The adoption of information security management standards: A literature review, Information Resources Management: Concepts, Methodologies, Tools and Applications (2010) 69–90.

[79] R. Leszczyna, I. N. Fovino, M. Masera, Approach to security assessment of critical infrastructures' information systems, IET Information Security 5 (3) (2011) 135–144.

[80] R. Von Solms, Information security management: why standards are important, Information Management & Computer Security (1999).

[81] U. G. A. Office, Critical infrastructure protection: Agencies need to assess adoption of cybersecurity guidance, Tech. rep., https://www.gao.gov/assets/720/718988.pdf (Accessed on 16 February 2022).

[82] M. P. Barrett, et al., Framework for improving critical infrastructure cybersecurity, National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep (2018).

[83] S. P. Marsh, Formalising trust as a computational concept (1994).

[84] J. Kindervag, et al., Build security into your network's dna: The zero trust network architecture, Forrester Research Inc 27 (2010).

[85] R. Anderson, Why information security is hard-an economic perspective, in: Seventeenth Annual Computer Security Applications Conference, IEEE, 2001, pp. 358–365.

[86] K. Rannenberg, It security certification and criteria, in: IFIP International Information Security Conference, Springer, 2000, pp. 1–10.

[87] D. Rice, Geekonomics: The real cost of insecure software, Pearson Education, 2007.

[88] R. Schierholz, K. McGrath, Security certification–a critical review, ISA Automation Week (2010) 156–178.

[89] B. Edelman, Adverse selection in online" trust" certifications, in: Proceedings of the 11th International Conference on Electronic Commerce, 2009, pp. 205–212.

[90] K. Schneider, E. Knauss, S. Houmb, S. Islam, J. Jürjens, Enhancing security requirements engineering by organizational learning, Requirements Engineering 17 (1) (2012) 35–56.

[91] M. Kamalrudin, J. Grundy, Generating essential user interface prototypes to validate requirements, in: 2011 26th IEEE/ACM International Conference on Automated Software Engineering (ASE 2011), IEEE, 2011, pp. 564–567.

[92] M. H. Henry, D. R. Zaret, J. R. Carr, J. D. Gordon, R. M. Layer, Cyber risk in industrial control systems, in: Cyber-security of SCADA and other industrial control systems, Springer, 2016, pp. 133–166.

[93] L. Chung, B. A. Nixon, E. Yu, J. Mylopoulos, Non-functional requirements in software engineering, Vol. 5, Springer Science & Business Media, 2012.

[94] D. Firesmith, Specifying reusable security requirements., J. Object Technol. 3 (1) (2004) 61–75.

[95] C. Haley, R. Laney, J. Moffett, B. Nuseibeh, Security requirements engineering: A framework for representation and analysis, IEEE Transactions on Software Engineering 34 (1) (2008) 133–153.

[96] A. Nhlabatsi, B. Nuseibeh, Y. Yu, Security requirements engineering for evolving software systems: A survey, in: Security-aware systems applications and software development methods, IGI Global, 2012, pp. 108–128.

[97] H. Mouratidis, P. Giorgini, Secure tropos: a security-oriented extension of the tropos methodology, International Journal of Software Engineering and Knowledge Engineering 17 (02) (2007) 285–309.

[98] H. Mouratidis, Secure software systems engineering: the secure tropos approach, J. Softw. 6 (3) (2011) 331–339.

[99] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, J. Mylopoulos, Tropos: An agent-oriented software development methodology, Autonomous Agents and Multi-Agent Systems 8 (3) (2004) 203–236.

[100] A. Van Lamsweerde, Elaborating security requirements by construction of intentional anti-models, in: Proceedings. 26th International Conference on Software Engineering, IEEE, 2004, pp. 148–157.

[101] A. Dardenne, A. Van Lamsweerde, S. Fickas, Goal-directed requirements acquisition, Science of computer programming 20 (1-2) (1993) 3–50.

[102] J. Jürjens, Umlsec: Extending uml for secure systems development, in: International Conference on The Unified Modeling Language, Springer, 2002, pp. 412–425.

[103] A. S. Ahmadian, S. Peldszus, Q. Ramadan, J. Jürjens, Model-based privacy and security analysis with carisma, in: Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, 2017, pp. 989–993.

[104] T. Lodderstedt, D. Basin, J. Doser, Secureuml: A uml-based modeling language for model-driven security, in: International Conference on the Unified Modeling Language, Springer, 2002, pp. 426–441.

[105] L. Lin, B. Nuseibeh, D. Ince, M. Jackson, J. Moffett, Introducing abuse frames for analysing security requirements, in: Proceedings. 11th IEEE International Requirements Engineering Conference, 2003., IEEE, 2003, pp. 371–372.

[106] M. Jackson, Problem frames: analysing and structuring software development problems, Addison-Wesley, 2001.

[107] I. Alexander, Initial industrial experience of misuse cases in trade-off analysis, in: Proceedings IEEE Joint International Conference on Requirements Engineering, IEEE, 2002, pp. 61–68.

[108] G. Sindre, A. L. Opdahl, Eliciting security requirements with misuse cases, Requirements engineering 10 (1) (2005) 34–44.

[109] N. R. Mead, T. Stehney, Security quality requirements engineering (square) methodology, ACM SIGSOFT Software Engineering Notes 30 (4) (2005) 1–7.

[110] G. Georg, I. Ray, K. Anastasakis, B. Bordbar, M. Toahchoodee, S. H. Houmb, An aspect-oriented methodology for designing secure applications, Information and Software Technology 51 (5) (2009) 846–864.

[111] Y. Roudier, M. S. Idrees, L. Apvrille, Improved security requirements engineering using knowledge representation, in: 9ème conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information, 2014.

[112] A. Souag, R. Mazo, C. Salinesi, I. Comyn-Wattiau, Reusable knowledge in security requirements engineering: a systematic mapping study, Requirements Engineering 21 (2) (2016) 251–283.

[113] A. Souag, C. Salinesi, R. Mazo, I. Comyn-Wattiau, A security ontology for security requirements elicitation, in: International symposium on engineering secure software and systems, Springer, 2015, pp. 157–177.

[114] N. I. of Standards, Technology, Fips 200 minimum security requirements for federal information and information systems, Tech. rep. (2006).

[115] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, R. McQuaid, Developing cyber resilient systems: a systems security engineering approach, Tech. rep., National Institute of Standards and Technology (2019).

[116] J. T. F. T. Initiative, Sp 800-30 rev. 1. guide for conducting risk assessments, Tech. rep., National Institute of Standards and Technology (2019).

[117] D. Byers, N. Shahmehri, Graphical modeling of security goals and software vulnerabilities, in: Handbook of Research on Innovations in Systems and Software Engineering, IGI Global, 2015, pp. 1–31.

[118] J. T. Force, T. Initiative, Sp 800-53 rev.5 security and privacy controls for federal information systems and organizations, NIST Special Publication 800 (53) (2020).

[119] J. T. F. T. Initiative, Sp 800-37 rev. 2 risk management framework for information systems and organizations: A system life cycle approach for security and privacy, Tech. rep., National Institute of Standards and Technology (2018).

[120] A. Sunyaev, Healthcare telematics in germany with respect to security issues, in: Health-Care Telematics in Germany, Springer, 2011, pp. 17–52.

[121] K. Beckers, I. Côté, S. Fenz, D. Hatebur, M. Heisel, A structured comparison of security standards, in: Engineering secure future internet services and systems, Springer, 2014, pp. 1–34.

[122] M. L. Hale, R. F. Gamble, Semantic hierarchies for extracting, modeling, and connecting compliance requirements in information

security control standards, Requirements Engineering 24 (3) (2019) 365–402.

[123] R. Baldoni, L. Montanari, Italian cyber security report. a national cyber security framework, Tech. rep., Tech. rep (2015).

[124] S. Yu, Cyber Defense Matrix, https://cyberdefensematrix.com/ (Accessed February 7, 2022).

[125] R. Leszczyna, Standards on cyber security assessment of smart grid, International Journal of Critical Infrastructure Protection 22 (2018) 70–89.

[126] R. E. Carlson, J. E. Dagle, S. A. Shamsuddin, Summary of control system security standards activities in the energy sector, in: United States. Office of Electricity Delivery & Energy Reliability, no. National SADA Test Bed, United States. Office of Electricity Delivery & Energy Reliability, 2005.

[127] C. Alcaraz, S. Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, International journal of critical infrastructure protection 8 (2015) 53–66.

[128] T. Sommestad, G. N. Ericsson, J. Nordlander, Scada system cyber security—a comparison of standards, in: IEEE PES general meeting, IEEE, 2010, pp. 1–8.

[129] G. Lykou, A. Anagnostopoulou, G. Stergiopoulos, D. Gritzalis, Cybersecurity self-assessment tools: evaluating the importance for securing industrial control systems in critical infrastructures, in: International Conference on Critical Information Infrastructures Security, Springer, 2018, pp. 129–142.

[130] C. . I. S. Agency, The Cyber Security Evaluation Tool (CSET), https://us-cert.cisa.gov/ics/Downloading-and-Installing-CSET (Accessed February 7, 2022).

[131] K. Stine, R. Kissel, W. Barker, J. Fahlsing, J. Gulick, Sp 800-60 vol. 1 rev. 1 guide for mapping types of information and information systems to security categories, Tech. rep., National Institute of Standards and Technology (2008).

[132] N. I. of Standards, Technology, Fips 199 standards for security categorization of federal information and information systems, Tech. rep., National Institute of Standards and Technology (2004).

[133] K. A. Lee, Cs2sat: The control systems cyber security self-assessment tool (1 2008).
URL https://www.osti.gov/biblio/924515

[134] C. . I. S. Agency, Cyber resilience review self-assessment package (crr), Tech. rep., Cybersecurity & Infrastructure Security Agency, https://us-cert.cisa.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf (Accessed February 7, 2022).

[135] M. Swanson, J. Hash, P. Bowen, Sp 800-18 rev. 1. guide for developing security plans for federal information systems (2006).

[136] U. G. A. Office, Federal information system controls audit manual (fiscam), Tech. rep., US Government Accountability Office, https://www.gao.gov/assets/gao-09-232g.pdf (Accessed February 7, 2022).

[137] N. B. of Standards, Fips 102 guideline for computer security certification and accreditation (1983).

[138] C. for Internet Security, Cis controls self assessment tool (cis csat), Tech. rep., Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/ (Accessed February 7, 2022).

[139] P. S. S. Council, Payment card industry (pci) data security standard - requirements and security assessment procedures version 3.2.1, Tech. rep., https://www.pcisecuritystandards.org/document_library (Accessed February 7, 2022).

[140] W. Piez, The open security controls assessment language (oscal): schema and metaschema, in: Balisage: The Markup Conference, 2019.

[141] C. P. Team, Cmmi for development, version 1.3, Tech. Rep. CMU/SEI-2010-TR-033, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9661 (Accessed February 7, 2022).

[142] J. D. Gilsinn, R. Schierholz, et al., Security assurance levels: a vector approach to describing security requirements, Other, National Institute of Standards and Technology, Gaithersburg, MD, USA (2010).

[143] E. S. Office of Cybersecurity, E. Response, Cybersecurity capability maturity model (c2m2), Tech. rep., https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf (Accessed February 7, 2022).

[144] S. Tweneboah-Koduah, W. J. Buchanan, Security risk assessment of critical infrastructure systems: A comparative study, The Computer Journal 61 (9) (2018) 1389–1406.

[145] M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger, A. Somani, A review of cybersecurity risk and consequences for critical infrastructure, 2019 Resilience Week (RWS) 1 (2019) 7–13.

[146] Information technology Security techniques Information security risk management, Standard, International Organization for Standardization, Geneva, CH (2011).

[147] M. Al Fikri, F. A. Putra, Y. Suryanto, K. Ramli, Risk assessment using nist sp 800-30 revision 1 and iso 27005 combination technique in profit-based organization: Case study of zzz information system application in abc agency, Procedia Computer Science 161 (2019) 1206–1215.

[148] W. T. Fine, Mathematical evaluations for controlling hazards, Tech. rep., NAVAL ORDNANCE LAB WHITE OAK MD (1971).

[149] H. Joh, Y. K. Malaiya, A framework for software security risk evaluation using the vulnerability lifecycle and cvss metrics, in: Proc. International Workshop on Risk and Trust in Extended Enterprises, Citeseer, 2010, pp. 430–434.

[150] L. A. Cox, Jr, Some limitations of "risk= threat× vulnerability× consequence" for risk analysis of terrorist attacks, Risk Analysis: An International Journal 28 (6) (2008) 1749–1761.

[151] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson, Introducing octave allegro: Improving the information security risk assessment process, Tech. rep., Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst (2007).

[152] J. Freund, J. Jones, Measuring and managing information risk: a FAIR approach, Butterworth-Heinemann, 2014.

[153] G. Giannopoulos, R. Filippini, M. Schimmer, Risk assessment methodologies for critical infrastructure protection. part i: A state of the art, JRC Technical Notes 1 (1) (2012) 1–53.

[154] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart, A review of cyber security risk assessment methods for scada systems, Computers & security 56 (2016) 1–27.

[155] A. Hudaib, R. Masadeh, M. H. Qasem, A. Alzaqebah, Requirements prioritization techniques comparison, Modern Applied Science 12 (2) (2018) 62.

[156] P. Achimugu, A. Selamat, R. Ibrahim, M. N. Mahrin, A systematic literature review of software requirements prioritization research, Information and software technology 56 (6) (2014) 568–585.

[157] P. Babashamsi, A. Golzadfar, N. I. M. Yusoff, H. Ceylan, N. G. M. Nor, Integrated fuzzy analytic hierarchy process and vikor method in the prioritization of pavement maintenance activities, International Journal of Pavement Research and Technology 9 (2) (2016) 112–120.

[158] A. Baykasoğlu, İ. Gölcük, Development of a novel multiple-attribute decision making model via fuzzy cognitive maps and hierarchical fuzzy topsis, Information Sciences 301 (2015) 75–98.

[159] T. L. Saaty, What is the analytic hierarchy process?, in: Mathematical models for decision support, Springer, 1988, pp. 109–121.

[160] C.-L. Hwang, Y.-J. Lai, T.-Y. Liu, A new approach for multiple objective decision making, Computers & operations research 20 (8) (1993) 889–899.

[161] C. W. Churchman, R. L. Ackoff, An approximate measure of value, Journal of the Operations Research Society of America 2 (2) (1954) 172–187.

[162] C. Duan, P. Laurent, J. Cleland-Huang, C. Kwiatkowski, Towards automated requirements prioritization and triage, Requirements engineering 14 (2) (2009) 73–89.

[163] N. Kukreja, S. S. Payyavula, B. Boehm, S. Padmanabhuni, Value-based requirements prioritization: usage experiences, Procedia Computer Science 16 (2013) 806–813.

[164] J. Karlsson, C. Wohlin, B. Regnell, An evaluation of methods for prioritizing software requirements, Information and software technology 39 (14-15) (1998) 939–947.

[165] M. I. Tariq, S. Ahmed, N. A. Memon, S. Tayyaba, M. W. Ashraf, M. Nazir, A. Hussain, V. E. Balas, M. M. Balas, Prioritization of information security controls through fuzzy ahp for cloud computing networks and wireless sensor networks, Sensors 20 (5) (2020) 1310.

[166] K.-Y. Park, S.-G. Yoo, J. Kim, Security requirements prioritization based on threat modeling and valuation graph, in: International Conference on Hybrid Information Technology, Springer, 2011, pp. 142–152.

[167] C. Duan, P. Laurent, J. Cleland-Huang, C. Kwiatkowski, Towards automated requirements prioritization and triage, Requirements engineering 14 (2) (2009) 73–89.

[168] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al., The prisma 2020 statement: an updated guideline for reporting systematic reviews, International Journal of Surgery 88 (2021) 105906.

[169] A. M. T. Thomé, L. F. Scavarda, A. J. Scavarda, Conducting systematic literature review in operations management, Production Planning & Control 27 (5) (2016) 408–420.

[170] H. Cooper, Research synthesis and meta-analysis: A step-by-step approach, Vol. 2, Sage publications, 2015.

[171] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, P. Group*, Preferred reporting items for systematic reviews and meta-analyses: the prisma statement, Annals of internal medicine 151 (4) (2009) 264–269.

[172] The BSI standards. IT-Grundschutz, Standard, German Federal Office for Information Security.

[173] Information Technology Security Techniques Information Security Management Systems Requirements, Standard, International Organization for Standardization, Geneva, CH (2013).

[174] Cyber Assessment Framework (CAF), Tech. rep., National Cyber Security Centre United Kingdom, https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework (Accessed on 3 February 2022).

[175] Information Technology –Security Techniques –Code of Practice for Information Security Controls, Standard, International Organization for Standardization, Geneva, CH (2013).

[176] Iec 62443, Standard, International Electrotechnical Commission, https://webstore.iec.ch/searchform&q=62443 (Accessed on 3 February 2022).

[177] H. N. Eve, Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants, Master's thesis, Tallinn University of Technology, Faculty of Information Technology, Department of Computer Science, Tallinn (2016).

[178] C. Kuligowski, Comparison of it security standards, Masters of Science Information Security and Assurance 65 (2009).

[179] V. Gazis, A survey of standards for machine-to-machine and the internet of things, IEEE Communications Surveys & Tutorials 19 (1) (2016) 482–511.

[180] Information security technology-baseline for classified protection of cybersecurity, Standard, State Administration of Markets and China National Standardization Administration, https://www.chinesestandard.net/Related.aspx/GBT22239-2019 (Accessed on 3 February 2022).

[181] Industrial communication networks - network and system security - part 3-3: System security requirements and security levels, Standard, International Electrotechnical Commission, https://webstore.iec.ch/publication/7033 (Accessed on 3 February 2022).

[182] U. Congress, Federal information security modernization act of 2014, Public Law (2014) 113–283.

[183] U. Congress, The privacy act (p.l. 93-579), Public Law (1974) 93–579.

[184] N. I. of Standards, Technology, Federal information processing standards, Tech. rep., https://csrc.nist.gov/publications/fips (Accessed on 3 February 2022).

[185] N. A. E. R. Corporation, Bulk electric system definition reference document version 3, Tech. rep., https://www.nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf (Accessed February 2, 2022).

[186] N. A. E. R. Corporation, Sanction guidelines of the north american electric reliability corporation, Tech. rep., https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%204B%20effective%2020210119.pdf (Accessed February 2, 2022).

[187] Power systems management and associated information exchange - Data and communications security, Standard, International Electrotechnical Commission, Geneva, CH (2022).

[188] Health Insurance Portability and Accountability Act for Professionals, Standard, U.S. Department of Health and Human Services (1996).

[189] NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity, Standard, National Institute of Standards and Technology (2014).

[190] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. Hahn, NIST SP 800-82 Rev.2 Guide to Industrial Control Systems (ICS) Security, Standard, National Institute of Standards and Technology (2015).

[191] Communication networks and systems for power utility automation, Standard, IInternational Electrotechnical Commission, Geneva, CH (2022).

[192] D. of Homeland Security, Catalog of control systems security: Recommendations for standards developers, Tech. rep., https://www.cisa.gov/uscert/sites/default/files/documents/CatalogofRecommendationsVer7.pdf (Accessed February 7, 2022).

[193] N. I. of Standards, Technology, Nist sp 800-53, revision 5 control mappings to iso/iec 27001, Tech. rep., https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx (Accessed February 7, 2022).

[194] C. Alcaraz, S. Zeadally, Critical control system protection in the 21st century, Computer 46 (10) (2013) 74–83.

[195] R. Sabillon, J. Serra-Ruiz, V. Cavaller, J. Cano, A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (csam), in: 2017 International Conference on Information Systems and Computer Science (INCISCOS), IEEE, 2017, pp. 253–259.

[196] O. of the Under Secretary of Defense for Acquisition & Sustainment, Cyber-security maturity model certification (cmmc), Tech. rep., https://www.acq.osd.mil/cmmc/docs/

CMMC_ModelMain_V1.02_20200318.pdf (Accessed February 7, 2022).

[197] J. F. Carias, M. R. Borges, L. Labaka, S. Arrizabalaga, J. Hernantes, The order of the factors does alter the product: Cyber resilience policies' implementation order, in: Computational Intelligence in Security for Information Systems Conference, Springer, 2019, pp. 306–315.

[198] T. Akinpelu, R. v. Eck, T. Zuva, Maturity models, challenges and open issues, in: Computer Science On-line Conference, Springer, 2021, pp. 110–118.

[199] S. C. Payne, A guide to security metrics, SANS Institute Information Security Reading Room (2006).

[200] P. Abrahamsson, O. Salo, J. Ronkainen, J. Warsta, Agile software development methods: Review and analysis, arXiv preprint arXiv:1709.08439 (2017).

[201] H. A. Simon, Administrative behavior, Simon and Schuster, 2013.

[202] B. W. Boehm, Software Engineering Economics, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 99–150. doi:10.1007/978-3-642-48354-7_5.

[203] M. Howard, S. Lipner, The security development lifecycle, Vol. 8, Microsoft Press Redmond, 2006.

[204] Security for industrial automation and control systems, part 4-1: Product security development life-cycle requirements, Standard, International Electrotechnical Commission, https://webstore.iec.ch/publication/33615 (Accessed on 3 February 2022).

[205] D. Geer, Are companies actually using secure development life cycles?, Computer 43 (6) (2010) 12–16.

[206] S. F. P. Mohamed, F. Baharom, A. Deraman, J. Yahaya, H. Mohd, An exploratory study on secure software practices among software practitioners in malaysia, Journal of Telecommunication, Electronic and Computer Engineering 8 (8) (2016) 39–45.

[207] H. Abdullah, J. Uli, Z. A. Mohamed, et al., Relationship between organizational characteristics and information security knowledge management implementation, Procedia-Social and Behavioral Sciences 123 (2014) 433–443.

[208] E. Siu-Kwong, Yu. modelling strategic relationships for process reengineering, Ph.D. thesis, PhD thesis, University of Toronto (1996).

[209] X. Franch, L. López, C. Cares, D. Colomer, The i* framework for goal-oriented modeling, in: Domain-specific conceptual modeling, Springer, 2016, pp. 485–506.

[210] X. Franch, Incorporating modules into the i* framework, in: International Conference on Advanced Information Systems Engineering, Springer, 2010, pp. 439–454.

[211] A. Herzog, N. Shahmehri, C. Duma, An ontology of information security, International Journal of Information Security and Privacy (IJISP) 1 (4) (2007) 1–23.

[212] G. F. O. for Information Security, Threat catalogue basic threats, Tech. rep., https://enos.itcollege.ee/~valdo/bsieng/en/gstoolhtml/g/g00/g00.html (Accessed February 2, 2022).

Biography

The work in this thesis is a synthesis of a very extensive background, which includes:

(1) The experience acquired working at a university on the topic of information security,

(2) The research conducted as part of the Ph.D. studies, covering various aspects of the information security,

(3) The work done in collaboration with the renowned software vendor, and

(4) The collaboration with researchers from different research areas.

Milan Stojkov received his B.Sc. degree in 2014 and M.Sc. degree in 2015, all in Computing and Control Engineering from the University of Novi Sad, Faculty of Technical Sciences. He is a Ph.D. candidate who started his academic journey as a teaching assistant within the Department of Computing and Control, Faculty of Technical Sciences, the University of Novi Sad in 2015. In parallel with his career in academia, Milan also works with renowned software vendors. This opportunity allows him to combine the different skillsets and focus his expertise on designing and implementing secure software systems. His research interests include: **(1)** information security, **(2)** critical infrastructures, **(3)** edge computing, **(4)** Internet of Things, and **(5)** software architectures.

As part of his Ph.D., Milan has studied secure software engineering methodologies and practices, covering both standard-defined processes and industry-proven methods. His narrow research focus includes security requirements engineering, particularly the analysis of the formal requirements defined by the different standardization bodies such as ISO and NIST.

Through his work at Schneider Electric as a security advisor, he has performed security design analysis on several modules of a complex software system for energy management. He has taken part in dozens of security advisory activities, examining tools, APIs, and 3rd-party components and providing security training for the developers. He was actively involved in introducing and certifying the security development lifecycle, as defined by the IEC 62443-4-1:2018, to the organization. His day-to-day activities include analyzing different standards, security guidelines, and regulations.

List of publications

Part of the work in this thesis has already been published and is listed here for reference:

- Stojkov M, Dalčeković N, Markoski B, Milosavljević B, Sladić G. Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid. Energies. 2021; 14(21):6862. https://doi.org/10.3390/en14216862

Milan has worked on other research topics not directly covered in this thesis throughout his doctoral studies. That work has been published in the following publications:

- Stojkov M, Simić M, Sladić G, Milosavljević B. Traditional and Blockchain-based access control models in IoT: A review, 10. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for Information Systems and Computer Networks, 8-11 March, 2020, pp. 51-55, ISBN 978-86-85525-24-7

- Simić M, Stojkov M, Sladić G, Milosavljević B. CRDTs as replication strategy in large-scale edge distributed system: An overview, 10. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for Information Systems and Computer Networks, 8-11 March, 2020, pp. 46-50, ISBN 978-86-85525-24-7

- Stojkov M, Sladić G, Milosavljević B, Zarić M, Simić M. Privacy concerns in IoT smart healthcare system, 9. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for information systems and computer networks, 10-13 March, 2019, pp. 62-65, ISBN 978-86-85525-24-7

- Simić M, Stojkov M, Sladić G, Milosavljević B, Zarić M. On container usability in large-scale edge distributed system, 9. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for Information Systems and Computer Networks, 10-13 March, 2019, pp. 97-101, ISBN pp.97-101, 2019

- Stojkov M, Simić M, Sladić G, Milosavljević B. Two-step process for secure registration of nodes in IoT systems, 8. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for information systems and computer networks, 11-14 March, 2018, pp. 28-31, ISBN 978-86-85525-22-3

- Simić M, Stojkov M, Sladić G, Milosavljević B. Edge computing system for large-scale distributed sensing systems, 8. International Conference on Information Science and Technology (ICIST), Kopaonik: Society for Information Systems and Computer Networks, 11-14 March, 2018, pp. 36-39

- Stojkov M, Milosavljević B, Sladić G. On the Usability of Access Control Models in IoT, 8. PSU-UNS International Conference on Engineering and Technology - ICET, Novi Sad: University of Novi Sad, Faculty of Technical Sciences, 8-10 June, 2017, pp. 1-4, ISBN 978-86-7892-934-2

- Luburić N, Stojkov M, Savić G, Sladić G, Milosavljević B. Cryptotutor: An educational tool for learning modern cryptography, 14. IEEE International Symposium on Intelligent Systems and Informatics (SISY), Subotica, 29-31 August, 2016, pp. 205-210

- Stojkov M, Gostojić S, Sladić G, Marković M, Milosavljević B. Open Government Data in Western Balkans: Assessment and Challenges, 6. International Conference on Information Science and Technology (ICIST), Kopaonik, 29-2 February, 2016, pp. 58-63

Овај Образац чини саставни део докторске дисертације, односно докторског уметничког пројекта који се брани на Универзитету у Новом Саду. Попуњен Образац укоричити иза текста докторске дисертације, односно докторског уметничког пројекта.

План третмана података

Назив пројекта/истраживања

Модел за праћење усклађености између безбедносних стандарда и приоритизацију захтева у критичним инфраструктурама / Model for Security Cross-Standard Compliance Tracking and Requirement Prioritization in Critical Infrastructure

Назив институције/институција у оквиру којих се спроводи истраживање

а) Факултет техничких наука, Универзитет у Новом Саду

Назив програма у оквиру ког се реализује истраживање

Рачунарство и аутоматика – докторска дисертација

1. Опис података

1.1 Врста студије

Укратко описати тип студије у оквиру које се подаци прикупљају

Докторска дисертација

1.2 Врсте података

а) квантитативни

б) **квалитативни**

1.3. Начин прикупљања података

а) анкете, упитници, тестови

б) клиничке процене, медицински записи, електронски здравствени записи

в) генотипови: навести врсту ________________________________

г) административни подаци: навести врсту _________________________

д) узорци ткива: навести врсту___________________________________

ђ) снимци, фотографије: навести врсту______________________________

е) текст, навести врсту **Актуелна литература у области истраживања**

ж) мапа, навести врсту ____

з) остало: описати ____

1.3 Формат података, употребљене скале, количина података

1.3.1 Употребљени софтвер и формат датотеке:

a) Excel фајл, датотека ___________________

b) SPSS фајл, датотека ___________________

c) PDF фајл, датотека ____________________

d) Текст фајл, датотека ___________________

e) JPG фајл, датотека ____________________

f) Остало, датотека _____________________

1.3.2. Број записа (код квантитативних података)

а) број варијабли ____

б) број мерења (испитаника, процена, снимака и сл.) _______________________

1.3.3. Поновљена мерења

а) да

б) **не**

Уколико је одговор да, одговорити на следећа питања:

а) временски размак између поновљених мера је ________________________________

б) варијабле које се више пута мере односе се на __________________________________

в) нове верзије фајлова који садрже поновљена мерења су именоване као ____________

Напомене: ____

Да ли формати и софтвер омогућавају дељење и дугорочну валидност података?

а) ***Да***

б) Не

Ако је одговор не, образложити ____

____

2. Прикупљање података

2.1 Методологија за прикупљање/генерисање података

2.1.1. У оквиру ког истраживачког нацрта су подаци прикупљени?

а) експеримент, навести тип ____

б) корелационо истраживање, навести тип ____

ц) анализа текста, навести тип **Анализа доступне литературе**

д) остало, навести шта ____

2.1.2 Навести врсте мерних инструмената или стандарде података специфичних за одређену научну дисциплину (ако постоје).

____

____

2.2 Квалитет података и стандарди

2.2.1. Третман недостајућих података

а) Да ли матрица садржи недостајуће податке? Да **Не**

Ако је одговор да, одговорити на следећа питања:

а) Колики је број недостајућих података? ___________________________

б) Да ли се кориснику матрице препоручује замена недостајућих података? Да Не

в) Ако је одговор да, навести сугестије за третман замене недостајућих података

____

2.2.2. На који начин је контролисан квалитет података? Описати

____

____

2.2.3. На који начин је извршена контрола уноса података у матрицу?

____

____

3. Третман података и пратећа документација

3.1. Третман и чување података

3.1.1. Подаци ће бити депоновани у _____________________________________ репозиторијум.

3.1.2. URL адреса ____

3.1.3. DOI ____

3.1.4. Да ли ће подаци бити у отвореном приступу?

а) Да

б) Да, али после ембарга који ће трајати до _______________________________________

в) Не

Ако је одговор не, навести разлог ____

3.1.5. Подаци неће бити депоновани у репозиторијум, али ће бити чувани.

Образложење

____

____

3.2 Метаподаци и документација података

3.2.1. Који стандард за метаподатке ће бити примењен? ____________________________________

3.2.1. Навести метаподатке на основу којих су подаци депоновани у репозиторијум.

____

____

Ако је потребно, навести методе које се користе за преузимање података, аналитичке и процедуралне информације, њихово кодирање, детаљне описе варијабли, записа итд.

____

____

3.3 Стратегија и стандарди за чување података

3.3.1. До ког периода ће подаци бити чувани у репозиторијуму? _______________________

3.3.2. Да ли ће подаци бити депоновани под шифром? Да   Не

3.3.3. Да ли ће шифра бити доступна одређеном кругу истраживача? Да   Не

3.3.4. Да ли се подаци морају уклонити из отвореног приступа после извесног времена?

Да   Не

Образложити

____

____

4. Безбедност података и заштита поверљивих информација

Овај одељак МОРА бити попуњен ако ваши подаци укључују личне податке који се односе на учеснике у истраживању. За друга истраживања треба такође размотрити заштиту и сигурност података.

4.1 Формални стандарди за сигурност информација/података

Истраживачи који спроводе испитивања с људима морају да се придржавају Закона о заштити података о личности *(https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html)* и одговарајућег институционалног кодекса о академском интегритету.

4.1.2. Да ли је истраживање одобрено од стране етичке комисије? Да **Не**

Ако је одговор Да, навести датум и назив етичке комисије која је одобрила истраживање

____

4.1.2. Да ли подаци укључују личне податке учесника у истраживању? Да **Не**

Ако је одговор да, наведите на који начин сте осигурали поверљивост и сигурност информација везаних за испитанике:

а)	Подаци нису у отвореном приступу

б)	Подаци су анонимизирани

ц)	Остало, навести шта

____

____

5. Доступност података

5.1. Подаци ће бити

*а) **јавно доступни***

б) доступни само уском кругу истраживача у одређеној научној области

ц) затворени

Ако су подаци доступни само уском кругу истраживача, навести под којим условима могу да их користе:

____

____

Ако су подаци доступни само уском кругу истраживача, навести на који начин могу приступити подацима:

____

____

5.4. Навести лиценцу под којом ће прикупљени подаци бити архивирани.

____

6. Улоге и одговорност

6.1. Навести име и презиме и мејл адресу власника (аутора) података

Милан Стојков stojkovm@uns.ac.rs

6.2. Навести име и презиме и мејл адресу особе која одржава матрицу с подацима

____

6.3. Навести име и презиме и мејл адресу особе која омогућује приступ подацима другим истраживачима

____