Association for Information Systems

AIS Electronic Library (AISeL)

UK Academy for Information Systems Conference Proceedings 2021

UK Academy for Information Systems

Spring 5-29-2021

Systematic Comparison of Methods in Threat and Risk Analysis of ICT Security in Industry 4.0

Marlene Meyer
University of Hohenheim, marlene.meyer@uni-hohenheim.de

Mareike Schoop
University of Hohenheim, schoop@uni-hohenheim.de

Dominik Schoop
Hochschule Esslingen – University of Applied Sciences, dominik.schoop@hs-esslingen.de

Follow this and additional works at: https://aisel.aisnet.org/ukais2021

Recommended Citation

Meyer, Marlene; Schoop, Mareike; and Schoop, Dominik, "Systematic Comparison of Methods in Threat and Risk Analysis of ICT Security in Industry 4.0" (2021). *UK Academy for Information Systems Conference Proceedings 2021*. 21.
https://aisel.aisnet.org/ukais2021/21

This material is brought to you by the UK Academy for Information Systems at AIS Electronic Library (AISeL). It has been accepted for inclusion in UK Academy for Information Systems Conference Proceedings 2021 by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

SYSTEMATIC COMPARISON OF METHODS IN THREAT AND RISK ANALYSIS OF ICT SECURITY IN INDUSTRY 4.0

Marlene Meyer[1,2], Mareike Schoop[1], Dominik Schoop[2]
1 Information Systems Group 1,
University of Hohenheim,
70599 Stuttgart, Germany
{marlene.meyer, schoop}@uni-hohenheim.de
2 Graduate School,
Hochschule Esslingen – University of Applied Sciences
73732 Esslingen, Germany
{marlene.meyer, dominik.schoop}@hs-esslingen.de

Abstract

Industry 4.0 is the connection of intelligent objects with information technology and thus with the internet. This leads to new fields of application in information technology. To protect intelligent objects security approaches are necessary. Several security standards already exist for ICT, but not for Industry 4.0. The present paper considers standards to conduct threat analysis and risk analysis of ICT security based on a literature review. A catalogue of criteria relevant to such standards for Industry 4.0 is developed which serves as the basis of their evaluation. Thirteen standards are identified as relevant regarding the criteria, among them IT-Grundschutz.

Keywords: ICT Security, Literature Review, TOPSIS, Industry 4.0, Risk Analysis, Threat Analysis

1.0 Introduction

The interconnection between information and communication technology (ICT) and industrial machinery leads to increased confrontation of information security in manufacturing (Rüßmann *et al.*, 2015). This combination of ICT and intelligent objects, such as machines and products, is called Industry 4.0 (Lasi *et al.*, 2014).

The aim of information security is the protection of any type of information, their sources, and the permanent maintenance of a certain safety level. Information security is exposed to continuous changes, therefore, it is essential to manage change actively (Bundesamt für Sicherheit in der Informationstechnik, 2017).

To establish fundamental information security mechanisms, various standards of information security management system (ISMS), such as ISO/IEC 27001, ITIL, and

COBIT, can be used (Bundesamt für Sicherheit in der Informationstechnik, 2017; Bundesamt für Sicherheit in der Informationstechnik, 2008; Susanto *et al.*, 2011).
In this paper, various standards of ISMS and contiguous fields are assessed regarding their support of a threat and risk analysis, which leads to the main research question:

- RQ1: Which well-known standards consider threat and risk analysis in information security?

The objective of this paper is to evaluate standards of information security for Industry 4.0. For this evaluation, a set of well-known criteria is necessary (Vorster and Labuschagne, 2005).

- RQ2: Which criteria can be used to evaluate well-known standards for threat and risk analysis in information security?

The evaluation of standards thus requires a catalogue of criteria to show how the standards deal with threat and risk analysis of information security in Industry 4.0.

- RQ3: Which results are provided with the criteria catalogues regarding to threats and risk analysis in Industry 4.0?

The following section contains theoretical foundations to compare methods in threat and risk analysis of ICT Security. Section 3 describes the methodology of this paper. In section 4, criteria of threat and risk analysis are applied to the identified standards. Finally, the results of the evaluation based on the criteria catalogues show the overall suitability of the standards.

2.0 Theoretical Background

The following section presents theoretical foundations of security in information systems, Industry 4.0, and risk analysis.

2.1 Security in Information Systems

Information security concentrates on the protection of information, their source and permanent maintenance of a certain security level (Bundesamt für Sicherheit in der Informationstechnik, 2020). Information security comprises the fundamental values integrity, confidentiality, and availability (ISO/IEC 27002:2013). Integrity depicts correctness of information. Confidentiality addresses the protection of personal data. Availability describes whether a function is existent and therefore executable as intended. (Bundesamt für Sicherheit in der Informationstechnik, 2020)

International Telecommunication Union (2008, p. 2) defines cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.”
A subset of information security is ICT security, which addresses the protection of collected information and their processing in electronic systems (Bundesamt für Sicherheit in der Informationstechnik, 2017). As Figure 1 depicts, ICT security comprises safety, security, and privacy.

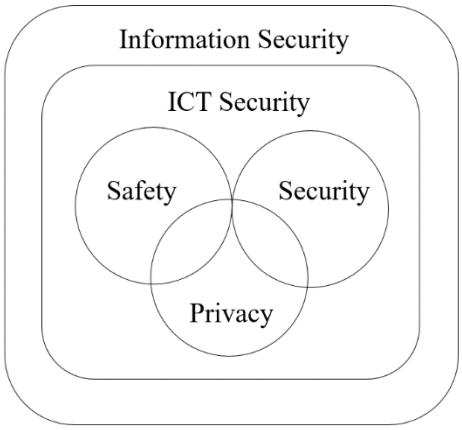

Figure 1. Definition of ICT Security

In automation, safety describes the protection against failures with inadvertent and undesirable behaviour in software or system (Kornecki and Zalewski, 2010). Security involves the protection against intentional attacks on software or system, which violate confidentiality, integrity, and availability (Avižienis *et al.*, 2004; Elmaghraby and Losavio, 2014). This paper focuses on security and on the identification of vulnerabilities but does not consider privacy that concentrates on data protection against third parties (Parent, 1983).

2.2 Industry 4.0

Industry 4.0 is defined as the fourth industrial revolution, that focusses on networking industrial computation systems with physical machines and processes (Lasi *et al.*, 2014). This networking is defined by two development directions: application-pull and technology-push. Application-pull describes changes in society, economics and politics, such as shortening development periods, increasing flexibility, and resource efficiency. Technology-push extends well-known and used technology in private areas

to an industrial context, such as automation, digitalisation, and networking. (Lasi *et al.*, 2014)

Usually, cyber-physical systems (CPS) were utilised to integrate this networking. Whereas CPS do not perform in controlled environments, the robustness of CPS has to be enhanced for them to be able to deal with unexpected states (Lee, 2008).

Industry 4.0 systems are subjected to threats and consequently to risks. A threat is an incident that might cause damage on subjects or objects. In ICT security, threats can cause damages to confidentiality, integrity, and availability, triggered by human misconduct (Bundesamt für Sicherheit in der Informationstechnik, 2020; Eckert, 2018). A risk rates a threat by calculating the product of probability of occurrence and impact of the potential damage. (Bundesamt für Sicherheit in der Informationstechnik, 2020)

2.3 Threats and Risk Analysis

The identification of threats and their rating is necessary to minimise the damage by potential attacks (Peltier, 2005). A structured procedure for identification and rating of these attacks is part of a risk analysis (ISO/IEC 27001:2013).

A threat analysis systematically identifies threats, which can cause damages to an organisation, technical object or user. Potential causes of threats are not only the behavior of a person or an organisation (so called aggressor), but also technical defects. For a complete threat identification, fundamental knowledge about vulnerabilities and security weaknessess of the considered system is required (Eckert, 2018; Peltier, 2005) to determine threats and aggressors. Thus, the results of the threat identification are potential threats and aggressors.

A threat analysis is a component of a risk analysis. A risk analysis determines risk values based on the identified and assessed threats. The risk values are calculated with a likelihood of occurrence of the threat t and an estimated amount of damage d. The value of risk r is defined as follows: $r = d \times t$ (Eckert, 2018; Peltier, 2005).

The estimated likelihood of occurrence consists of an estimated effort and an estimated benefit of a successful attack. To estimate the effort, penetration tests are applied. A penetration test is defined as a simulation of an aggressor's attack behavior to identify potential vulnerabilities and defects of a system (Eckert, 2018).

The estimation of the likelihood of occurrence of threat t comprises the estimated amount of damage d and an estimated value of the vulnerability (Eckert, 2018). The

Common Vulnerability Scoring System (CVSS) determines dependencies among actual properties of the considered vulnerability, index progression of time, and explicit technology infrastructure (FIRST.ORG Inc.). Therefore, the risk analysis is affected by the described model of the aggressor (Eckert, 2018).

The estimated amount of damage a threat can cause consists of primary damage and secondary damage. Primary damages, such as costs of production downtime and recovery, can generally be quantified whereas secondary damages are caused by consideration of long-time effects, such as loss of image (Eckert, 2018).

2.4 Standards for ICT Security

A standard defines a consistent, recognised and established approach. In ICT security, standards depict an approach to protect the digital environment from uncertainty. An established practice-oriented standard of ICT security in Industry 4.0 does not yet exist (Hofmann and Rüsch, 2017; Bundesministerium für Bildung und Forschung). The variety of ICT security standards reveals a large amount of potential standards for ICT security in Industry 4.0, which are evaluated in this paper regarding to their usefulness.

3.0 Methodology

The approach of the methodology is shown in Figure 2 and is broken down into three phases: literature review, criteria catalogues, and evaluation. The literature review considers standards for threat and risk analysis in ICT security. The second phase deals with the development of the criteria catalogue and is subdivided into three subphases, namely definition of criteria for the criteria catalogues, evaluation of the criteria regarding to their relevance, and applying the determined standards of the literature review at the criteria catalogues. The evaluation focuses on the interpretation and rating of the results from the criteria catalogues.

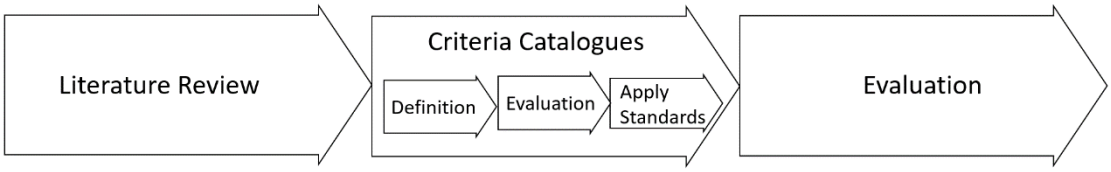

Figure 2. Approach of Methodology

3.1 Literature Review

To identify relevant standards, a literature review was conducted according to Webster and Watson (2002) to evaluate standards regarding to threat and risk analysis of ICT security. To this purpose, standards of ICT security in different subjects, such as ISMS, further common ICT security standards and identified standards of the project IUNO, were examined. The project IUNO is a national reference project that focused on the identifiaction of methods of risk evaluation for ICT security in Industry 4.0. These methods were considered as standards for ICT security and Industry 4.0 (Fraunhofer SIT, 2016; Fraunhofer IESE). Through backward search to these standards (Webster and Watson, 2002), suitability regarding to Industry 4.0 and ICT security was reviewed and further standards were identified. In addition, databases of institutions, authorities, and consortia in the field ICT and contiguous areas, such as engineering, were examined regarding approaches for evaluating risk of ICT systems.

The literature review used the keywords standards, ISMS, risk analysis, threat analysis, ICT security, and the German translations of these terms.

The identified standards are categorised in the categories *open standards*, *fee-based standards*, *practical guidance*, *service management*, and *external provider*. The standards were assigned to the most suited category. Note that the categories are not necessarily distinct. Fee-based standards are mainly international standards, which could be relevant to global institutions. Open standards are partly international and partly national standards, which are freely available and could thus be relevant to institutions with a low budget. Practical guidance is defined as further standards in particular subjects, which describes concrete implementation guidance and concrete threats. Service management includes well-known standards of threat and risk analysis in service management. Standards of external providers describe the implementation of case-specific threat and risk analyses by those providers.

All in all, 62 standards were examined by the literature review. Seven of these standards were excluded beforehand, since these standards were either replaced, withdrawn or only a reference to other standards. The standards ISO/IEC 27001 and ISO/IEC 27002 were collected as ISO/IEC 27000 family. Therefore, only 54 standards were considered further. The mentioned catagories and the related standards are contained in Table 1.

Category	Description	Matching Standards
Open standards	Free access	Common Criteria (ISO/IEC 15408)
		IT-Grundschutz (Bundesamt für Sicherheit in der Informationstechnik, 2020)
		Cyber-Sicherheits-Check (Bundesamt für Sicherheit in der Informationstechnik and ISACA Germany Chapter e.V., 2014)
		Cyber-Sicherheits-Exposition (Allianz für Cyber-Sicherheit, 2018)
		PCIDSS (Payment Card Industry Security Standards Council, 2019)
		VdS 10000
		FitSM (IT Education Management Organisation, o.D.)
		FITSAF (Computer Security Division, 2000)
		NIST SP 800-34 (Swanson *et al.*, 2010)
		NIST SP 800-82 (Stouffer *et al.*, 2015)
		NIST SP 1500-4r2 (National Institute of Standards and Technology, 2019)
		NIST IR 8183A (Stouffer *et al.*, 2019a, 2019b, 2019c)
		NIST IR 8228 (Boeckl *et al.*, 2019)
		NIST IR 8200 (Hogan and Piccarreta, 2018)
Fee-based standards	Predominant ISO, IEC, ISO/IEC	ISO/IEC 27000 family (ISO/IEC 27001:2013; ISO/IEC 27002:2013)
		ISO/IEC 27701:2019
		ISO/IEC 29100:2011
		ISO 31000:2018
		IEC 62443-1-1:2009; IEC 62443-2-1:2010
		IEC 61508-1:2010
Practical guidance	ICT security in industrial automation	NE 153 (NAMUR Working Group WG 4.18 Automation Security, 2015)
		VDI/VDE 2182-1
		VDI/VDE 2182-2.1
		VDI/VDE 2182-2.2
		VDI/VDE 2182-2.3
		VDI/VDE 2182-3.1
		VDI/VDE 2182-3.2
		VDI/VDE 2182-3.3
		VDI/VDE 2182-4
	Method of risk evaluation	CORAS (Lund *et al.*, 2011)
	Context of urban regeneration	Model of Risk Assessment (MORA) (Apollo and Urbańska-Galewska, 2014)
Service management	Standards known from service management	SDL (Microsoft Corporation, 2012)
		ITIL (Limited, 2019)
		COBIT (ISACA, 2018)
		TOGAF (The Open Group)
		MOF (Microsoft Corporation, 2008)
		O-ISM3 (The Open Group, 2017)
External provider	Externals perform analysis	TISAX-Modell (Gleich, 2019)
		VSA Questionnaire (Vendor Security Alliance)

Table 1. Frameworks

3.2 Definition of Criteria Catalogues

After identifying various standards, criteria catalogues were conducted to rate these standards regarding to suitability. These criteria catalogues were used to evaluate in an identical way and on the same level of abstraction. Three catalogues were used:

- *Criteria Catalogue in General*
- *Criteria Catalogue Threat Analysis*
- *Criteria Catalogue Risk Analysis*

The criteria of the criteria catalogues were found via brainstorming. Main criteria of these catalogues are Industry 4.0, ICT security, threat analysis, and risk analysis. The results of a first brainstorming were too generic, hence, further criteria were determined. These criteria were then evaluated as to whether the standards are suitable for threat analysis or for risk analysis. Further, the criteria catalogues evaluate how exactly the regarded standard describes the approach of the analyses.

The *Criteria Catalogue in General* considers no explicit criteria of Industry 4.0 whereas the remaining two criteria catalogues consider criteria of Industry 4.0.

All three criteria catalogues depict the criteria name, provider, and relevance of the regarded standard. The criterion relevance distinguishes the following characteristics:

- *Relevant* for Industry 4.0, ICT security, and threat and risk analysis
- *Possibly later relevant* for Industry 4.0 and/or ICT security, but not to threat and risk analysis
- *Not relevant* for Industry 4.0, ICT security, threat analysis, risk analysis, or a replaced standard

Relevant Standards, which utilise the same approach and receive identical quantitative rating such as sheets of VDI/VDE 2182 are summarised as one standard.

In each criteria catalogues, all as relevant identified standards were ranked based on their relevance and relative closeness and sorted in descending order by the relative closeness with a range of values between 0 (lowest usefulness) and 1 (highest usefulness).

Considered standards, which fulfil the criterion of being not relevant, are either too conceptual, without any Industry 4.0 context or do not describe threat and risk analysis.

Further criteria, which all criteria catalogues contain, are explanation, quantitative rating, and conducted analysis:

- Explanation: The explanation clarifies the result of the criterion relevance. Both criteria of relevance and explanation were considered separately for every criteria catalogue.
- Quantitative rating: This criterion is calculated by the extent of the relevance for the examined standard and is indicated as a relative closeness out of all considered criteria within the regarded criteria catalogue. The relative closeness is calculated based on the TOPSIS approach with a comparison of the positive ideal solution und the negative ideal solution (Hwang and Yoon, 1981) and measure the degree of fulfilment of a standard compared to the criteria.
  As the description of a framework is conceptual and the fulfilment is not just a simple yes or no, following four catagories (adapted by Chen (2000)) were used: non-fulfilment (0), medium fulfilment (3), good fulfilment (7), and very good fulfilment (10).
- Conducted analysis: The criterion conducted analysis distinguishes between standards having their own approach (shown as particular) and standards without (shown as general) for threat and risk analysis.

All criteria catalogues contain specific criteria, which are described in the following.
In the *Criteria Catalogue in General*, the criteria to calculate the quantitative rating are general concepts of threat analysis, general concepts of risk analysis, precise realisations of threat analysis, and precise realisations of risk analysis. All criteria were weighted equally.
The criteria *general concept of threat analysis* and *general concept of risk analysis* are taken as fulfilled, whenever the regarded standard comprises the word risk analysis or threat analysis. If the standard considers a precise concept of threat or risk analysis, the criterion *precise realisation of threat analysis* or *precise realisation of risk analysis* is fulfilled.

Overall, 33 criteria are considered in the *Criteria Catalogue Threat Analysis*. These criteria are summarised into the categories *general criteria*, *safety measures criteria*, *criteria in Industry 4.0*, and *criteria of the infrastructure*. Table 2 lists the categories and their remaining criteria. The categories *safety measures criteria*, *criteria in Industry 4.0*, and *criteria of the infrastructure* comprise sub criteria and, therefore, their values are calculated as a mean of the sub criteria.

Comprised Criteria (Weighting)	Category	Category for Calculation
Consideration of threats (1/5) Approach to identify threats (1/5) Definition of ICT goals (1/5) ICT as an ongoing process (1/5) Safety measures total (1/5)	General criteria	Relative closeness
Safety measures Industry 4.0 (1/2) Safety measures in general (1/2)	Safety measures criteria	Safety measures total (Mean)
Protection cyber physical systems (1/5) Protection IoT (1/5) Protection cloud services (1/5) Protection Big Data (1/5) Protection virtualisation (1/5)	Criteria in Industry 4.0	Safety measures Industry 4.0 (Mean)
Sensitizing employees (1/14) Authentication (1/14) Protection of networks (1/14) Protection office ICT (1/14) Protection production ICT (1/14) Protection of information on data carrier (1/14) Backup (1/14) Protection of remote workplace and sales (1/14) Protection against infected goods (1/14) Protection packaging area (1/14) Protection of products in shipment (1/14) Protection against power outage (1/14) Protection against fire/ water damage (1/14) Protection of business (1/14)	Criteria of the infrastructure	Safety measures in general (Mean)

Table 2: Criteria of Criteria Catalogue Threat Analysis

The criteria safety measures and consideration of threats are determined in the *Criteria Catalogue Risk Analysis*. These two critera were already examined more precisely in the *Criteria Catalogue Threat Analysis*. The criteria consideration of Industry 4.0 threats examine, whether general threats in Industry 4.0 are considered, and summarises the Industry 4.0 criteria of the *Criteria Catalogue Threat Analysis*. Table 3 illustrates further criteria, their related category, and their related category for calculation. The categories *criteria of threats*, *criteria of analysis*, *criteria of calculation*, and *criteria of approach* comprise sub criteria and, hence, their values are calculated as a mean of the sub criteria.

Comprised Criteria (Weighting)	Category	Category for Calculation
General process of risk analysis (1/7) Approach risk identification (1/7) Business impact analysis (1/7) Total threats (1/7) Safety analysis total (1/7) Calculation total (1/7) Approach total (1/7)	General criteria	Relative closeness
Consideration of threats (1/3) Consideration of Industry 4.0 threats (1/3) Safety measures (1/3)	Criteria of threats	Total threats (Mean)
Particular safety analysis for cloud (1/3) Particular safety analysis for IoT (1/3) Particular safety analysis for cyber physical systems (1/3)	Criteria of analysis	Safety analysis total (Mean)
Calculation method (1/2) Necessary variables for calculation (1/2)	Criteria of calculation	Calculation total (Mean)
Periodic internal/ external inspection (1/5) Adequate protection in accordance to the value of the organisation (1/5) Adequate protection in accordance to the importance of the customer (1/5) Reduction of resource consumption of external ICT security provider (1/5) Reduction of resource consumption internal (1/5)	Criteria of approach	Approach total (Mean)

Table 3: Criteria of Criteria Catalogue Risk Analysis

In the criteria catalogues for threat analysis and risk analysis, the *general criteria* category calculates the relative closeness of all main criteria to increase comparability of standard. The overall usefulness of one standard is determined by the calculation of a total relative closeness of all three criteria catalogues.

4.0 Results

This section represents the results of comparing the standards based on criteria catalogues.

4.1 Criteria Catalogue in General

In the criteria catalogue in general only 22 of 54 standards are identified as relevant. Further eight standards are classified as possibly later relevant and 24 standards as not relevant.

Table 4 illustrates a ranking of all relevant standards. The highest value is reached by four standards. The second highest value is reached by IT-Grundschutz; followed by the standards ISO/IEC 27000 family, NIST IR 8183A, MORA, IEC 62443-2-1:2010,

NIST SP 800-82 and TOGAF. The remaining standards reach a relative closeness of less than 0.5.

By considering the criteria *conducted analysis,* nine of the relevant standards have their own approach. Half of the four standards ranked highest have their own approach. IT-Grundschutz, NIST IR 8183A, and NIST SP 800-82 have also their own approach whereas ISO/IEC 27000 family, MORA, IEC 62443-2-1:2010 and TOGAF describe general analyses. Half of the standards with the relative closeness of less than 0.5 are characterised a general analysis.

Rank	Name	Conducted Analysis	Euclidean Distance from Positive Ideal	Euclidean Distance from Negative Ideal	Relative Closeness
1	CORAS	General	0	1.21180448	1
	Cyber-Sicherheits-Exposition	Particular	0	1.21180448	1
	SDL	General	0	1.21180448	1
	VDI/VDE 2182 (1, 2.2, 2.3, 3.3)	Particular	0	1.21180448	1
5	IT-Grundschutz	Particular	0.41043702	0.98808243	0.70652033
6	ISO/IEC 27000	General	0.54664561	0.77164941	0.58533894
	NIST IR 8183A	Particular	0.54664561	0.77164941	0.58533894
8	MORA	General	0.70795684	0.98349744	0.5814508
9	IEC 62443-2-1:2010	General	0.73234841	0.90887173	0.55377807
10	NIST SP 800-82	Particular	0.80477847	0.90598107	0.52957826
	TOGAF	General	0.80477847	0.90598107	0.52957826
12	IEC 62443-1-1:2009	General	1.07185413	0.56533071	0.34530659
	ITIL	Particular	1.07185413	0.56533071	0.34530659
	PCIDSS	General	1.07185413	0.56533071	0.34530659
	VDI/VDE 2182-4	Particular	1.07185413	0.56533071	0.34530659
	VdS 10000	General	1.07185413	0.56533071	0.34530659
17	Cobit 2019	Particular	1.18089407	0.27195456	0.18718712
18	Cyber-Sicherheits-Check	Particular	1.14016845	0.2178551	0.16042071
	MOF	General	1.14016845	0.2178551	0.16042071

Table 4: Results of Criteria Catalogue in General

Having considered the criteria in general, the standards are evaluated regarding the threat analysis.

4.2 Criteria Catalogue Threat Aanalysis

The level of abstraction and the missing context of Industry 4.0 cause only 15 of 54 standards to be classified as relevant. Further six standards were identified as possibly later relevant and overall 33 standards were identified as not relevant.

Table 5 illustrates a ranking of all 15 relevant standards. The highest possible mean value of 1 is reached once, namely by IT-Grundschutz, followed by the standards IEC 62443-2-1:201 and ISO/IEC 27000 family with a relative closeness greater than 0.6. NIST IR 8183A, IEC 62443-1-1:2009, and NIST SP 800-72 reach a relative closeness around 0.43. The remaining standards have a relative closeness of less than 0.4.
Seven of the relevant standards have their own approach. IT-Grundschutz (Rank 1), NIST IR 8183A (Rank 4), and NIST SP 800-82 (Rank 6) have their own approach whereas ISO/IEC 27000 family, IEC 62443-2-1:2010, and IEC 62441-1:2009 describe a general analysis. The remaining standards, with a relative closeness of less than 0.4, are characterised six times as particular and three times as general.

Rank	Name	Conducted Analysis	Euclidean Distance from Positive Ideal	Euclidean Distance from Negative Ideal	Relative Closeness
1	IT-Grundschutz	Particular	0	1.756464291	1
2	IEC 62443-2-1:2010	General	0.73478431	1.328505547	0.64387732
3	ISO/IEC 27000	General	0.8814955	1.337949778	0.60283071
4	NIST IR 8183A	Particular	1.37526707	1.064445029	0.43629944
5	IEC 62443-1-1:2009	General	1.39743441	1.064116483	0.43229514
6	NIST SP 800-82	Particular	1.26881809	0.95159438	0.42856649
7	VDI/VDE 2182-2.3	Particular	1.4348162	0.944194686	0.3968854
8	VDI/VDE 2182-2.2	Particular	1.45607725	0.943824281	0.39327625
9	VDI/VDE 2182-1	Particular	1.48257608	0.941878423	0.38849086
10	VDI/VDE 2182-3.3	Particular	1.43232165	0.835717528	0.36847579
11	SDL	General	1.52199188	0.876759674	0.36550666
12	ITIL	Particular	1.50548655	0.826868428	0.35452083
13	VdS 10000	General	1.37243552	0.725103176	0.3456924
14	Cyber-Sicherheits-Check	Particular	1.52711656	0.689172807	0.31095795
15	CORAS	General	1.5602195	0.65151513	0.29457202

Table 5: Results of Criteria Catalogue Threat Analysis

Having considered the criteria in general and the *Criteria Catalogue Threat Analysis*, the standards will be evaluated regarding the risk analysis.

4.3 Criteria Catalogue Risk Analysis

The level of abstraction and the missing context in Industry 4.0 cause only 15 of 54 standards to be classified as relevant. Further six standards are identified as possibly later relevant and 33 standards are identified as not relevant.

Table 6 illustrates a ranking of all relevant standards. IT-Grundschutz is ranked highest. All other standards reach a relative closeness of less than 0.4. Overall, nine of the relevant standards have their own approach.

Rank	Name	Conducted analysis	Euclidean distance from positive ideal	Euclidean distance from negative ideal	Relative closeness
1	IT-Grundschutz	Particular	0.659519415	1.572547555	0.704525257
2	NIST IR 8183A	Particular	1.400962061	0.891849727	0.388976423
3	IEC 62443-1-1:2009	General	1.431278808	0.854642588	0.373872255
4	ISO/IEC 27000	General	1.443396147	0.742170033	0.339577927
5	CORAS	Particular	1.48311622	0.739291945	0.332653541
6	SDL	Particular	1.470562601	0.706063796	0.324384468
7	ITIL	Particular	1.585101215	0.632144387	0.285103457
8	TOGAF	Particular	1.605954185	0.607783494	0.27455082
9	VDI/VDE 2182-1	Particular	1.610156313	0.606452755	0.273594818
10	Cyber-Sicherheits-Exposition	Particular	1.61805214	0.605968888	0.272465449
11	IEC 62443-2-1:2010	General	1.47779795	0.466171916	0.239804085
12	VDI/VDE 2182 (2.2, 2.3, 3.3)	Particular	1.595475334	0.502729993	0.239599998
13	VdS 10000	General	1.533348761	0.309379269	0.167891986

Table 6: Results of Criteria Catalogue Risk Analysis

4.4 Summary of all Criteria Catalogues

The results of all three criteria catalogues vary regarding the considered standards. Thus, this section compares the results of all of the criteria catalogues with respect to relevance, relative closeness, and conducted analysis.

Table 7 compares all relevant standards of the three criteria catalogues based on their relevance. The usage of a considered standard is defined as conflict-free if the standard is characterised as relevant in all criteria catalogues. In contrast, the usage of a standard is defined as conflictual if at least in one criteria catalogues the standard is characterised as not relevant, such as MORA. Overall, nine standards contain such conflict.

Seven standards, namely Cyber-Sicherheits-Exposition, PCIDSS, COBIT 2019, MOF, TOGAF, VDI/VDE 2182-4, and MORA, are characterised as relevant in the *Criteria Catalogue in General*; whereas these standards are characterised as not relevant in the

Criteria Catalogue Threat Analysis. The standards ISO 31000 and FITSAF are characterised as possibly later relevant in the *Criteria Catalogue in General but* are characterised as not relevant in the *Criteria Catalogue Threat Analysis*.

Seven standards, namely Cyber-Sicherheits-Check, PCIDSS, COBIT 2019, MOF, VDI/VDE 2182-4, NIST SP 800-82, and MORA, are characterised as relevant in the *Criteria Catalogue in General*; whereas these standards are characterised as not relevant in the *Criteria Catalogue Risk Analysis*. The standards ISO 31000 and FITSAF are characterised as possibly later relevant in the *Criteria Catalogue in General*; whereas these standards are characterised as not relevant in the *Criteria Catalogue Risk Analysis*. Reasons for the change of the relevance between the criteria catalogues could be the lack of specific threat or risk descriptions.

Only those standards, which are characterised as relevant in all criteria catalogues, will be considered further. The remaining standards in Table 7 are not relevant to the approach of threat and risk analysis, since a conflict exists.

Name of Standard	Criteria Catalogue in General	Criteria Catalogue Threat Analysis	Criteria Catalogue Risk Analysis	Conflict
Cobit 2019	Relevant	Not relevant	Not relevant	Yes
CORAS	Relevant	Relevant	Relevant	No
Cyber-Sicherheits-Check	Relevant	Relevant	Not relevant	Yes
Cyber-Sicherheits-Exposition	Relevant	Not relevant	Relevant	Yes
IEC 62443-1-1:2009	Relevant	Relevant	Relevant	No
IEC 62443-2-1:2010	Relevant	Relevant	Relevant	No
ISO/IEC 27000	Relevant	Relevant	Relevant	No
IT-Grundschutz	Relevant	Relevant	Relevant	No
ITIL	Relevant	Relevant	Relevant	No
MOF	Relevant	Not relevant	Not relevant	Yes
MORA	Relevant	Not relevant	Not relevant	Yes
NIST IR 8183A	Relevant	Relevant	Relevant	No
NIST SP 800-82	Relevant	Relevant	Not relevant	Yes
PCIDSS	Relevant	Not relevant	Not relevant	Yes
SDL	Relevant	Relevant	Relevant	No
TOGAF	Relevant	Not relevant	Relevant	Yes
VDI/VDE 2182-1	Relevant	Relevant	Relevant	No
VDI/VDE 2182-2.2	Relevant	Relevant	Relevant	No
VDI/VDE 2182-2.3	Relevant	Relevant	Relevant	No
VDI/VDE 2182-3.3	Relevant	Relevant	Relevant	No
VDI/VDE 2182-4	Relevant	Not relevant	Not relevant	Yes
VdS 10000	Relevant	Relevant	Relevant	No

Table 7: Comparison Relevance of all Criteria Catalogues

The relevant standards are now considered in more detail by comparing all criteria catalogues (see Table 8). This comparison is conducted by mean values of all relevant standards. The relative closeness of all three criteria catalogues is calculated as one mean value over all criteria catalogues for a single standard.

The highest relative closeness is reached by IT-Grundschutz, followed by SDL. VDI/VDE 2182 are ranked at positions three, four, five, and seven. VDI/VDE 2182 standards are followed by CORAS and the international standard ISO/IEC 27000, and IEC 62443-2-1:2010. NIST IR 8183A is ranked after the IEC 62443-2-1:201. The lowest relative closeness, smaller than 0.4, is obtained by IEC 62443-1-1:2009, ITIL, and VdS 10000.

To have an additional measure, the standard deviation represents the mismatch among the relevance of all three criteria catalogues. The smaller the mismatch among the relevance, the higher the consistency within the standard with respect to the abstraction level.

Rank	Name	Total Relative Closeness	
		Mean	SD
1	IT-Grundschutz	0.803681863	0.138820275
2	SDL	0.563297043	0.309251637
3	VDI/VDE 2182-1	0.55402856	0.318818829
4	VDI/VDE 2182-2.3	0.545495133	0.327735341
5	VDI/VDE 2182-2.2	0.544292084	0.328284812
6	CORAS	0.542408519	0.323939318
7	VDI/VDE 2182-3.3	0.536025263	0.332271636
8	ISO/IEC 27000	0.509249193	0.120188032
9	IEC 62443-2-1:2010	0.47915316	0.17319633
10	NIST IR 8183A	0.470204936	0.08367296
11	IEC 62443-1-1:2009	0.383824661	0.036203497
12	ITIL	0.328310293	0.030782555
13	VdS 10000	0.28629699	0.083725129

Table 8. Results TOPSIS Method

Further, the standards are examined based on our conducted analysis in the particular criteria catalogues. The standards consider a particular analysis or a general analysis. If a standard considers both types, it should be evaluated which analysis will be conducted. Both types of conducted analysis are considered in SDL and CORAS (see Table 4, Table 5, Table 6). The remaining standards consider either a general analysis or a particular analysis.

5.0 Discussion

This section represents the evaluation of the results of the criteria catalogues. Further, the defined research question will be answered in the subsections and limitations will be outlined.

5.1 Standards in Information System

To answer RQ1 (Which well-known standards consider threat and risk analysis?) 62 standards in various subjects areas were considered. To distinguish between various fields of application, the standards were categorised into open standards, fee-based standards, practical guidance, service management, and external provider. Almost at least one standard was identified in every category as relevant. Several standards do not elaborate on risk analysis. Even fewer standards consider Industry 4.0 in risk analysis. There are no established and practice-oriented standards of threat and risk analysis in Industry 4.0, yet (Hofmann and Rüsch, 2017; Bundesministerium für Bildung und Forschung). Thus, further standards from continuous areas of ICT security were considered. As many relevant standards as possible were determined in a literature review.

Only 13 standards were defined as overall relevant from the three criteria catalogues (see Table 8). The relative closeness of the relevant standards was defined which describes to what extent the criteria are fulfilled. These standards were ranked according to the results of the relative closeness.

IT-Grundschutz as an open standard with practical guidance is the best performer. The second best performer is SDL known from service management; followed by five standards of practical guidance. The first fee-based standard is placed at a lower rank.

The standards show different levels of abstraction. In our evaluation, they were compared on similar abstraction levels which makes the standards comparable. Due to the defined criteria, some well-known standards such as COBIT 2019 were characterised as not relevant. These results are based on the conduct of threat and risk analysis in Industry 4.0 and thus do not question the quality of the standards themselves.

5.2 Criteria to Evaluate Standards

Answering RQ2 (Which criteria are used to evaluate the standards?), several criteria were defined. To increase transparency, several criteria were summarised to a main topic, such as *criteria in Industry 4.0*, *criteria of threats*, and *criteria of analysis*.

The criteria of the criteria catalogues were verified regarding to their quality by the adaption of quality criteria of the requirements engineering (Ebert, 2014; Denger and Olsson, 2005). The focus on the quality check is the comparison of the criteria in various criteria catalogues.

The criteria relevance and quantitative rating evaluate the standards regarding to their importance, which constitutes the necessity of the criteria (Ebert, 2014).

To verify the criteria catalogues various criteria were evaluated in more than one criteria catalogue. The criteria *consideration of threats*, *consideration of Industry 4.0 threats*, and *safety measures* were considered in both *Criteria Catalogue Threat Analysis* and *Criteria Catalogue Risk Analysis*. These criteria are identical regarding to their content and characteristics and, therefore, satisfy the quality criteria consistency and unambiguousness (Ebert, 2014; Denger and Olsson, 2005).

The *Criteria Catalogue in General* already considers whether the standards describe a threat analysis and a risk analysis in general. The *Criteria Catalogue Threat Analysis* specifies in particular whether and to what extent the standard considers a threat analysis; the same procedure applies to risk analysis. The remaining criteria are identical with respect to their content and characteristics and thus satisfy the quality criteria consistency and unambiguousness (Ebert, 2014; Denger and Olsson, 2005).

The *Criteria Catalogue Threat Analysis* considers various criteria regarding specific threats, e.g. Industry 4.0 threats. These criteria evaluate the relevance of the considered standard and are therefore relevant regarding to the quality criteria (Ebert, 2014).

The *Criteria Catalogue Risk Analysis* considers various criteria, such as approach to identify risk, consider threats, and calculate risk values. These criteria evaluate the relevance of the considered standard and thus are relevant regarding to the quality criteria (Ebert, 2014).

5.3 Evaluation the Criteria Catalogues

To answer RQ3 (Which results are provided with the criteria catalogues?), the results of the three criteria catalogues were summarised and evaluated. Overall, only 13 standards can be characterised as relevant in all criteria catalogues.

By using TOPSIS, the relative closeness of a standard to the criteria in the criteria catalogues were calculated. The results of the standards in the single criteria catalogues varied (see Table 4, Table 5, Table 6).

To evaluate the relevance of a standard, a total relative closeness was calculated from the relative closeness of all criteria catalogues. The total relative closeness is calculated as a mean value of the relative closeness of the criteria catalogues. The results show that both, mean and standard deviation, of the relative closeness vary significantly.

IT-Grundschutz reaches the best relative closeness by far with a value of around 0.8 and a standard deviation of around 0.13. IT-Grundschutz is characterised as practice-oriented and particular. Further, IT-Grundschutz is edited annually and already considers security in Industry 4.0 components (Bundesamt für Sicherheit in der Informationstechnik, 2020). However, IT-Grundschutz does not provide any calculation methods for risk analysis but describes concrete measures to reduce risk.

IT-Grundschutz is followed by SDL with a significant discrepancy between the total relative closeness of around 0.26 and the standard deviation. This standard is around the medium value and, therefore, the criteria are fulfilled as on a medium level. Furthermore, the standard deviation indicates a mismatch of the usefulness rated in the single criteria catalogues. SDL and CORAS use both general and particular analyses. Therefore, two analyses have to be conducted. CORAS is ranked on position six with a relative closeness of around 0.54.

Rank three to five and seven are taken by the relevant VDI/VDE 2182 standards. These standards are very similar; hence, the relative closeness and the standard deviation are not distinct. However, the standard deviation of these standards shows the greatest value of all fourteen considered standards. Consequently, the criteria demonstrate an inconsistent abstraction level within the standard.

The international standards, ISO/IEC 27000 and IEC 62443-2-1:2010 are located in the second half of the ranking. These standards define generic approaches for threat and risk analysis; hence, the criteria of particular threats and risk specification are not fulfilled. The relative low standard deviations of these standards are clarified by the consistent abstraction level within the standard.

NIST IR 8183A specifies a particular analysis and a specific method to calculate risk. Further approaches are partially linked to other documents (Stouffer *et al.*, 2015; Stouffer et al. 2019a). The relative low standard deviation demonstrates a consistent partial fulfilment within the standard.

IEC 62443-1-1:2009, ITIL, and VdS 10000 reach the lowest standard deviation but also the lowest relative closeness with values lower than 0.4.

The first seven standards contain at least a partial particular analysis. Hence, standards with at least a partial particular analysis perform better than standards with a general analysis. This is due to the more specific description of the approach and examples of threats and risks.

The *Criteria Catalogue in General* shows on a general level whether threat and risk analysis are considered. The actual usefulness of the standards is considered in the two remaining criteria catalogues.

Especially the relative closeness of seven standards in the *Criteria Catalogue Risk Analysis* is less than 0.3. Hence, these standards are limited in their support for a risk analysis and other approaches have to be applied.

Furthermore, only a few standards consider Industry 4.0. None of the international ISO, IEC, and ISO/IEC standards considers methods for a precise approach. Therefore, further approaches have to be searched to identify threats and perform a risk analysis.

IT-Grundschutz considers precise security measures, also for Industry 4.0, and it is updated annually. Hence, IT-Grundschutz is the most suitable standard.

5.4 Limitations

The literature review strives to adapt all relevant and well-known standards to conduct threat and risk analysis. Since there are no established standards for Industry 4.0 and threats and risk analysis as yet, standards will be adjusted or generated in the future.

Standards often require additional documents to be applied to the approach. Therefore, related standards and the corresponding documents should be evaluated together.

The standards were evaluated based on a generic use case considering Industry 4.0. Based on the relevance of the standards to a particular organisation the criteria catalogues should be evaluated regarding to specific requirements of the considered organisation.

6.0 Conclusion

A literature review was conducted to obtain an overview of various standards with the utilisation of threat and risk analysis in Industry 4.0. All in all, 62 standards were considered.

Criteria catalogues were created and standards were applied to the criteria catalogues to evaluate them. To have a quantitative measure of the standards fulfilling the criteria from all three catalogues, the TOPSIS method was used to calculate the degree of relevance as relative closeness. The results of the criteria catalogues were summarised and ranked according to the degree of relevance.

Thirteen standards remained as relevant of all considered standard. The highest ranked standard and the only standard that considers Industry 4.0, is IT-Grundschutz. Even IT-Grundschutz does not completely fulfil the criteria, since this standard does not consider methods to calculate risk.

Future research must develop a literature-based approach for standards with a general analysis. Furthermore, the identified standards must be applied in practice and their degree of suitability must be applied in practical scenarios. Based on these results, a generic standard for risk and threats analysis in Industry 4.0 can be designed.

7.0 References

Allianz für Cyber-Sicherheit (2018) *Cyber-Sicherheits-Exposition,* 2nd ed., available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_013.pdf?__blob=publicationFile&v=1 (accessed 4 February 2021).

Apollo, M. and Urbańska-Galewska, E. (2014) *Model of Risk Assessment (MORA) concept for the investment part of urban regeneration projects,* In Proceedings of The 9th International Conference Environmental Engineering 2014, Vilnius, Lithuania.

Avižienis, A., Laprie, J.-C. and Randell, B. (2004) *Dependability and Its Threats: A Taxonomy*, In Advances in Building the Information Society (Eds. Jacquart, R.), *IFIP International Federation for Information Processing*, 156, Springer US, Boston, MA, pp. 91–120.

Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K.N., Nadeau, E., O'Rourke, D.G., Piccarreta, B. and Scarfone, K. (2019) *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228.

Bundesamt für Sicherheit in der Informationstechnik (2008) *BSI-Standard 100-4: Business Continuity Management*.

Bundesamt für Sicherheit in der Informationstechnik (2017) *BSI-Standard 200-1: Information Security Management Systems (ISMS)*.

Bundesamt für Sicherheit in der Informationstechnik (2020) IT-Grundschutz-Compendium, Unternehmen und Wirtschaft, Reguvis Bundesanzeiger Verlag; Bundesanzeiger Verlag, Köln.

Bundesamt für Sicherheit in der Informationstechnik and ISACA Germany Chapter e.V. (2014) *Leitfaden Cyber-Sicherheits-Check: Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden*, Bonn, available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/leitfaden_CSC_v2.pdf?__blob=publicationFile&v=1 (accessed 4 February 2021).

Bundesministerium für Bildung und Forschung Sichere Industrie 4.0 in der Praxis, available at: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/i40 (accessed 28 May 2020).

Chen, C.-T. (2000) *Extensions of the TOPSIS for group decision-making under fuzzy environment*, Fuzzy Sets and Systems, 114 1 1–9.

Computer Security Division (2000) *Federal Information Technology Security Assessment Framework: Prepared for Security, Privacy, and Critical Infrastructure Committee*, available at: https://csrc.nist.gov/CSRC/media/Publications/white-paper/2000/11/28/federal-information-technology-security-assessment-framework/final/documents/Federal-IT-SAF-2000.pdf (accessed 30 March 2020).

Denger, C. and Olsson, T. (2005) *Quality Assurance in Requirements Engineering*, In Advances in Engineering and Managing Software Requirements (Eds. Aurum, A., Wohlin, C.), 12, Springer-Verlag, Berlin/Heidelberg, pp. 163–185.

Ebert, C. (2014) Systematisches Requirements Engineering: Anforderungen ermitteln, spezifizieren, analysieren und verwalten, 5. überarbeitete Auflage, dpunkt Verlag, Heidelberg.

Eckert, C. (2018) IT-Sicherheit: Konzepte - Verfahren - Protokolle, 10. Auflage, De Gruyter, Berlin/Boston.

Elmaghraby, A.S. and Losavio, M.M. (2014) *Cyber security challenges in Smart Cities: Safety, security and privacy*, Journal of advanced research, 5 4 491–497.

FIRST.ORG Inc. *CVSS: Common Vulnerability Scoring System version 3.1*, Specification Document, 1st ed., available at: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (accessed 4 June 2020).

Fraunhofer IESE IUNO - National Reference Project for IT Security in Industry 4.0, available at: https://www.iese.fraunhofer.de/en/innovation_trends/industrie40/iuno.html (accessed 15 January 2021).

Fraunhofer SIT (2016) *Risikomodell für Wertschöpfungsnetzwerke der Industrie 4.0*, IUNO – Nationales Referenzprojekt IT-Sicherheit in Industrie 4.0.

Gleich, F. (2019) *TISAX Participant Handbook: Getting through the TISAX assessment process and sharing assessment results with your partners,* 2.1.2nd ed.

Hofmann, E. and Rüsch, M. (2017) *Industry 4.0 and the current status as well as future prospects on logistics*, Computers in Industry, 89 1 23–34.

Hogan, M. and Piccarreta, B. (2018) *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, NISTIR 8200.

Hwang, C.-L. and Yoon, K. (1981) *Methods for Multiple Attribute Decision Making*, In Advances in Multiple Attribute Decision Making (Eds. Beckmann, M., Künzi, H. P., Hwang, C.-L., Yoon, K.), *Lecture Notes in Economics and Mathematical Systems*, 186, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 58–191.

IEC 61508-1:2010 (2010) *Functional safety of electrical/ electronic/ programmable electronic safety-related systems*: Part 1: General requirements.

IEC 62443-1-1:2009 (2009) *Industrial communication networks - Network and system security*: Part 1-1: Terminology, concepts and models.

IEC 62443-2-1:2010 (2010) *Industrial communication networks - Network and system security*: Part 2-1: Establishing an industrial automation and control system security program.

International Telecommunication Union (2008) *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY: Telecommunication security - Overview of cybersecurity,* Recommendation, available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (accessed 22 December 2020).

ISACA (2018) COBIT 2019 Framework: Introduction and Methodology, ISACA, Schaumburg, IL, USA.

ISO 31000:2018 (2018) *Risk Management*: Guidelines.

ISO/IEC 15408 (2017) *Common Criteria for Information Technology Security Evaluation*.

ISO/IEC 27001:2013 (2013) *Information technology — Security techniques — Information security management systems*: Requirements.

ISO/IEC 27002:2013 (2013) *Information technology — Security techniques*: Code of practice for information security controls.

ISO/IEC 27701:2019 (2019) *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*: Requirements and guidelines.

ISO/IEC 29100:2011 (2011) *Information technology — Security techniques*: Privacy framework.

IT Education Management Organisation (o.D.) FITSM PARTS, available at: https://www.fitsm.eu/fitsm-parts/ (accessed 4 June 2020).

Kornecki, A.J. and Zalewski, J. (2010) *Safety and security in industrial control,* In Proceedings of the Sixth Annual Workshop, Oak Ridge, Tennessee, ACM Press, New York, New York, USA, p. 1.

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T. and Hoffmann, M. (2014) *Industry 4.0*, Business & Information Systems Engineering, 6 4 239–242.

Lee, E.A. (2008) *Cyber Physical Systems: Design Challenges,* In Proceedings of 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, Orlando, FL, USA, IEEE, pp. 363–369.

Limited, A. (2019) ITIL Foundation ITIL 4 edition: ITIL 4, The Stationery Office Ltd, London.

Lund, M.S., Solhaug, B. and Stølen, K. (2011) Model-Driven Risk Analysis: The CORAS Approach, Springer-Verlag Berlin Heidelberg, Berlin, Heidelberg.

Microsoft Corporation (2008) *Microsoft Operations Framework: MOF Overview,* 4th ed.

Microsoft Corporation (2012) *Security Development Lifecycle: SDL Process Guidance Version 5.2,* 5.2nd ed.

NAMUR Working Group WG 4.18 Automation Security (2015) *Automation Security 2020: Design, Implementation and Operation of Industrial Automation Systems*, NE 153, Leverkusen.

National Institute of Standards and Technology (2019) *NIST Big Data Interoperability Framework*, NIST Special Publication 1500-4r2, 3rd ed.

Parent, W.A. (1983) *Privacy, Morality, and the Law*, Wiley, pp. 269–288.

Payment Card Industry Security Standards Council (2019) *Software Security Framework Secure Software Standard: Program Guide,* 1st ed.

Peltier, T.R. (2005) Information Security Risk Analysis, CRC Press, Hoboken.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P. and Harnisch, M. (2015) *Industry 4.0: The Future of Productivity and Growth in Manufactoring Industries*.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015) *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*, NIST Special Publication 800-82 Revision 2.

Stouffer, K., Zimmerman, T., Tang, C., Cichonski, J., Pease, M., Shah, N. and Downard, W. (2019a) *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance*, NISTIR 8183A Volume 1.

Stouffer, K., Zimmerman, T., Tang, C., Cichonski, J., Pease, M., Shah, N. and Downard, W. (2019b) *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case*, NISTIR 8183A Volume 2.

Stouffer, K., Zimmerman, T., Tang, C., Cichonski, J., Pease, M., Shah, N. and Downard, W. (2019c) *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case*, NISTIR 8183A Volume 3.

Susanto, H., Almunawar, M.N. and Tuan, Y.C. (2011) *Information Security Management System Standards: A Comparative Study of the Big Five*, International Journal of Electrical & Computer Sciences IJECS-IJENS, 11 5 23-29.

Swanson, M., Bowen, P., Phillips, A.W., Gallup, D. and Lynes, D. (2010) *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Rev. 1.

The Open Group Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group, available at: https://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html (accessed 4 June 2020).

The Open Group (2017) *Open Information Security Management Maturity Model*, O-ISM3, 2nd ed.

VDI/VDE 2182-1 (2011) *IT-security for industrial automation*: General model.

VDI/VDE 2182-2.1 (2013) *IT-security for industrial automation*: Example of use of the general model for device manufacturer in factory automation - Programmable logic controller (PLC).

VDI/VDE 2182-2.2 (2013) *IT-security for industrial automation*: Example of use of the general model in factory automation for plant and machinery installers - Forming press.

VDI/VDE 2182-2.3 (2013) *IT-security for industrial automation*: Example of use of the general model for plant managers in factory automation - Stamping plant.

VDI/VDE 2182-3.1 (2013) *IT-security for industrial automation*: - Example of use of the general model for manufacturers in factory automation - Process control system of an LDPE plant.

VDI/VDE 2182-3.2 (2013) *IT-security for industrial automation*: Example of use of the general model for integrators in process industry - LDPE reactor.

VDI/VDE 2182-3.3 (2013) *IT-security for industrial automation*: Example of use of the general model for plant managers in process industry - LDPE-plant.

VDI/VDE 2182-4 (2018) *IT-security for industrial automation*: Recommendations for the implementation of security properties for components, systems, and equipment.

VdS 10000 (2018) *Information Security Management System for SMEs*: Requirements.

Vendor Security Alliance How it works, available at: https://www.vendorsecurityalliance.org/#howItWorks (accessed 30 March 2020).

Vorster, A. and Labuschagne, L. (2005) *A framework for comparing different information security risk analysis methodologies*.

Webster, J. and Watson, R.T. (2002) *Analyzing the Past to Prepare for the Future: Writing a Literature Review*, MIS Quarterly, 26 2 xiii–xxii.