 doi:10.20944/preprints201904.0133.v1

University of Oxford

Cyber Risk Management for the Internet of Things

Petar Radanliev[1], David Charles De Roure[1], Jason R.C. Nurse[2], Pete Burnap[3], Eirini Anthi[3], Uchenna Ani[4], La'Treall Maddox[5], Omar Santos[5], Rafael Mantilla Montalvo[5]

[1]Oxford e-Research Centre, Department of Engineering Sciences, University of Oxford, UK; [2]School of Computing, University of Kent, UK; [3]School of Computer Science and Informatics, Cardiff University; [4]STEaPP, Faculty of Engineering Science, University College London; [5]Cisco Research Centre, Research Triangle Park, USA

Corresponding author: Petar Radanliev: petar.radanliev@oerc.ox.ac.uk [1*]

Abstract: The Internet-of-Things (IoT) enables enterprises to obtain profits from data but triggers data protection questions and new types of cyber risk. Cyber risk regulations for the IoT however do not exist. The IoT risk is not included in the cyber security assessment standards, hence, often not visible to cyber security experts. This is concerning, because companies integrating IoT devices and services need to perform a self-assessment of its IoT cyber security posture. The outcome of such self-assessment need to define a current and target state, prior to creating a transformation roadmap outlining tasks to achieve the stated target state. In this article, a comparative empirical analysis is performed of multiple cyber risk assessment approaches, to define a high-level potential target state for company integrating IoT devices and/or services. Defining a high-level potential target state represent is followed by a high-level transformation roadmap, describing how company can achieve their target state, based on their current state. The transformation roadmap is used to adapt IoT risk impact assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart model. The main contributions from this paper represent a transformation roadmap for standardisation of IoT risk impact assessment; and transformation design imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach. Verified by epistemological analysis defining a unified cyber risk assessment approach. These can be used for calculating the economic impact of cyber risk; for international cyber risk assessment approach; for quantifying cyber risk; and for planning for impact of cyber-attacks, e.g. cyber insurance. The new methods presented in this paper for applying the roadmap include: IoT Risk Analysis through Functional Dependency; Network-based Linear Dependency Modelling; IoT risk impact assessment with a Goal-Oriented Approach; and a correlation between the Goal-Oriented Approach and the IoTMM model.

Keywords: Functional Dependency; Network-based Linear Dependency Modelling; Internet of Things; Micro Mart model; Goal-Oriented Approach; Transformation Roadmap; Cyber risk regulations; Empirical Analysis; cyber risk self-assessment; cyber risk target state.

1. Introduction

Economic impact of Internet-of-Things (IoT) cyber risk is increasing with the integration of digital infrastructure in the digital economy [1]. Cyber security standardisation and regulation

 doi:10.20944/preprints201904.0133.v1

would play a key role in the process of reducing cyber-attacks while continuing to harness the economic values.

The cyber risk from IoT devices is present across different and sometimes at a higher level in sectors where such risk is unexpected. For example, in the US, healthcare is now the largest target of cyber security attacks, reportedly at greater risk than manufacturing and banking [2]. According to the same report [2], the value of stolen personal health information is ten to twenty times greater than the value of a stolen credit card number. To understand and define a generic target state for cyber maturity, we need to understand the business context and the cyber risk priorities through discussions between cyber security experts and decision makers [3].

This research article conducts epistemological analysis focused on understanding the best approach for increasing safety, security and economic value in the IoT space. Our research has two objectives. To identify and capture a detailed target state for the mitigation of cyber risk vectors from the IoT, and to adapt existing cyber security practices and standards to include IoT cyber risk in a high-level cyber security transformation roadmap. We discuss and expand on these further in the remainder of this article. In Section 2 we present the research methodology.

2. Methodology

There is a strong interest in regulating the cyber risk assessment procedures. Regulation and standardisation of cyber security frameworks, models and methodologies has not been done until present. Standardisation in this article refers to the compounding of knowledge to advance the efforts on integrating cyber risk standards and governance, and to offer a better understanding of cyber risk assessments. Here we combine literature analysis with epistemological analysis, and an empirical with a comparative analysis. The empirical analysis is conducted with seven cyber risk frameworks and two cyber risk models. The comparative analysis engages with fifteen high-tech national strategies.

The research firstly identifies the best approach to define a target state according to existing cyber security models. Secondly, the methodology compares the high-profile target state with the main cyber security frameworks to design a high-level transformation roadmap, describing how IoT companies can achieve the target state based on their current state. The transformation roadmap is based on comparing the target state with recommendations from the main cyber security frameworks, and the most recent cyber security literature on this subject. The results of the research outline a detailed target state and a high-level cyber security transformation roadmap.

The methodology of the research article is structured in the following format. In Section 3 we conduct literature analysis. In section 4 through epistemological analysis we seek to probe the current understanding of cyber risk impact assessment. With epistemological analysis, we evaluate the design principles by conducting theoretical evaluation to uncover the best method to define a unified cyber risk assessment. In section 5 we propose cyber risk target state for the IoT vectors, by conducting a comparative empirical research on national IoT strategies and cyber risk assessment frameworks, methods and quantitative models. The literature analysis and the comparative empirical research examine the emerging IoT technologies and we propose design principles to define a transformation roadmap for standardisation of IoT risk impact assessment. In section 6 we evaluate the design principles with case study research od secondary and primary data and we populate the design principles of the transformation roadmap with transformation imperatives. To organise the case study data, we apply the controlled convergence with a goal-oriented approach. In section 7 the transformational roadmap framework and the transformation imperatives are

used to adapt IoT risk impact assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart model and we discuss the new impact assessment principles. In Section 8 we discuss the findings. In Section 10 we present the conclusions and limitations of the research.

3. Current state of cyber risk

Current state of cyber risk concerns are beyond the machine to machine risk [4,5], even further than the cyber physical systems risk [6]. Current cyber risk trends are based on intelligent manufacturing equipment [1,7–10]. Followed by risk trends from artificial intelligence, the cloud, and IoT [4,9,11,12]. This creates risk from systems of machines capable of interacting with the cyber-physical world [1,13–18].

The cyber risk impact analysis faces technical assessment challenges from software defined networks [19] and storage [20], cloud hosting [15], and mesh networks [21]. The integration of such technologies creates cyber security risk, e.g. integrating less secured systems [15] in manufacturing [22]. Existing cyber risk assessment models [23–29] ignore the risk impacts of sharing infrastructure [22,24,25,30,31] and the cyber risk estimated loss range variously [22,24,25,32,33]. To analyse cyber risk, the impact assessment need to evaluate risk from cloud technologies [9,13,34–38]; internet-based system and service oriented architecture [10,37–43] and IoT processes and services [14,44–48] and (4) machine decision making [9,13,37,49].

Further cyber risk assessment challenges emerge from compiling of connected systems [50–52] devices [9,49] and platforms [5,53], in manufacturing [37,38,54,55]. The machines are becoming social CPS [1,36,49] operating as real-time [51,56,57] IoT systems of systems [8,43]. The real-time IoT technology [46] creates cyber risk from data in transit [22,31,49,58–62]. This requires standardisation of design and process [25,63] because such system security is complex [64–66]. The cyber risk assessment need to be integrated in the businesses [36] and cyber strategy [30,67–70] assessing heterogeneous IoT technologies [25,71] supported by cloud computing techniques [72]. This evolution of cyber risks is specifically concerning for small and medium sized enterprises (SME's). The large enterprises have the recourses to control the entire supply chain, while SME's frequently have to integrate their supply chain operations [73,74]. Integrating multiple SME's in the supply chain requires higher visibility and coordination between participants [75,76].

4. Epistemological analysis to uncover the best method to define a unified cyber risk assessment

The colour coding in the NIST framework traffic light protocol [77], represent conventional abstractions or in CVSS [78] a mathematical approximation. In in CVSS [78] a modified attack vector is allocated to a numerical value of 0.85 for a network metric value, and a numerical value of 0.62 for adjacent network metric value [79]. The question is why 0.85 and why 0.62 and why red represents information not for disclosure [77]. These units of measurement in effect represent symbols with a defined set of rules in a conventional system, where truths about their validity can be derived from expert opinions, hence proven to be correct. These units of measurement do not, however, represent quantitative units based on statistical methods for predicting uncertainty.

The examples represent a conventional system where symbols are based on true or false, right or wrong. But the rules in the examples describe an ethical system, where the absolute true or false is hard and almost impossible to verify. For example, in the above described scenario, the number values of 0.85 or 0.62, are not based on probabilistic data. The allocated numbers

 doi:10.20944/preprints201904.0133.v1

emerge from an assessment, which is based on multiple statements from experts, but the experts do not claim that these numbers are representative of the attack vectors. It seems more appropriate for the described examples to be perceived as ethical systems, where validity is conditional and output is presented as better or worse, in the form of a colour coded system (e.g. NIST). This is the best result that can be obtained from ethical analysis, where ethical decisions cannot represent sums. Logical proofs are not a valid way of deriving ethical verification. Instead, ethical decisions can be weighted. The alternative is to conduct quantitative assessment, based on established statistical and mathematical methods and probabilistic data.

This analysis can be confirmed by comparing knowledge with understanding. Knowledge in this scenario, refers to the knowledge that red represents information not for disclosure and a numerical value of 0.62 is allocated for adjacent network metric value. Understanding requires that such knowledge can be applied in a meaningful way. But the numerical value of 0.62 does not represent a measurement unit for cyber risk for all adjacent network. Such numerical value would be case-specific and depend on many other factors that the proposed conventional systems are not designed to understand.

Knowledge requires 'truth, belief and justification' as individual conditions [80]. Knowledge that a numerical value of 0.62 is 'true' metric value for adjacent network, as the related CVSS approach 'believes', needs to be 'justified' to confirm it does not represent just a guess of luck. Since a numerical value. Justification needs to be based on evidentialism [81,82], where a proposition e.g. numerical value of 0.62, is epistemically justified as determined entirely by evidence. The debate whether cyber risk standards can be epistemically justified, must be based on the facts and evidence currently available. In evidentialism, epistemic evaluations are separate from moral believes and practical assessments, as epistemically justified evaluations might conflict with moral and practical estimations [81].

Analysing the cyber risk assessment approaches with evidentialism is not intended to discard the validity of these standards. Quite the opposite, evidentialism theory includes justified beliefs and experiences as evidence and the prior analysis in this article argues that current cyber risk standards do have knowledge level justification. The argument is that the knowledge level justification of the discussed cyber risk assessment standards, seem to be based on other externalist theories such as reliabilism [83,84]. This is confirmed with presenting numerical values (e.g. 0.62) represented as metric values, despite the lack of quantitative evidence or other conditions that justify such knowledge. Most cyber security standards follow the reliabilists theory where a cyber risk assessment process can be justified and constitute knowledge, even if the process that makes the assessment reliable is not understood. This is known as the generality problem [84], where a given justification of knowledge can also be identified with different and concurrently operating processes, which may, or may not be statistically reliable. Reliabilism is also associated with the 'the new evil demon problem' [85], where 'we believe ourselves to be doing things that we are not doing'. The discussed cyber risk assessment standards appear to be based on reliabilism, because the standards attribute quantitative knowledge to cyber risk measurements, that would otherwise be considered incapable of measuring quantitatively.

5. Comparative empirical research study

5.1. Comparative analysis

Following the academic literature analysis, this section represents a comparative analysis of national IoT strategies in this space. The comparative analysis starts with the American

Industrial Internet Consortium (IIC) [86,87] partnership; the British Department for Culture, Media and Sport (DCMS) [88] report; the German Industrie 4.0 initiative [37]; and the Japanese Industrial Value Chain Initiative (IVI) [89,90]. The IoT strategies have been initially selected because they represent the most comprehensive and well-documented initiatives. These are compared with the Russian National Technology Initiative (NTI) [91]. The Russian IoT strategy is selected for the initial comparative research because of the divergence from the approaches taken in all other IoT strategies. The NTI focuses on market creation instead of technology creation and promotes regulations vs loosely defined standards. The comparative analysis is followed by a review of an additional ten less evolved IoT strategies. These are added to the analysis, in the pursuit of answers for the emerging gaps in the well-documented initiatives in terms of IoT cyber risk assessment. This section represents a comparative analysis, conducted to understand cyber risk impact assessment in national IoT strategies.

In the Industrial Internet Consortium (IIC) [86,87], similarly to the Industrie 4.0 [37], and the UK report by Department for Culture, Media and Sport (DCMS) [88], cyber security strategies are proposed in the form of Cloud-computing platforms, but there is no mention on how these cloud computing platforms actually provide/allow for cyber risk impact assessment. In similar fashion the Industrial Value Chain Initiative (IVI) [89,90] promotes loosely defined standards that can evolve simultaneously with new cyber risks. The Russian IoT strategy (NTI) [91], takes different approach and does not assess risks in real-time cloud networks.

Some IoT strategies have explicitly developed cyber risk architectures; e.g. IIC [86,87]; and impact assessment e.g. Industrie 4.0 [37,92]. Other focus on loosely defined impact assessment that emerge from forums, such as in the case of IVI [89]; or blogs, in the case of Made Different [93]; or surveys, in the case of High Value Manufacturing Catapult (HVM) [94]. In terms of defining the IoT cyber risk vectors, the most interesting approach is the direct electronic open submission of recommendations for changing or editing the strategy, such as the NTI [91]. Because IoT cyber risk is often invisible to cyber security experts and direct feedback mechanism would enhance visibility of IoT cyber risks.

Some IoT strategies promote cyber risk assessment through workgroups (e.g. IVI) in a similar methodological approach to the Operationally Critical Threat, Asset, and Vulnerability Evaluation method [95]. While other promote activities in the format of testbeds (e.g. IIC) or digital catapults (e.g. HVM). From the comparative research, it emerges that the direction of impact assessment, seems to be decided by the cyber risk assessment activities, e.g. workgroups [89] and testbeds [86], supported by economic assessments [96]. Impact is also decided by assessing key projects in the digital industry, e.g. Fabbrica Intelligente [97] and Industrie 4.0 [98].

The different approaches to impact assessment, could be resulting from the differences in focus on IoT technologies. The Industrial Internet Consortium [86] focuses on promoting core IoT industries; while other strategies, such as the New France Industrial (NFI) [99], the High Value Manufacturing Catapult [94] and the National Technology Initiative [91], all focus on promoting the development of key IoT technologies. Another IoT strategy, Made in China 2025 [100], promotes tech sectors, while the Made Different [93] promotes key IoT transformations. The diversity of the approaches in IoT strategies grows in magnitude. Some can be described as less evolved in identifying IoT cyber risk vectors (e.g. The Netherlands - Smart Industry [101]; Belgium - Made Different [93]; Spain - Industrie Conectada [102]; Italy - Fabbrica Intelligente [97]; G20 - New Industrial Revolution [103]). This could be because some IoT strategies lack documentation and appear disorganised, or simply are not ready for the I4.0. Such arguments are present in literature [104]. Although some appear to be purposely

elusive in terms of defining IoT cyber risk vectors (e.g. China - Made in China 2025 [100]; Russia - National Technology Initiative [91]).

The main IoT risk elements of each IoT strategy are compounded into categories representing the most prominent IoT cyber risk vectors. However, the compelling of data into these categories is quite challenging, as some strategies, represent a collection of descriptive explanations and do not provide explicit IoT cyber risk vectors. Such descriptive explanations present complexities in developing a unifying strategy. There are problems, when, for example, some of the IoT strategies differ in terms of IoT cyber risk vectors and propose very different impact assessment approaches. For example The Catapult programme [96] and the New France Industrial (NFI) [99], promote economic impact assessments. While the National Technology Initiative [91] promotes market assessment. To resolve this issue, we use the grounded theory methodology, where most prominent IoT cyber risk vectors are categorised and used as reference themes. Then, the categories are used for examining IoT cyber risk, to define a standardisation approach that relates various IoT risk vectors to eliminate conflicts in different and sometimes contrasting assessments of risk vectors. The comparative research also identifies a number of gaps in IoT strategies. By gaps, we refer to topics or IoT cyber risks not incorporated or discussed in the associated strategies.

The differences in impact assessment approaches in the IoT strategies do not necessarily represent a lack of understanding of such risk vectors. It does, however, represent a lack of presence or recommendation in these vectors. Considering the volume of gaps, especially in the emerging and less evolved areas, and the roughly defined IoT strategies, the overall understanding of cyber risks emerging from the IoT becomes questionable. In some strategies, e.g. the Advanced Manufacturing Partnership [105], these gaps are understandable, because one strategy would have evolved into a new high-the strategy, e.g. IIC [86]. Similarly, in some IoT strategies the IoT cyber risk vectors are not discussed e.g. the Digital Catapults [94,96], because of the separate national IoT strategies that cover these areas, e.g. the DCMS report [88]. Some IoT strategies are very narrowly focused on futuristic IoT technologies, e.g. New Robot Strategy [106]; Robot Revolution Initiative [107]; and the IoT technologies do not yet exist. Hence, we can only speculate on the expected cyber risks. In such cases, the IoT cyber risks are better assessed by reviewing the associated strategies for IoT technologies that are currently in use, e.g. the Industrial Value Chain Initiative [89].

The most concerning gaps in discussions or recommendations on IoT cyber risk, are present the emerging and less evolved IoT strategies [93,97,101,102] and the elusively defined IoT strategies [91,100,103]. It is unclear if some of these national IoT strategies e.g. Made Different [93] are aware of the IoT cyber risks, or in other strategies [91,100], whether the IoT cyber risk are ignored and not considered as a cause of concern.

5.2. Empirical analysis of gaps in cyber risk impact assessment approaches

The empirical analysis initiates with identifying cyber security frameworks and comparing with most recent cyber security literature on this subject. The empirical analysis includes the qualitative approaches to measuring cyber risk [79,95,108–110], and the quantitative approaches [111,112].

Some of the frameworks propose diverse qualitative methods, such as the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [95], measures cyber risk through workshops. Apart from frameworks, some qualitative approaches for measuring cyber risk propose methodologies. The Threat Assessment & Remediation Analysis (TARA) [109] methodology applies a threat matrix. There also systems that combine qualitative and quantitative approaches. The Common Vulnerability Scoring System (CVSS) is a

 doi:10.20944/preprints201904.0133.v1

mathematical quantification calculator [78,79] that applies expert's opinions, presented as statements, where each statement is allocated a level of cyber risk and the calculator assesses the overall level of risk form all statements. Such mathematical quantifications of qualitative data has been considered by other quantitative approaches as misrepresentation [111]. But considering the lack of more precise methods, the modified base metrics represent the state of the art at present. CVSS calculator does not calculate the cyber risk from shared infrastructure, e.g. supply chains, and does not assess the cyber risk from IoT connected devices.

To identify a current cyber risk state that includes supply chain cyber risks, the Exostar system [113], which represent a qualitative approach, can be used for complimenting the CVSS and covering the supply chain aspect of cyber risk. The Exostar system [113] provides guidance points for assessing the supply chain cyber risk. The design principles of the CVSS calculator and the Exostar system can be compounded to design a process for depicting the maturity levels. Such a combined method could use primary data based on interview and survey responses, to create and compare a current state of cyber controls required for different levels of cybersecurity maturity. The results could be verified with the Exostar survey for determining supply chain cyber security maturity levels [113]. Excluding the supply chain cyber risk, the overall current state of cyber maturity can be verified with the Capability Maturity Model Integrated (CMMI) [110], which integrates five levels of the original Capability Maturity Model (CMM) [114].

To reach the required cyber security maturity level, the current cyber state can be transformed into a given a target cyber state by applying the National Institute of Standards and Technology's (NIST) [108] cyber security framework implementation guidance [115]. However, the NIST guidance is specifically designed for Federal Agencies and requires adaptations to be applicable to enterprises.

The most concerning aspect of the NIST framework is the fourth step of the guidance point, which requires organisations to conduct a risk assessment. The risk assessment approach is based on the framework for improving cybersecurity of critical infrastructure [116] and follows recommendations for qualitative risk assessments e.g. standards based approach, or internal controls approach. In addition, the recommendations [116] are few years old and the cyber risk environment is changing at a rapid pace [22]. This could render the recommendations obsolete if the standards are not continuously updated at a similar speed as cyber risk are changing. While NIST is working hard on an updated version [117], the cyber risk seems to be changing at a faster pace, especially the IoT cyber risk. By probing the characteristic for the NIST framework, additional gaps emerge. The NIST framework requires determining a detailed current cyber profile and a maturity level, but does not provide a model for these steps. The CVSS calculator [78,79] could be used to create a current cyber profile, in addition to the Exostar system [113] for determining the supply chain cyber maturity level, and CMMI [110] the overall current state of cyber maturity. The final gap in the NIST framework is the lack of cyber risk quantitative assessment, which is crucial for making an informed and detailed recommendations for a target cyber profile. The risk assessment is a core step in the framework, and they provide several informative references on how it can be conducted. However, the informative references are not related to the recommendations from the World Economic Forum [23,118] and FAIR institute [111,112].

Another approach to understanding risk is through the use of emerging quantitative cyber risk models, such as the Factor Analysis of Information Risk Institute (FAIR) approach [119]. FAIR suggests the development of a framework for 'understanding, measuring and analysing information risk'. The FAIR approach is complementary to existing risk frameworks that are

deliberately distanced from quantitative modelling (e.g. NIST) and adapts existing quantitative models, e.g. RiskLens [111], and Cyber VaR (CyVaR) [112]. In a way, FAIR is complementing the work of NIST and the International Organisation for Standardisation (ISO) [120], which is the international standard-setting body and includes cyber risk standards. For example, the ISO 27032 provides specific recommendations and ISO 27001 sets requirements for cyber security. Notable for this discussion, only FAIR [119] provides recommendations for quantitative risk estimation, which some of the other frameworks and models have focused on qualitative estimation approaches. The state of the art in current risk estimation (also known as risk analysis) is based on the high, medium, low scales (also known as the trafic lights system or colour system).

The Exostar system [113], CMMI [110], CVSS [78,79], represent approaches to assess risk (including vulnerabilities/threats/impacts), but their risk estimation techniques use likelihood of impact on high, medium, low scales, and only CVSS [116], [120], try to use actual figures and mathematical formulae to come up with quantified risk values. The mathematical formulae however, are not based on probabilistic data. Hence CVSS simply allocates a number to the high, medium, low scales does not quantify risk with the traditional statistical probability approach. To clarify this argument, risk assessment covers three main areas: risk identification, risk estimation and risk prioritisation [66]. While recovery planning is a part of risk treatment, which is covered by risk management. A key point to note here is that risk estimation is used for risk management, and as such quantitative risk impact estimation is needed for making decisions on topics such as cyber risk insurance. The IoT cyber risk insurance requires precision and given the lack of actuarial tables, qualitative quantification is its subjective and lack precision [66]. Given this lack of precision, one expert perception of a threat as low might not conform to another expert perception or belief. On the other side of the argument, probabilistic models lack sufficient actuarial data and given the complexity of the analysis in interconnected systems, there are very few probabilistic models that claim success in quantitative risk estimation and analysis. These risk assessment approaches e.g. FAIR [119], RiskLens [111], and CyVaR [112], are still be in their infancy and could benefit from considering recovery planning in the quantitative risk impact assessment. Although even quantitative risk impact assessment approaches do not provide guidance on recovery planning, these approaches enable the recovery planning function of risk management, through the quantitative risk impact estimation and analysis.

Continuing with the gap analysis of current state of the art approaches, OCTAVE is a risk assessment method based on a qualification technique (high, medium, low) to measure risk. OCTAVE does not provide a quantification of risk estimation with a quantitative technique (i.e., actual figures, costs, etc.). Quantification of risk estimation is required for calculating the required level of recovery and for ensuring that cyber risk insurance policies cover the required level of recovery. For example, a cyber risk insurance policy with the required level of recovery, would enable a company to recover better, then a company with estimated level of recovery. Similarly, TARA, does not quantify level of exposure through risk estimation. These risk assessment frameworks and methodologies need to be concentrated on cyber risk impact estimation, because that is the area of risk assessment they have not covered. One approach for bringing the focus on risk impact estimation, is to integrate the cyber recovery recommendations from the ISO and NIST frameworks. Once the element of recovery is considered, then the risk impact estimation becomes of great importance for relating the risk assessment with the risk management functions. Another approach for bringing the focus on risk impact estimation, is to integrate the FAIR recommendation for quantifying the level of exposure.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 April 2019 doi:10.20944/preprints201904.0133.v1

There seems to be a disconnection from the aforementioned risk assessment approaches and the quantitative risk assessment approaches. The discussed frameworks and methodologies, including the Exostar systems and CVSS calculator, all represent a qualitative approach to assessing cyber risk. For the purposes of the empirical analysis, two quantitative risk assessment models are compared: RiskLens and CyVaR. The main difference between the two models is that RiskLense uses BetaPERT distributions [111] and the CyVaR is based on the Value at Risk model [25,112,118,121]. Both models however, do not assess the cost of recovery but only the financial impact.

5.3. Transformation roadmap for standardisation of IoT risk impact assessment

To define a transformation roadmap for standardisation of IoT risk impact assessment, the methodology follows established approaches [122–128] and few recently developed design processes [122,129–137] .The following section performs strengths, weaknesses, opportunities and threats (SWOT) analysis. This diversity of approaches identified in the gap analysis, presents conflict in risk assessment, e.g. qualitative versus quantitative, or Threat Matrix versus Maturity models versus BetaPERT distributions. To enable the standardisation design, in Table 1, firstly the core cyber impact assessment concepts are extracted to defining the design principles for cyber risk impact assessment from IoT vectors. Then the design principles are examined with SWOT analysis. The design principles define how to identify, manage, estimate, and prioritise cyber risk. These are described as:

- Risk identification (measure) – calculate economic impact of cyber risk.
- Risk management (standardise) – international cyber risk assessment approach.
- Risk estimation (compute) – quantify cyber risk.
- Risk prioritisation (strategy) – plan for impact of cyber-attacks, e.g. cyber insurance.

Vectors	FAIR	CMMI	CVSS	ISO	NIST	Octave	TARA
Risk identification (measure)	Financial	Maturity models	Base metrics	ISO 27032	Categorising	Workshops	Threat Matrix
Risk management (standardise)	Compliance	ISO 15504 - SPICE	Mathematical approximation	ISO 27001	Assembling	Repeatability	Template threats
Risk estimation (compute)	Quantitative	Maturity levels	Qualitative	Compliance	Compliance	Qualitative	Qualitative
Risk prioritisation (strategy)	Level of exposure	N/A	N/A	ISO 27031	Compliance	Impact areas	System recovery
The strengths, weaknesses, opportunities and threats (SWOT) analysis of the reviewed frameworks, methods, systems and models can be summarised as follows:							
The strengths of the reviewed approaches include:							
OCTAVE has developed a standardised questionnaire that can be applied to investigate and categorise recovery impact areas.							
TARA is a predictive framework that enables targeting of the most crucial exposures, as opposed to promoting the defence of all possible vulnerabilities.							
CVSS is relatively easy to use and translate results. Moreover, it is based on input and feedback from various sources and can be used to translate simple qualitative input into a numerical score reflecting severity and characteristics of a vulnerability.							
Exostar System enables enterprises to assess, measure, and mitigate risk in real-time across multi-tier partner and supplier networks and determines the gaps between cybersecurity posture and regulatory compliance.							
CMMI combines set of best practices in the disciplines of systems analysis and design, software engineering and management. CMMI can simultaneously address multiple as opposed to stand alone improvements. This enables improvement in the entire enterprise risk and the full product development life cycle risk.							
The NIST framework is valuable in assessing cyber risk, but more valuable in managing cyber risks. NIST is also the most advanced framework in terms of disaster and recovery planning.							
FAIR model promotes a quantitative, risk based, acceptable level of loss exposure.							
ISO promotes standardisation of cyber risk and reflects international experience and knowledge. ISO provides standards for cyber risk and disaster recovery.							
RiskLense presents a quantitative assessment with Monte Carlo simulations.							
CyVaR presents a method to quantitatively assess risk with Monte Carlo simulations.							
The weaknesses of the reviewed approaches can be summarised as follows:							
OCTAVE fails to provide a quantification method for calculating the required level of recovery.							
TARA fails to quantify the impact of cyber risks, which is crucial for deciding on appropriate recovery planning.							
CVSS contains scoring range between 0.0 to 10.0, but is based on a 3-level system and because the score is derived from a limited number of variables, it creates dissimilar vulnerabilities receiving similar score.							
Exostar System does not assess enterprises own cyber risk exposure. Instead, it helps enterprises to manage risk by understanding the strengths and vulnerabilities of their supply chain partners.							

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 April 2019 doi:10.20944/preprints201904.0133.v1

CMMI does not explain how to implement improvements, but only indicates where improvements are needed. The improvements are not methodological processes and the actual processes an enterprise chooses depend on multiple factors. The CMMI may simply not map the processes in a specific enterprise.
NIST framework is documented, not an automated tool and does not contain an impact assessment model for quantifying cyber risk.
FAIR framework promotes standardisation of quantitative models, but is difficult to use and is not as documented as other frameworks, e.g. OCTAVE. The greatest shortcoming is the lack of access to current information about the methodology and examples of how the methodology is applied.
ISO is based on voluntary shared knowledge and is consensus based. International standardisation requires a level of compulsory compliance.
RiskLense contains a lack of details on the algorithm supporting its risk assessment.
CyVaR has the potential issue of a lack of the required risk data to perform adequate and comprehensive assessments.
The opportunities of the reviewed approaches can be summarised as follows:
OCTAVE is aimed at companies with limited resources, it is free and can be used as the foundation risk-assessment component or process for other risk methodologies.
TARA is a methodology that can be implemented as a complementary method, in combination with other risk assessment processes.
CVSS currently has a 3-level scoring system, and as such the biggest opportunity is to integrate more levels in the calculator to represent cyber risk with greater precision. Since the numbers are based on experts' opinion and do not represent an ultimate precision, the calculator represents a guiding point. As such, colour coded system with more risk categories could be easier to understand than a number. Numbers may also provide a fake sense of precision, while the numbers in the calculator are not based on established mathematical or statistical probabilistic data.
Exostar System could evolve into a system that assesses enterprises own cyber risk exposure, while enabling the assessment of cyber risk from supply chain partners.
CMMI is related to ISO 9001. The ISO 9001 specifies a minimal acceptable quality level, while CMMI specifies continuous process improvement. Biggest opportunity is to adapt CMMI with continuous updates from ISO 9001 and other standards.
The NIST is based on an extensive use of acronyms, which can be confusing and require a detailed understanding of the standards referred to in the acronyms. Hence, the greatest opportunity would be changing and simplifying the design. This could be done by replacing the acronyms with a new user friendly tool to incorporate a fully automated guidance process (e.g. such as CVSS calculator).
FAIR is complementary to existing risk frameworks and applies knowledge from existing quantitative models. This represents an opportunity for developing a standardisation reference architecture.
ISO could evolve into an international standardisation of cyber risk/security frameworks, models and methodologies.
RiskLense could evolve into the first standardised quantitative model for cyber risk assessment. More academic research is required on this model to define and disclose the algorithm. This would increase the acceptance of this model, as academic research would enable the model to be verified and validated.
CyVaR needs to be adapted and modified to include units of measurement for IoT cyber risk vectors.
The threats of the reviewed approaches can be summarised as follows:
OCTAVE method is complex and takes time to understand. This is the main weakness as it is a qualitative method that does not provide mathematical or financial modelling.
TARA focuses on reducing cost by covering only the exposures that are most likely to occur. Considering that not all exposures are covered, greater focus should be on recovery planning. TARA promotes and facilitates system recovery, but does not address the level of cyber risk impact.
CVSS converting qualitative data into a quantitative result, with relatively low level mathematical approximation, could create a false level of security.
Exostar System uses third-party sources to provide insights in the cyber health and viability of supply chain partners. The validity of the data depends on the third-party sources and if this cyber data is incomplete or compromised, the insights would also be compromised.
CMMI measures are easy to recognise but difficult to develop. For instance, CMMI does not provide guidance on how to implement improvements, it simply indicates where improvements are required.
NIST as a documented model, depends on many documents being continuously updated. Unless it evolves into a more automated process, the framework would need constantly to be reviewed and updated as new technology and laws emerge.
FAIR depends on a computational engine for calculating risk and a model for analysing complex risk scenarios RiskLens [111]. RiskLens [111] is a commercial product and the software comes at a cost. Standardisation of commercial products could create disadvantages for small enterprises that lack resources of large enterprises. Small enterprises may choose free models such as OCTAVE.
ISO contains members from 161 countries and 778 technical committees and subcommittees. This presents a major challenge in coordination and integration of specific standards.
RiskLense, without the academic peer-review rigour and industry expert review, represents a model that is very difficult to verify and validate. Without such validation, the results would be questionable.
CyVaR is a fairly complicated approach and unless simplified, in a software format, similar to the CVSS, it could be difficult to implement as a standard model for cyber impact risk assessment.

Table 1: Transformation roadmap for standardisation of IoT risk impact assessment

The resulting definition of transformation roadmap emerges from the gap analysis and the SWOT analysis of existing cyber risk impact assessment approaches. To reduce the content of the emerging concepts from the comparative empirical analysis, the controlled convergence methods was applied in a case study research.

6. Case study research

6.1. The case study

The case study research involved four workshops that included 18 distinguished engineers from Cisco Systems, and 2 distinguished engineers from Fujitsu. The workshops with Cisco Systems were conducted in the USA in four different Cisco research centres. These centres were as follows: First Centre - Security and Trust Organisation; Second Centre - Advanced Services; Third Centre - Security Business Group; and Fourth Centre - Cisco Research Centre. In pursuit of validity, a separate workshop was conducted with two experts from Fujitsu centre for Artificial Intelligence the UK. The Fujitsu workshop was conducted separately to avoid those experts being influenced or outspoken by the larger goup from Cisco systems.

The first two Cisco workshops were conducted to apply the controlled convergence [138,139]. The following two Cisco workshops, and the Fujitsu workshop, to verify the design. This approach to pursuing validity follows existing literature on this topics [140,141] and provides clear definitions that specify the units of analysis for IoT cyber risk vectors. The reason for pursuing clarity on the units of analysis for IoT cyber risk, was justified by existing literature, where these are identified as recommended areas for further research [142]. The IoT risk units of analysis from individual IoT strategy are combined into standardisation vectors. The process of defining the standardisation vectors followed the Pugh controlled convergence method, where experts were asked to confirm the valid concept, merge duplicated concepts, and delete conflicting concepts. The main limitation of the Pugh controlled convergence method is the difficulty in gathering large number of experts in one location.

To resolve this, the workshops were limited to two hours and the results from the comparative analysis, the empirical analysis, the gap analysis and the SWOT analysis were distributed in advance, through Cisco secured server to all participants. The experts were asked to perform the first round of concept selections online and distribute their results anonymously in a secured file. Considering the participants included distinguished engineers, senior managers and directors of the Cisco centres, anonymity was considered crucial to ensure the answers are not biased or influenced by what the management wanted to hear. To increase participation, secure WebEx video conferences were established in Cisco Research Centre in North Carolina, U.S. That enabled experts from other parts of the U.S. to join in the workshops. The data from the controlled convergence workshops was transcribed and stored on the Cisco secured file.

6.2. Transformation imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach

Following the identification of a high-level target state in the comparative empirical analysis, the controlled convergence was applied to narrow the emerging implementation tasks through case study. The controlled convergence was applied for the development of a high-level transformation roadmap. To build the transformation imperatives in Table 2, the case study reviewed secondary data the main cyber risk impact assessment approaches. The emerging categories are validated with applying the controlled convergence with a group of experts. The process of confirming validity of the data in Table 2, included four workshops with experts in the field. Table 2 outlines the transformation process but does not include all the steps as the aim is to present a methodology, not the actions. The rationale is that different enterprises will have different cyber security steps to perform in order to transition to a higher

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 April 2019 doi:10.20944/preprints201904.0133.v1

maturity lever. A long and detailed list of steps can be found in the NIST framework and the Exostar system.

High level transformation imperatives
Training and awareness
Control goal (parent) 1: Security skills assessment and training
Control objective (child) 1: Skills and integrated plan to support defence of the enterprise.
Control element (orphan) 1: Analysis of needed skills; provide training to match the required skills and validate skills through periodic tests. More advanced control orphans include: security assessments using real-world examples to measure mastery or skills.
Control goal (parent) 2: Penetration testing.
Control objective (child) 2: Test the defences by simulating cyber-attacks.
Control element (orphan) 2: Regular focussed penetration tests for detecting unprotected systems through vulnerability scanning and penetration testing combined.
Control goal (parent) 3: Mobile device
Control objective (child) 3: Mitigate cyber risk from mobile devices.
Control element (orphan) 3: Mobile devices should have access controls to enforce policies and option to remotely clean the device.
Cyber threat intelligence
Control goal (parent) 1: Boundary defence
Control objective (child) 1: Manage the flow of information between network trust levels.
Control element (orphan) 1: Prevent communications with malicious IP addresses, use two-factor identification; design DMZ network and scan connections that aim to bypass the DMZ; block known bad signature or attack behaviour.
Security event monitoring
Notes: links with: (a) network security; (b) identity and access management.
Control goal (parent) 1: Maintenance, monitoring and analysis of audit logs
Control objective (child) 1: Collect, manage and analyse audit logs of events.
Control element (orphan) 1: Two synchronised timestamps in logs to ensure consistency; develop a log retention policy.
Control goal (parent) 2: Secure configurations for network devices such as firewalls, routers and switches
Control objective (child) 2: Actively manage the security configuration of the network infrastructure.
Control element (orphan) 2: Documenting all new configurations rules that allow traffic to flow through network security devices; use two-factor identification and encryption.
Control goal (parent) 3: Account monitoring and control
Control objective (child) 3: Control the life-cycle of system and application accounts.
Control element (orphan) 3: Disable unused account; imprint accounts expiration date; enable revoking system access accounts; log-off users after a standard period of inactivity; encrypt transmitted passwords.

Table 2: Transformation imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach

For implementing the recommendations emerging from the transformational imperatives, we refer to the NIST cyber security implementation tiers as support guidance. NIST advocates transforming current cyber profiles that dictate reactive approach, into risk informed, repeatable and adaptive target cyber profiles [115]. The NIST implementation tiers are developed specifically for critical infrastructure and needed to be adapted for enterprise cyber risks. In developing the target profile implementation tiers on enterprise level, we used a broader approach, considering risk management across the entire enterprise cyber risk, rather than examining individual categories and subcategories. The target state implementation tiers should firstly focus on the network security e.g. cyber security through vigilance, resilience and behaviour, and security by design and by control [143]. These implementation steps are the prime focus of government and industry efforts for improving cyber security exposure. In the following section, the transformation roadmap and imperatives are used to define a new IoT risk impact assessment with a goal-oriented approach and the Internet of Things Micro Mart model.

7. IoT risk impact assessment with the transformation roadmap and imperatives

Dependency goal-oriented modelling can be applied to connect unconnected risk models and to build a risk model for a complex IoT systems. The first step is to link separate models. This requires identifying the shared principles from the multiple models that we are connecting. Then, to determine the level of dependency risk, we need to understand the dependencies of the shared principles.

7.1. IoT Risk Analysis through Functional Dependency

Dependency modelling and analysis (DA&M) provides a means to support the management of functional and operational complexities within IoT systems with focus on the system elements, measures of a design or operational challenge, as well as the functional dependencies that define their associations. Dependency modelling and analysis can support a superior understanding of connectivity and its implications on performance, and can assist in constructing, improving, and maintaining of such complex system.

The construct and exchanges that happen in IoT domain defines a tightly coupled association amongst constituting components and sub-systems such considerably on the correct functions of another linked component or system. This is considered a dependency relationship, and can either be direct (a first order dependency) or indirect (a subsequent higher order dependency) [144]. For example, from a typical IoT architecture [145], normal functions for components and services on the application layer typically depend on the normal functioning of their counterparts on the network layer. This latter also relies on the perception layer component and services. If a component or service on the perception layer is compromised, such impairment can alter the correct functioning of connected component or service on the network or application layers. Thus, security risks in an IoT domain may not exactly be drawn from the failure of one specific IoT component, but most often extend to the failure of other IoT components that can be recipients of rippling impacts. This dependency amongst IoT sub-systems and components can also cause impacts or failures to cascade from one affected system or component onto another; worsening the damaging impacts [146,147].

Depending on the evaluation approach, security and safety-critical impacts typically vary amongst assets, their functionalities (services), placement positions, and configurations within industrial networked systems [148] including IoT. However, to support effective decision-making from both security and safety perspectives, IoT adopters need to adopt risk assessment methods that exceed considering risk scenarios one-by-one, qualitatively or statically, to considering the relationship between the risk factors (Muller et al. 2017). This way, they can achieve the quantification of security-related dependencies that can help provide deeper insights on how an impact to IoT infrastructure that prevents it from delivering the relevant and requite service(s), can affect the performance levels of other sub-systems that connect and rely on an affected target. This can help in the development and adoption of effective security incidence response and recovery [144], as well as help reduce and manage the effects of IoT disruptions.

Indeed, existing complex system dependency modelling approaches provide a good starting point for understanding IoT dependency analysis. A simulation-based approach through scenario-driven what-if analysis can provide platform for such complex dependency analysis bordering on simulating the consequences of discrete events, and the physical economic flows amongst IoT sub-systems [149]. This method provides a method for resolving disparate events and controls strategies. Leontief-based input-output approach [150] can support IoT interdependency modelling from failure risk dimension. As a common approach for analysing risk transmission among interdependent components, the input-output Leontief-based model offers an explorable approach deriving dependency-oriented attributes such as; disruption probability, risk transmission, and cascading impacts [149]. A network-based approach can also assist the evaluation of physical dependencies and cascading disruptions within and across geographical dimensions. These typically explore stochastic modelling [147,151], especially the Markov-based techniques [152,153]. An important point to draw from these approaches is that topological characteristics of networked infrastructures, such as connectivity, path length,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 April 2019 doi:10.20944/preprints201904.0133.v1

degree of vertex, and redundancy ratio can be leveraged for interdependency analysis, and used to resolve the spatial impacts of risks and disruptions in the IoT.

7.1.1 Network-based Linear Dependency Modelling

One way of achieving IoT dependency modelling is through a network-based functionality dimension – analysing how the functionality of one system or component can affect the functionalities of other systems or components [149], explorable on the basis of connectivity and process configurations over multi-layered IoT architecture. Graph theory [144,154] - using vertices and edges; provides a way to simply represent (directly or logically) the dependency of IoT components within and across multiple functionality layers. In this case, dependency can be derived if a component or service of system *j* (vertex) is linked (edge) to another *i*, such that *i* relies on the outputs from the normal functionality of *j* for its own basic functionality. It becomes an interdependency if *j* also relies on some functional output from *i* to achieve further functionality. This can mean that an impact in *i* can cause impacts in *j*, which can subsequently affect another entity *k*, which is functionality dependent on *j* ($i \rightarrow j \rightarrow k$). This indicates a higher-order (inter)dependency scenario, which can introduce complexities to the size of the IoT system. In a higher-order dependency structure, impacts can cascade from a single component, service, or system to others in multiple layers. Using this approach, clearly articulating the security-related functional dependency status of a component in the network requires answering questions such as: is the component connected to an industrial network? Does the component have a known exploitable vulnerability? Does its function contribute to the actualisation of a set of system operations? Does the component have one or more other components depending on it for data or instruction set to accomplish a desirable process? And Does it depend on any component(s) to accomplish its set operation in the system? Providing answers to these questions can guide the correct mapping of node dependencies in the ICS network.

With these, a functional dependency scenario can be modelled using directed graph G as an ordered pair *(V, E)* composed of a finite set of vertices *V*, and a binary relation *E* on *V*. The elements of *E* are referred to as edges (arrows) and represent the *'impact link'* that cascades along successive edges. These arrows form an ordered pair $e = (v_i, v_j)$, where $v_i, v_j \in V$ represent components in the network, and *e* represents the dependency impact link from an originating component v_i to a destination component v_j. To develop a functional dependency and impact model, every component (physical execution, logical execution and monitoring, control and workflow management, and boundary-based devices) is mapped to a *vertex* and every dependency impact link to an *arrow* in a graph. This graph-based structure can be used to model the topological dependencies in ICSE network and used to capture attack impacts. On a typical directed graph structure, this corresponds to the sum of the number of directed edges *e* going out of a source node v_i, and that of the target destination node(s) v_j. However, the impact of an attack starts from a source node, so that the determination of a dependency impact captures all possible impact points on the graph or network. For every vulnerability attributed to a component *v* on the network, a corresponding functional dependency impact index $y = f(v)$ is proposed as the cumulative dependency links across the component from the vertex *v* inclusive. When a component is attacked, the functional dependency index is conceived to as the number of components that are included along a path following the vertex from the originating component. This represents a simplistic implementation based on linear analysis on a conditional existence of configured connectivity amongst IoT components. A Boolean True (1) or False (0) specification can be obtained as values from establishing functional/physical dependency queries between IoT components. With this, aggregate values

 doi:10.20944/preprints201904.0133.v1

can be derived to represent the degree of functional dependencies associated to individual components in the IoT network.

If combined with dynamic vulnerability information such as the environmental severity attributes (*collateral damage* potential of a vulnerability, its *target distribution*, and its *target security requirement violation*) from standard CVSS [155,156] often considered optional when undertaking security analysis, then the outcome can potentially be used to understand potential impact associated to component vulnerabilities – estimating how wide or otherwise an impact on a component or system can ripple through and affect other components and systems. Such insights can support a more accurate estimation of risks, incident response, and recovery in the IoT domain. Thus, an organisation embracing IoT integrations into their networks and services need to perform a perform such multi-factor security analysis to derive of its IoT cyber security posture. The IoT organisation needs to be clear about its current and target security posture, before designing and adopting a transformation roadmap outlining tasks to achieve the stated target posture. In developing a target profile, a broad range of approach may be used, considering more effective and efficient risk management approaches across the entire in-scope organisations

7.2. IoT risk impact assessment with a Goal-Oriented Approach

Identifying shared principles for multiple independent cyber risk models is challenging, because risk assessment is not based on shared risk estimation. This can partially be resolved by focusing on the success factors and concentrating on the external dependencies. In this approach, individual risk vertices are considered as representative of a larger complex IoT system. This advocates a top-down, or goal-oriented modelling approach, where success factors are traversing across multiple isolated models. Such goal-oriented modelling approach can be analysed with Bayesian methods. Statistical inference can be updated with Bayes theorem as more evidence and probabilistic data becomes available. The paradigm can provide a real-time statistical assessment of cyber risk of all the entities in the model. The dependencies between a dynastic metaphor, such as ‘parent’, ‘child’, ‘orphan’ are explained in the transformational roadmap, can be analysed with computational statistics using a Bayesian analysis engine [157,158]. Therefore, the proposed goal-oriented dependency modelling approach, is dependent on Bayesian analysis engine to determine a range of sensitivities or vulnerabilities. To develop Bayesian inferences, the model requires the statistical relationships between ‘parent’, ‘child’, and ‘orphan’. The level of achievement is articulated as the ‘state’ of the goal, which is usually correlated with failure and success. However, while ‘state’ is usually identified according to a value judgement, e.g. bad-good, no-yes or 0-1, a ‘state’ could also be identified with a number of possible states, not necessarily two single states. In addition, with the Internet of Things real-time updating, the decision model can provide real time risk assessment, where the impact of changes in state can be immediately identified. This is evaluated in more detail with the introduction of the Internet of Things - MicroMort model.

7.3. Micro Mort

Since there is no International IoT Asset Classification (IIoTAC) and no established Key IoT Cyber Risk Factors (KIoTCRF), for the calculations of the new model, we would firstly need to determine the IIoTAC and the KIoTCRF. After the establishment of IIoTAC and KIoTCRF, the new model could be applied to calculate more precise ‘willingness to pay’ to reduce IoT cyber risk.

7.4. Relationship between the Goal-Oriented Approach and the IoTMM model

The relationship between the IoTMM and the Goal-Oriented Approach is that the IoTMM expresses a conditional probability for the Goal-Oriented Approach dynastic metaphor. The conditional probability is the probability of a goal in the dynastic metaphor (in the transformational roadmap), being in a 'state' according to the states of its 'parents', 'children', and 'orphans'. Since Bayesian inferences are based on a logical AND or OR function then the IoTMM provides more clarity than a simple structure consisting merely of 0s and 1s.

In scenarios where there is a lack the probabilistic data to determine the IoTMM, then the goal is considered as 'uncontrollable'. In such scenarios, the IoTMM still provides a conditional probability as an isolated model. However, in uncontrollable scenarios, the IoTMM only presents a catalogue of the probabilities in each possible 'state'. The advantages of combining the IoTMM with dependency modelling is more obvious when the uncontrollable states are dynamically analysed from other distributed states that contain the actual 'state' and dependencies. With this approach, it becomes possible to assess uncontrollable states in complex systems.

8. Conclusion

This article combines existing literature and performs comparative, empirical and theoretical analysis of common cyber risk assessment approaches and integrates current standards. The findings present a map of the present initiatives, frameworks, methods and models for assessing the impact of cyber risk. Hence, the article advances the efforts of integrating cyber risk standards and governance and offers a better understanding of a holistic impact assessment approach for IoT cyber risk. This enables visualising the interactions among different sets of cyber security assessment criteria and results with a new design criterion specific for cyber risk from the IoT. The contributions from this paper constitute;

1. Transformation roadmap for standardisation of IoT risk impact assessment;
2. Transformation imperatives describing how IoT companies can achieve their target state based on their current state with a Goal-Oriented approach;
3. Followed by epistemological analysis defining a unified cyber risk assessment approach.

The roadmap and the design imperatives can be applied for:

a. Risk identification (measure IoT risk) – calculate economic impact of cyber risk;
b. Risk management (standardise IoT risk) – international cyber risk assessment approach;
c. Risk estimation (compute IoT risk) – quantify cyber risk;
d. Risk prioritisation (design IoT risk strategy) – plan for impact of cyber-attacks, e.g. cyber insurance.

The paper also presents new methods for applying the roadmap through: IoT Risk Analysis through Functional Dependency; Network-based Linear Dependency Modelling; IoT risk impact assessment with a Goal-Oriented Approach; and a correlation between the Goal-Oriented Approach and the IoTMM model.

In addition, the paper outlines a process for visualising IoT cyber risk. This was identified as one of the key problems faced by cybersecurity practitioners, because installation of new IoT devices was confirmed as often not reported to the cybersecurity professionals. The visualisation of cyber risk can be used by practitioners and regulators to inform organisations

in this space of best practices. The design principles, with the transformational roadmap, can be applied to assess the impact of cyber compromises and to make cyber security recommendations. The findings are relevant to national and international I4.0 networks, specifically for IoT cyber risk planning.

8.1. Limitations and further research

The set selection of IoT strategies was based on documented availability. There are additional frameworks, models and methodologies that are not considered in this article, such as risk assessment approaches for SCADA. In the risk assessment approaches that are not covered, there could be concepts that are relevant to standardisation of risk assessment approaches. Holistic analysis of all risk assessment approaches was considered beyond the scope of this study. Additional research is required to integrate the knowledge from other studies. The epistemological framework in this article presents a generic approach to guide researchers and practitioners [73,74,129–131,133–139,75,159–165,122–128].

9. References:

1. Marwedel, P. & Engel, M. Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions. in 1–30 (Springer International Publishing, 2016). doi:10.1007/978-3-319-26869-9_1
2. IBM. *2016 Cyber Security Intelligence Index infographic for Healthcare*. (2016).
3. Deloitte. *Cyber security: everybody's imperative A guide for the C-suite and boards on guarding against cyber risks*. (2017).
4. Wan, J., Chen, M., Xia, F., Di, L. & Zhou, K. From machine-to-machine communications towards cyber-physical systems. *Comput. Sci. Inf. Syst.* **10**, 1105–1128 (2013).
5. Stojmenovic, I. Machine-to-Machine Communications With In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems. *IEEE Internet Things J.* **1**, 122–128 (2014).
6. Drath, R. & Horch, A. Industrie 4.0: Hit or Hype? [Industry Forum]. *IEEE Ind. Electron. Mag.* **8**, 56–58 (2014).
7. Lee, J., Bagheri, B. & Kao, H.-A. *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*. *Manufacturing Letters* **3**, (2015).
8. Leitão, P., Colombo, A. W. & Karnouskos, S. Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Comput. Ind.* **81**, 11–25 (2016).
9. Shafiq, S. I., Sanin, C., Szczerbicki, E. & Toro, C. Virtual Engineering Object / Virtual Engineering Process: A specialized form of Cyber Physical System for Industrie 4.0. *Procedia Comput. Sci.* **60**, 1146–1155 (2015).
10. Posada, J., Toro, C., Barandiaran, I., Oyarzun, D., Stricker, D., de Amicis, R., … Vallarino, I. Visual Computing as a Key Enabling Technology for Industrie 4.0 and Industrial Internet. *IEEE Comput. Graph. Appl.* **35**, 26–40 (2015).
11. Kambatla, K., Kollias, G., Kumar, V. & Grama, A. Trends in big data analytics. *J. Parallel Distrib. Comput* **74**, 2561–2573 (2014).
12. Pan, M., Sikorski, J., Kastner, C. A., Akroyd, J., Mosbach, S., Lau, R. & Kraft, M.

Applying Industry 4.0 to the Jurong Island Eco-industrial Park. *Energy Procedia* **75**, 1536–1541 (2015).

13. Wang, L. Machine availability monitoring and machining process planning towards Cloud manufacturing. *CIRP J. Manuf. Sci. Technol.* **6**, 263–273 (2013).
14. Brettel, M., Fischer, F. G., Bendig, D., Weber, A. R. & Wolff, B. Enablers for Self-optimizing Production Systems in the Context of Industrie 4.0. *Procedia CIRP* **41**, 93–98 (2016).
15. Carruthers, K. Internet of Things and Beyond: Cyber-Physical Systems - IEEE Internet of Things. *IEEE Internet of Things* (2016).
16. Leonard, T. C. Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness. *Const. Polit. Econ.* **19**, 356–360 (2008).
17. Rutter, T. The rise of nudge – the unit helping politicians to fathom human behavior. *Guard.* **7**, 2015 (2015).
18. Lewis, D. & Brigder, D. Market Researchers make Increasing use of Brain Imaging. *Adv. Clin. Neurosci. Rehabil.* **5**, 36–37 (2004).
19. Kirkpatrick, K. Software-defined networking. *Commun. ACM* **56**, 16 (2013).
20. Ouyang, J., Lin, S., Jiang, S., Hou, Z., Wang, Y., Wang, Y., … Hou, Zhenyu; Wang, Yong; Wang, Y. SDF: software-defined flash for web-scale internet storage systems. in *Proceedings of the 19th international conference on Architectural support for programming languages and operating systems - ASPLOS '14* **42**, 471–484 (ACM Press, 2014).
21. Wark, T., Corke, P., Sikka, P., Klingbeil, L., Guo, Y., Crossman, C., … Bishop-Hurley, G. Transforming Agriculture through Pervasive Wireless Sensor Networks. *IEEE Pervasive Comput.* **6**, 50–57 (2007).
22. DiMase, D., Collier, Z. A., Heffner, K. & Linkov, I. Systems engineering framework for cyber physical security and resilience. *Environ. Syst. Decis.* **35**, 291–300 (2015).
23. World Economic Forum. *Partnering for Cyber Resilience Towards the Quantification of Cyber Threats*. (2015).
24. Koch, R. & Rodosek, G. *Proceedings of the 15th European Conference on Cyber Warfare and Security : ECCWS 2016 : hosted by Universität der Bundeswehr, Munich, Germany 7-8 July 2016*. (2016).
25. Ruan, K. Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Comput. Secur.* **65**, 77–89 (2017).
26. Roumani, M. A., Fung, C. C., Rai, S. & Xie, H. Value Analysis of Cyber Security Based on Attack Types. *ITMSOC Trans. Innov. Bus. Eng.* **01**, 34–39 (2016).
27. Anderson, R. & Moore, T. The Economics of Information Security. *Sci. AAAS* **314**, 610–613 (2006).
28. Gordon, L. A. & Loeb, M. P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **5**, 438–457 (2002).
29. Rodewald, G. & Gus. Aligning information security investments with a firm's risk tolerance. in *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05* 139 (ACM Press, 2005). doi:10.1145/1107622.1107654

30. Zhu, Q., Rieger, C. & Basar, T. A hierarchical security architecture for cyber-physical systems. in *2011 4th International Symposium on Resilient Control Systems* 15–20 (IEEE, 2011). doi:10.1109/ISRCS.2011.6016081

31. Rajkumar, R., Lee, I., Sha, L. & Stankovic, J. Cyber-Physical Systems: The Next Computing Revolution. in *Proceedings of the 47th Design Automation Conference on - DAC '10* 731 (ACM Press, 2010). doi:10.1145/1837274.1837461

32. Biener, C., Eling, M. & Wirfs, J. H. Insurability of Cyber Risk 1. *The Geneva Association* 1–4 (2014).

33. Shackelford, S. J. Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Rev.* **19**, 412–445 (2016).

34. Ribeiro, L., Barata, J. & Ferreira, J. An agent-based interaction-oriented shop floor to support emergent diagnosis. in *2010 8th IEEE International Conference on Industrial Informatics* 189–194 (IEEE, 2010). doi:10.1109/INDIN.2010.5549436

35. Thramboulidis, K. A cyber–physical system-based approach for industrial automation systems. *Comput. Ind.* **72**, 92–102 (2015).

36. Giordano, A., Spezzano, G. & Vinci, A. A Smart Platform for Large-Scale Cyber-Physical Systems. in 115–134 (Springer International Publishing, 2016). doi:10.1007/978-3-319-26869-9_6

37. Wahlster, W., Helbig, J., Hellinger, A., Stumpf, M. A. V., Blasco, J., Galloway, H. & Gestaltung, H. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. (2013).

38. Wan, J., Cai, H. & Zhou, K. Industrie 4.0: Enabling technologies. in *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things* 135–140 (IEEE, 2015). doi:10.1109/ICAIOT.2015.7111555

39. La, H. J. & Kim, S. D. A Service-Based Approach to Designing Cyber Physical Systems. in *2010 IEEE/ACIS 9th International Conference on Computer and Information Science* 895–900 (IEEE, 2010). doi:10.1109/ICIS.2010.73

40. Weyer, S., Schmitt, M., Ohmer, M. & Gorecky, D. Towards Industry 4.0 - Standardization as the crucial challenge for highly modular, multi-vendor production systems. *IFAC-PapersOnLine* **48**, 579–584 (2015).

41. Dillon, T. S., Zhuge, H., Wu, C., Singh, J. & Chang, E. Web-of-things framework for cyber-physical systems. *Concurr. Comput. Pract. Exp.* **23**, 905–923 (2011).

42. Faller, C. & Feldmüller, D. Industry 4.0 Learning Factory for regional SMEs. *Procedia CIRP* **32**, 88–91 (2015).

43. Wang, L., Törngren, M. & Onori, M. Current status and advancement of cyber-physical systems in manufacturing. *J. Manuf. Syst.* **37**, 517–527 (2015).

44. Stock, T. & Seliger, G. Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP* **40**, 536–541 (2016).

45. Hussain, F. Internet of Everything. in *Internet of Things: Building Blocks and Business Models: SpringerBriefs in Electrical and Computer Engineering* 1–11 (Springer International Publishing, 2017). doi:10.1007/978-3-319-55405-1_1

46. Hermann, M., Pentek, T. & Otto, B. Design Principles for Industrie 4.0 Scenarios. in

2016 49th Hawaii International Conference on System Sciences (HICSS) 3928–3937 (IEEE, 2016). doi:10.1109/HICSS.2016.488

47. Wang, S., Wan, J., Li, D. & Zhang, C. Implementing Smart Factory of Industrie 4.0: An Outlook. *Int. J. Distrib. Sens. Networks* **12**, 1–10 (2016).
48. Müller, J. M., Buliga, O. & Voigt, K.-I. Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. *Technol. Forecast. Soc. Change* (2018). doi:10.1016/J.TECHFORE.2017.12.019
49. Evans, P. C. & Annunziata, M. *Industrial Internet: Pushing the Boundaries of Minds and Machines*. (2012).
50. Jensen, J. C., Chang, D. H. & Lee, E. A. A model-based design methodology for cyber-physical systems. in *2011 7th International Wireless Communications and Mobile Computing Conference* 1666–1671 (IEEE, 2011). doi:10.1109/IWCMC.2011.5982785
51. Shi, J., Wan, J., Yan, H. & Suo, H. A survey of Cyber-Physical Systems. in *2011 International Conference on Wireless Communications and Signal Processing (WCSP)* 1–6 (IEEE, 2011). doi:10.1109/WCSP.2011.6096958
52. Wang, L., Wang, X. V., Gao, L. & Váncza, J. A cloud-based approach for WEEE remanufacturing. *CIRP Ann. - Manuf. Technol.* **63**, 409–412 (2014).
53. Ringert, J. O., Rumpe, B. & Wortmann, A. Architecture and Behavior Modeling of Cyber-Physical Systems with MontiArcAutomaton. (2015).
54. Bauer, W., Hämmerle, M., Schlund, S. & Vocke, C. Transforming to a Hyper-connected Society and Economy – Towards an "Industry 4.0". in *Procedia Manufacturing* **3**, 417–424 (2015).
55. Lee, J., Kao, H.-A. & Yang, S. Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. *Procedia CIRP* **16**, 3–8 (2014).
56. Tan, Y., Goddard, S. & Pérez, L. C. A Prototype Architecture for Cyber-Physical Systems. *ACM SIGBED Rev. - Spec. issue RTSS forum Deep. Embed. real-time Comput.* **5**, (2008).
57. Kang, W., Kapitanova, K. & Son, S. H. RDDS: A Real-Time Data Distribution Service for Cyber-Physical Systems. *IEEE Trans. Ind. Informatics* **8**, 393–405 (2012).
58. Longstaff, T. A. & Haimes, Y. Y. A holistic roadmap for survivable infrastructure systems. *IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans* **32**, 260–268 (2002).
59. Toro, C., Barandiaran, I. & Posada, J. A Perspective on Knowledge Based and Intelligent Systems Implementation in Industrie 4.0. *Procedia Comput. Sci.* **60**, 362–370 (2015).
60. Sokolov, B. & Ivanov, D. Integrated scheduling of material flows and information services in industry 4.0 supply networks. *IFAC-PapersOnLine* **48**, 1533–1538 (2015).
61. Benveniste, A. Loosely Time-Triggered Architectures for Cyber-Physical Systems. *2010 Des. Autom. Test Eur. Conf. Exhib. Dresden* 3–8 (2010). doi:doi: 10.1109/DATE.2010.5457246
62. Benveniste, A., Bouillard, A. & Caspi, P. A unifying view of loosely time-triggered architectures. in *Proceedings of the tenth ACM international conference on Embedded software - EMSOFT '10* 189 (ACM Press, 2010). doi:10.1145/1879021.1879047

63. Sangiovanni-Vincentelli, A., Damm, W. & Passerone, R. Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems * g. *Eur. J. Control* **18**, 217–238 (2012).

64. Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. & Yang, H. Next Big Thing in Big Data: The Security of the ICT Supply Chain. in *2013 International Conference on Social Computing* 1066–1073 (IEEE, 2013). doi:10.1109/SocialCom.2013.172

65. Woods, D., Agrafiotis, I., Nurse, J. R. C. & Creese, S. Mapping the coverage of security controls in cyber insurance proposal forms. *J. Internet Serv. Appl.* **8**, 8 (2017).

66. Nurse, J., Creese, S. & De Roure, D. Security Risk Assessment in Internet of Things Systems. *IT Prof.* **19**, 20–26 (2017).

67. Waslo, R., Lewis, T., Hajj, R. & Carton, R. Industry 4.0 and cybersecurity in the age of connected production | Deloitte University Press. *Deloitte University Press* (2017). Available at: https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html. (Accessed: 4th August 2017)

68. Bhave, A., Krogh, B., Garlan, D. & Schmerl, B. Multi-domain Modeling of Cyber-Physical Systems Using Architectural Views. *Proc. Anal. Virtual Integr. Cyber-Physical Syst. Work.* (2010).

69. Niggemann, O., Biswas, G., Kinnebrew, J. S., Khorasgani, H., Volgmann, S. & Bunte, A. Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control. in *International Workshop on the Principles of Diagnosis (DX)* 185–192 (2015).

70. Almeida, L., Santos, F. & Oliveira, L. Structuring Communications for Mobile Cyber-Physical Systems. in 51–76 (Springer International Publishing, 2016). doi:10.1007/978-3-319-26869-9_3

71. Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B. & Ralph, D. Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe. *Cambridge Risk Framew. Ser. Cent. Risk Stud. Univ. Cambridge.* (2014).

72. Petrolo, R., Loscri, V. & Mitton, N. Cyber-Physical Objects as Key Elements for a Smart Cyber-City. in 31–49 (Springer International Publishing, 2016). doi:10.1007/978-3-319-26869-9_2

73. Radanliev, P. Architectures for Green-Field Supply Chain Integration. *J. Supply Chain Oper. Manag.* **13**, (2015).

74. Radanliev, P. Supply Chain Systems Architecture and Engineering Design: Green-field Supply Chain Integration. *Oper. Supply Chain Manag. An Int. J.* **9**, (2016).

75. Radanliev, P. Engineering Design Methodology for Green-Field Supply Chain Architectures Taxonomic Scheme. *J. Oper. Supply Chain Manag.* **8**, 52–66 (2015).

76. Radanliev, P. Green-field Architecture for Sustainable Supply Chain Strategy Formulation. *Int. J. Supply Chain Manag.* **4**, 62–67 (2015).

77. Johnson, C., Badger, L., Waltermire, D., Snyder, J. & Skorupka, C. Guide to Cyber Threat Information Sharing. *NIST Spec. Publ.* 800–150 (2016). doi:10.6028/NIST.SP.800-150

78. CVSS. Common Vulnerability Scoring System SIG. *FIRST.org* (2017). Available at: https://www.first.org/cvss/. (Accessed: 26th December 2017)

79. FIRST. CVSS v3.0 Specification Document. Available at: https://www.first.org/cvss/specification-document#8-4-Metrics-Levels. (Accessed: 3rd October 2017)

80. Steup, M. *Epistemology: Stanford encyclopedia of philosophy*. (Stanford University. Center for the Study of Language and Information (U.S.), 2005).

81. Conee, E. & Feldman, R. *Evidentialism*. (Oxford University Press, 2004). doi:10.1093/0199253722.001.0001

82. Mittag, M. D. *The internet encyclopedia of philosophy*. (Internet Encyclopedia of Philosophy Pub, 2011).

83. Goldman, A. I. & Olsson, E. J. *Reliabilism and the Value of Knowledge*. (2009).

84. Conee, E. & Feldman, R. The Generality Problem for Reliabilism. *Philos. Stud. An Int. J. Philos. Anal. Tradit.* **89**, 1–29 (1998).

85. Comesaña, J. The Diagonal and the Demon. *Philos. Stud.* **110**, 249–266 (2002).

86. IIC. *The Industrial Internet of Things Volume G5: Connectivity Framework; Industrial Internet Consortium*. (2017).

87. IIC. *The Industrial Internet of Things, Volume B01: Business Strategy and Innovation Framework; Industrial Internet Consortium*. (2016). doi:IIC:PUB:B01:V1.0:PB:20161115

88. DCMS. *UK Digital Strategy 2017 - GOV.UK; Department for Culture, Media and Sport*. (2017).

89. IVI. *Industrial Value Chain Reference Architecture; Industrial Value Chain Initiative*. (2017).

90. IVI. Industrial Value Chain Initiative. An Outline of Smart Manufacturing Scenarios 2016. in *Monozukuri Nippon Conference* (2016).

91. ASI, A. for strategic initiatives. National Technology initiative, Agency for Strategic Initiatives. *Government of Russia* (2016). Available at: https://asi.ru/eng/nti/. (Accessed: 10th May 2017)

92. Industrie 4.0. Plattform Industrie 4.0 - Testbeds. (2017). Available at: http://www.plattform-i40.de/I40/Navigation/EN/InPractice/Testbeds/testbeds.html. (Accessed: 13th May 2017)

93. Sirris and Agoria. Made Different: Factory of the Future 4.0. (2017). Available at: http://www.madedifferent.be/en/what-factory-future-40. (Accessed: 9th May 2017)

94. John, P. *High Value Manufacturing Catapult*. (2017).

95. Caralli, R. A., Stevens, J. F., Young, L. R. & Wilson, W. R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. (2007).

96. Catapult UK. The Catapult Programme - Catapult. (2017). Available at: https://catapult.org.uk/. (Accessed: 13th May 2017)

97. MIUR. Italian Technology Cluster: Intelligent Factories; Ministry of Education Universities and Research. *Cluster Tecnologico Nazionale Fabbrica Intelligente | Imprese, università, organismi di ricerca, associazioni e enti territoriali: insieme per la crescita del Manifatturiero* (2014). Available at: http://www.fabbricaintelligente.it/en/. (Accessed: 9th May 2017)

98. GTAI. *Industrie 4.0 Smart Manufacturing for the Future*. (2014).

99. NIF. *New Industrial France: Building France's industrial future - updated text from the 2013 version*. (2016).

100. SCPRC. Made in China 2025; The State Council People Republic of China. *www.english.gov.cn* (2017). Available at: http://english.gov.cn/2016special/madeinchina2025/. (Accessed: 10th May 2017)

101. Bouws, T., Kramer, F., Heemskerk, P., Van Os, M., Van Der Horst, T., Helmer, S., … De Heide, M. *Smart Industry: Dutch Industry Fit for the Future*. (2015). doi:527727

102. MEICA. *Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa; Ministry of Economy Industry and Competitiveness Accessibility*. (2015).

103. G20. *G20 New Industrial Revolution Action Plan*. (2016).

104. Kim, J. Are countries ready for the new meso revolution? Testing the waters for new industrial change in Korea. *Technol. Forecast. Soc. Change* (2017). doi:10.1016/J.TECHFORE.2017.11.006

105. AMP. *Advanced Manufacturing Partnership*. *NIST Advanced Manufacturing Office* (2013).

106. METI. *NRS, New Robot Strategy - Vision Strategy and Action Plan; Ministry of Economy Trade and Industry of Japan*. (2015).

107. METIJ. *RRI, Robot Revolution Initiative - Summary of Japan's Robot Strategy - It's vision, strategy and action plan; Ministry of Economy, Trade and Industry of Japan*. (2015).

108. NIST, C. *Cybersecurity Framework | NIST*. *NIST Website* (2016).

109. Wynn, J., Whitmore, G., Upton, L., Spriggs, D., McKinnon, R., McInnes, R., … Clausen, J. *Threat Assessment & Remediation Analysis (TARA) Methodology Description Version 1.0*. (2011).

110. CMMI. What Is Capability Maturity Model Integration (CMMI)®? | CMMI Institute. *CMMI Institute* (2017). Available at: http://cmmiinstitute.com/capability-maturity-model-integration. (Accessed: 26th December 2017)

111. RiskLens. Risk Analytics Platform | FAIR Platform Management. (2017). Available at: https://www.risklens.com/platform. (Accessed: 26th December 2017)

112. FAIR. What is a Cyber Value-at-Risk Model? (2017). Available at: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model. (Accessed: 26th December 2017)

113. Shaw, R., Takanti, V., Zullo, T., Director, M. & Llc, E. *Best Practices in Cyber Supply Chain Risk Management Boeing and Exostar Cyber Security Supply Chain Risk Management Interviews*. (2017).

114. U.S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2) | Department of Energy*. (2014).

115. Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G. & Feldman, L. *Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies*. (2017).

116. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*. (2014).

117. NIST. Update to Cybersecurity Framework | NIST. *National Institute of Standards and Technology, U.S. Department of Commerce* (2017). Available at: https://www.nist.gov/news-events/news/2017/12/update-cybersecurity-framework. (Accessed: 31st March 2018)

118. Buith, J. *Cyber Value at Risk in the Netherlands*. (2016).

119. FAIR. Quantitative Information Risk Management | The FAIR Institute. *Factor Analysis of Information Risk* (2017). Available at: http://www.fairinstitute.org/. (Accessed: 26th December 2017)

120. ISO. ISO - International Organization for Standardization. (2017). Available at: https://www.iso.org/home.html. (Accessed: 26th December 2017)

121. Jacobs, V., Bulters, J. & Van Wieren, M. Modeling the Impact of Cyber Risk for Major Dutch Organizations.

122. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Eirini Anthi, Ani, U., … Montalvo, R. M. *Design principles for cyber risk impact assessment from Internet of Things (IoT). Wokring paper.* (2019). doi:10.13140/RG.2.2.33014.86083

123. Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S. & Burnap, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **102**, 14–22 (2018).

124. Nurse, J. R. C., Radanliev, P., Creese, S. & De Roure, D. Realities of Risk: 'If you can't understand it, you can't properly assess it!': The reality of assessing security risks in Internet of Things systems. in *Living in the Internet of Things: Cybersecurity of the IoT - 2018* 1–9 (The Institution of Engineering and Technology, 2018). doi:10.1049/cp.2018.0001

125. Taylor, P., Allpress, S., Carr, M., Lupu, E., Norton, J., Smith, L., Blackstock, J., Boyes, H., Hudson-Smith, A., Brass, I., Chizari, H., Cooper, R., Coulton, P., Craggs, B., Davies, N., De Roure, D., Elsden, M., Huth, M., Lindley, J., Maple, C., Mittelstadt, B., Nicolescu, R., Nurse, J., Procter, R., Radanliev, P., Rashid, A., Sgandurra, D., Skatova, A., Taddeo, M., Tanczer, L., Vieira-Steiner, R., … R.J., Westbury, P. S. *Internet of Things realising the potential of a trusted smart world*. (2018).

126. Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. ., Nicolescu, R. & Huth, M. Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. in *Living in the Internet of Things: Cybersecurity of the IoT - 2018* 3 (9 pp.) (Institution of Engineering and Technology, 2018). doi:10.1049/cp.2018.0003

127. Radanliev, P., De Roure, C. D., Nurse, .R.C., Nicolescu, R., Huth, M., Cannady, C. & Montalvo, R. M. Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-things in Industry 4.0. in *Living in the Internet of Things: Cybersecurity of the IoT - 2018* 41 (6 pp.)-41 (6 pp.) (IET, 2018). doi:10.1049/cp.2018.0041

128. Nicolescu, R., Huth, M., Radanliev, P. & De Roure, D. Mapping the values of IoT. *J. Inf. Technol.* 1–16 (2018). doi:10.1057/s41265-018-0054-1

129. Radanliev, P., De Roure, D. C., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. *New developments in Cyber Physical Systems, the Internet of*

Things and the Digital Economy – future developments in the Industrial Internet of Things and Industry 4.0. (2019). doi:10.13140/RG.2.2.14133.93921

130. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Rafael, M. M. & Burnap, P. *Supply Chain Design for the Industrial Internet of Things and the Industry 4.0*. (2019). doi:10.13140/RG.2.2.36311.32160

131. Radanliev, P., Charles De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R. & Ani, U. *Cyber Risk in IoT Systems*. *Journal of Cyber Policy* (2019). doi:10.13140/RG.2.2.29652.86404

132. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *Definition of Internet of Things (IoT) Cyber Risk – Discussion on a Transformation Roadmap for Standardisation of Regulations, Risk Maturity, Strategy Design and Impact Assessment*. (Preprints, 2019). doi:10.13140/RG.2.2.17305.88167

133. Radanliev, P., DeRoure, D., Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *Definition of Cyber Strategy Transformation Roadmap for Standardisation of IoT Risk Impact Assessment with a Goal-Oriented Approach and the Internet of Things Micro Mart. Working paper.* (2019). doi:10.13140/RG.2.2.12462.77124

134. Radanliev, P., De Roure, D., Nicolescu, R. & Huth, M. *A reference architecture for integrating the Industrial Internet of Things in the Industry 4.0. Working paper.* (2019). doi:10.13140/RG.2.2.26854.47686

135. Radanliev, P., De Roure, D., Nurse, J. R. C. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. *Cyber risk impact assessment – assessing the risk from the IoT to the digital economy*. (2019). doi:10.13140/RG.2.2.11145.49768

136. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. & Burnap, P. *The Industrial Internet-of-Things in the Industry 4.0 supply chains of small and medium sized enterprises*. *Working paper.* (2019). doi:10.13140/RG.2.2.14140.49283

137. Radanliev, P., Charles De Roure, D., Nurse, J. R. C., Burnap, P. & Montalvo, R. M. *Methodology for designing decision support supply chain systems for visualising and mitigating cyber risk from IoT technologies*. *Working paper.* (2019). doi:10.13140/RG.2.2.32975.53921

138. Radanliev, P. A conceptual framework for supply chain systems architecture and integration design based on practice and theory in the North Wales slate mining industry. (British Library, 2014). doi:ISNI: 0000 0004 5352 6866

139. Nicolescu, R., Huth, M., Radanliev, P. & De Roure, D. *State of The Art in IoT - Beyond Economic Value*. (2018).

140. Axon, L., Alahmadi, B., Nurse, J. R. C., Goldsmith, M. & Creese, S. Sonification in Security Operations Centres: What do Security Practitioners Think? in *Proceedings of the Workshop on Usable Security (USEC) at the Network and Distributed System Security (NDSS) Symposium* 1–12 (2018).

141. Eggenschwiler, J., Agrafiotis, I. & Nurse, J. R. Insider threat response and recovery strategies in financial services firms. *Comput. Fraud Secur.* **2016**, 12–19 (2016).

142. de Reuver, M., Sørensen, C. & Basole, R. C. The digital platform: a research agenda. *J. Inf. Technol.* 1–12 (2017). doi:10.1057/s41265-016-0033-3

143. Viljoen, T., Hobbis, D., Thomas, R., Stathos, G., Blatchford, I. & Maharaj, S. *Cyber*

security Empowering the CIO. (2014).

144. Laugé, A., Hernantes, J. & Sarriegi, J. M. Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *Int. J. Crit. Infrastruct. Prot.* **8**, 16–23 (2015).

145. Bilal, M. A Review of Internet of Things Architecture , Technologies and Analysis Smartphone-based Attacks Against 3D printers. *arXiv Prepr. arXiv1708.04560* 1–21 (2017).

146. Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D. Cascading Effects of Common-Cause Failures in Critical Infrastructures. in *Critical Infrastructure Protection VII* (eds. Butts, J. & Shenoi, S.) **417**, 171–182 (Springer Berlin Heidelberg, 2013).

147. Bloomfield, R., Buzna, L., Popov, P., Salako, K. & Wright, D. *Stochastic modelling of the effects of interdependencies between critical infrastructure*. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **6027 LNCS**, (Springer Berlin Heidelberg, 2010).

148. Ani, U. D., Daniel, N. C. & Adewumi, S. E. Evaluating Industrial Control System (ICS) Security Vulnerability through Functional dependency Analysis. *J. Comput. Sci. its Appl.* **25**, 73–89 (2018).

149. Zhang, P. & Peeta, S. A generalized modeling framework to analyze interdependencies among infrastructure systems. *Transp. Res. Part B Methodol.* **45**, 553–579 (2011).

150. Setola, R., De Porcellinis, S. & Sforna, M. Critical infrastructure dependency assessment using the input-output inoperability model. *Int. J. Crit. Infrastruct. Prot.* **2**, 170–178 (2009).

151. Huang, J., Chen, G. & Cheng, B. A stochastic approach of dependency evaluation for IoT devices. *Chinese J. Electron.* **25**, 209–214 (2016).

152. Nozick, L. K., Turnquist, M. A., Jones, D. A., Davis, J. R. & Lawton, C. R. Assessing the performance of interdependent infrastructures and optimizing investments. in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the* **00**, 7 pp. (2004).

153. Qiao, J., Jeong, D., Lawley, M., Richard, J.-P. P., Abraham, D. M. & Yih, Y. Allocating security resources to a water supply network. *IIE Trans.* **39**, 95–109 (2007).

154. Stergiopoulos, G., Kotzanikolaou, P., Theocharidou, M., Lykou, G. & Gritzalis, D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. *Int. J. Crit. Infrastruct. Prot.* **12**, 46–60 (2016).

155. Mell, P., Scarfone, K. & Romanosky, S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. *FIRSTForum Incid. Response Secur. Teams* 1–23 (2007).

156. Chejara, P., Garg, U. & Singh, G. Vulnerability Analysis in Attack Graphs Using Conditional Probability. *Int. J. Soft Comput. Eng. 13* **3**, 18–21 (2013).

157. Weinberg, M. D. Computational statistics using the Bayesian Inference Engine. *Mon. Not. R. Astron. Soc.* **434**, 1736–1755

158. Hanson, K. M. & Cunningham, G. S. *THE BAYES INFERENCE ENGINE*. *Maximum Entropy and Bayesian Methods* (1996).

159. Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R. & Huth, M.

Analysing IoT cyber risk for estimating IoT cyber insurance. (2019). doi:10.13140/RG.2.2.25006.36167

160. Radanliev, P., De Roure, D. C., Nurse, J. R. C., Montalvo, R. M. & Burnap, P. *Standardisation of cyber risk impact assessment for the Internet of Things (IoT)*. (2019). doi:10.13140/RG.2.2.27903.05280

161. Radanliev, P., Roure, D. C. De, Nurse, J. R. C., Burnap, P., Anthi, E., Ani, U., … Montalvo, R. M. *Cyber risk from IoT technologies in the supply chain – decision support system for the Industry 4.0*. (2019). doi:10.13140/RG.2.2.17286.22080

162. Radanliev, P., De Roure, D., Nurse, J. R., Burnap, P., Anthi, E., Ani, U., … Mantilla Montalvo, R. Cyber risk from IoT technologies in the supply chain-discussion on supply chains decision support system for the digital economy. *Univ. Oxford* (2019). doi:10.13140/RG.2.2.17286.22080

163. Radanliev, P., Roure, D. De, Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. New Developments in Cyber Physical Systems, the Internet of Things and the Digital Economy – Discussion on Future Developments in the Industrial Internet of Things and Industry 4.0. (2019). doi:10.20944/PREPRINTS201903.0094.V1

164. Radanliev, P., Roure, D. De, Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S. & Montalvo, R. M. Cyber Risk impact Assessment - Assessing the Risk from the IoT to the Digital Economy. *Univ. Oxford* (2019). doi:10.20944/PREPRINTS201903.0109.V1

165. Radanliev, P., Rowlands, H. & Thomas, A. Supply Chain Paradox: Green-field Architecture for Sustainable Strategy Formulation. in *Cardiff: Sustainable Design and Manufacturing 2014, Part 2, International Conference* (eds. Setchi, R., Howlett, R. J., Naim, M. & Seinz, H.) 839–850 (Future Technology Press, 2014).