RISK ASSESSMENT METHODS FOR CONVERGED IOT AND SCADA SYSTEMS: REVIEW AND RECOMMENDATIONS

Rakan Aldmour, Pete Burnap, Mike Lakoju
School of Computer Science & Informatics, University of Cardiff, Wales, UK,
Aldmourr@cardiff.ac.uk*, burnapp@cardiff.ac.uk , lakojum@cardiff.ac.uk

Abstract
Risk assessment is used to identify, estimate and prioritise risks that could impact organisations. Existing risk assessment methods are not particularly adapted to include dynamic systems such as the Internet of Things (IoT). Recently, IoT has been used to develop a natural extension of Supervisory Control and Data Acquisition (SCADA) systems that support industrial control in various sectors such as transportation, energy, and manufacturing. However, incorporating IoT systems without due attention to new risks posed could enable attacks, increase the cybersecurity concerns, and impact operations and safety. In this paper, special considerations for risk assessment methods in the context of converged IoT and SCADA systems are identified, and we present recommendations for the inclusion of the special considerations alongside standard methods for managing risks.

Keywords: ICS/SCADA/IoT systems risk assessment, Converge ICS/SCADA/IoT systems

1 Introduction
Internet of Things (IoT) is a collection of devices, sensors, and services that exist in an interconnected ecosystem with the aim of sharing data within and between systems. The number of connected things is predicted to reach up 50 billion by 2020 [1]. IoT technology has four core elements (1) Internet: to provide anywhere, anytime communication between devices and Cloud using Wireless or cellular. (2) Perception: the embedded communication hardware, for example barcodes, actuators, and tags. This element is responsible for collecting real data from the physical environment, processing data locally at the edge of the network, then transferring it to other devices through the network. (3) Middleware: This is used to connect IoT components such as people, objects, and services, etc. (4) Presentation: Visualisation of the data acquired and analytical results [2]. The proposed benefits of IoT are to improve and facilitate application quality, cost reduction, enhance functionality and automation, and increase access to resources as well as optimise real-time operations in daily life [6].

In industrial applications, IoT can support process optimisation and factory management [2]. Although IoT systems offer many benefits, they are still vulnerable to existing Internet-enabled attacks and threats to privacy. Indeed IoT adds a new layer of vulnerability, which is arguably more difficult to harden against attacks due to lower compute power on devices [3]. Moreover, bringing IoT technology to the industrial environment could increase security concerns because, in the industrial setting, security is often related to safety. For example, a breach in security in a factory could damage the machines and cause injury to the human operators [2]. In the industrial sector, IoT is a natural extension of Supervisory Control and Data Acquisition (SCADA) systems [4]. SCADA is used to monitor and control safety critical industrial equipment and forms part of many existing industrial control systems (ICS) which serve Critical National Infrastructure (CNI) such as transportation, water, and energy. Due to increased connectivity and sensory capability, IoT has the potential to support significant advances in SCADA systems but arguably opens up one of the most disruptive threat surfaces to potential attackers.

Risk assessments are used to "identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems." [5]. Risk assessment is an essential element of best practice in SCADA and ICS systems [6] to ensure threats are actively managed and mitigated [7]. Without risk assessment, threats can lead to injury if the system is breached [2], or privacy, confidentiality and integrity breaches [7]. This indicates the importance of an appropriate risk assessment analysis [7]. However, risk assessment methods for IoT systems have challenges, because the majority of methods were designed and proposed prior to the uptake of IoT which has a dynamic and pervasive nature [8]. This means they may not capture and support the complexity or pervasiveness in IoT systems. Therefore, the new threats posed by converging IoT and industrial systems such as SCADA may be not captured and managed, subsequently leading to cyberattack [9].

SCADA and IoT systems have been discussed in various academic publications and industry whitepapers. In this paper, previously published works have been studied and analysed to define and understand the strengths and weaknesses of existing risk assessment methods when considering the convergence of ICS/SCADA systems and IoT. We identify some special considerations that are required to be included alongside risk assessment methods for such converged systems and critique existing methods with this in mind. From our analysis, we propose that a hybrid risk assessment method for converged ICS/SCADA

and IoT systems could be followed, and identify points in the standard risk assessment and management process where our proposed considerations are most relevant.

2 Embedding IoT in SCADA Systems

SCADA systems collect data and remotely control ICS systems consisting of hardware, software, and communication. IoT capabilities, such as processing, storage, interfaces, sensing, actuating, and software usage & management are complimentary to SCADA and thus a natural extension of Internet connected control systems [11].

2.1 Enhancement in SCADA when using IoT

SCADA systems focus on controlling and monitoring equipment, while Industrial IoT (IIoT) offers a wider range of possibilities, including the ability to analyse and predict control requirements at the edge of the network [12]. Despite their added value, there are a range of different types of attacks on IoT system [13] e.g.:

1. Physical Attacks: these types of attacks are related to hardware components, such as particle beam techniques, layout reconstruction, de-packaging of chip, and micro-probing.
2. Side Channel Attacks: these attacks are based on Side Channel Information which could be retrieved from the encryption device. Encryption devices create timing information which includes power consumption statistics and radiation of various sorts. Side channel attacks use this information to recover the key the device is using.
3. Cryptanalysis attacks: these kinds of attacks are focused on ciphertext and breach the encryption, such as Man-in-the-middle attack, chosen-plaintext attack, and ciphertext-only attack.
4. Software Attacks: this type of attack consists of using worms or viruses, trojan horse, and exploiting buffer overflows to reach the system and inject malicious code.
5. Network Attacks: there is a possibility of network security attacks for wireless communication systems due to the transmission medium. The attacks are categorised into two types: *active,* such as denial of service attacks and *passive* attacks such as traffic analysis.

Thus, when converging IoT and SCADA systems, it is important to have a suitable set of risk assessment methods than capture the threats posed in both systems and can provide a structure to handle the differences and complexity of both independently while capturing the risks of the converged systems. In the sections that follow we provide an overview of risk assessment, the methods for IoT and SCADA, and make recommendations on how to synthesize them into a single IoT/SCADA risk model.

3 Risk Assessment in IoT and SCADA

3.1 Risk Management Stages

The process of risk management as defined in ISO 31000:2009(E) and ISO/IEC 27005:2011, is divided into levels as shown below [8]:

- **Context Establishment:** define the scope for risk management process and adjust procedures to assess risks.
- **Risk Identification**: find, recognize, and describe risk.
- **Risk Analysis:** network overview and security architecture, analysis of the infrastructure, connections between components.
- **Risk Evaluation:** risk profile, failure mode, attack mode, and effects.
- **Risk Treatment:** develop a variety of options to mitigate risks, then create action plans.

Developing a risk model requires processes such as:
1.Defining the assets / use cases (depending on whether a component / system level method is used): defining components, business objectives/perspectives; building a use case for each variation;
2.Identifying likely vulnerabilities: data flows, interfaces and possible attack surfaces;
3.Identifying threats: analysing and understanding the threats to defined vulnerabilities;
4.Identifying related impacts: including the worst-case scenarios and covering all related external threats with all possibilities [14].

3.2 Special Considerations for ICS/SCADA Risk Assessment

The considerations are adapted in the most part from work in [10].

3.2.1 Consideration 1: Safety and Security Risk Assessment

A major concern for risk assessments in SCADA is safety and physical systems; while information security risk assessments are often focussed on the digital world. However, it is likely that physical and digital worlds overlap in an ICS environment. It is essential that we consider both aspects when performing risk framing, risk tolerance, and safety assessments [10].

3.2.2 Consideration 2: Potential Physical Impacts of an ICS Incident

Consider the physical impact of an ICS incident. The impact might be inside the ICS factory and effect physical processes such as a steam or gas leak; or it could be an external impact in the wider environment such as pollution, fire and contamination [10].

3.2.3 Consideration 3: Incorporating Non-digital Aspects of ICS

The impact on the ICS cannot be well-defined if only focused on the digital features of the system. There are non-digital mechanisms that offer fault tolerance and ensure ICS operate within acceptable parameters. Such mechanisms could help to reduce any negative impact and must be integrated into the risk assessment process. An example of an ICS non-digital control is a mechanical relief pressure valve. This can prevent the ICS from working outside of a safe boundary, so it restricts the impact of an attack. The failure of this non-digital asset would need to be considered in the risk

assessment along with analogue warning mechanisms, such as meters and alarms [10].

3.2.4 Consideration 4: Considering the Propagation of Impact to Connected Systems

Evaluating the impact of the incident should include the impact that might propagate into other systems that are interconnected with an ICS internally or external to the organisation. The impact propagation might occur to physical and logical dependencies. The system could be impacted, for example when a virus or worm propagates to a connected ICS [10].

3.3 Special Considerations for IoT Risk Assessment

The considerations are adapted in the most part from work in [9].

3.3.1 Consideration 1: Periodic Risk Assessment is Not Dynamic Enough

IoT being dynamic and ad-hoc means that static or periodic risk assessment may not be suitable. For example, adding new devices to an ad-hoc IoT system is likely to introduce the possibility of a new threat surface [9].

3.3.2 Consideration 2: Changing Boundaries, Limited Systems Knowledge

As IoT devices may be added within different parts of the system, or at the edge of a network, the boundaries of perimeter security are blurred. This creates a challenge to deal with change or shift in the boundaries and scope of a risk assessment [9].

3.3.3 Consideration 3: Heterogeneity Within Systems

IoT systems with a range of devices and actors will establish a wide range of connections. This may bring many advantages such as enriched information, greater situational awareness, higher quality services & products, and quicker response. The inner workings of the IoT devices, such as how they process data & respond, and how inputs create outputs vary across devices, which makes it difficult to capture the risk of attacks between different devices in a single system. There is therefore a need for risk assessment to consider the logical components within IoT devices [9].

3.3.4 Consideration 4: Failure to Consider Assets as an Attack Platform

In current risk assessment methods, assets are mostly considered as value to the organisation, not as an attack platform. Recent IoT based attacks such as Mirai [15], have shown this to be a major risk. So it is crucial to accommodate this in the risk assessment process [9].

4 Risk Assessment Models for SCADA Systems and IoT

4.1 Assessment Methods for SCADA Systems

In this section we review existing risk assessment methods for SCADA with a view to meeting the SCADA Special Considerations (SSC) set out in section 3.2. Note this is not an exhaustive analysis due to page limitations. We propose future extensions could follow the same mapping process.

4.1.1 RAIM Model [16]

RAIM is a security framework for SCADA systems consisting of four sections (real-time monitoring, anomaly detection, impact analysis and mitigation strategies). Real time monitoring, and anomaly detection are based on the continuous monitoring in the system log and they require data collection for impact analysis to study intrusion behaviour and the possibility of cyber-attack on SCADA systems. This process consists of four steps: **1)** capture the system configurations, **2)** power flow simulation, **3)** vulnerability index computation, and **4)** security enhancement. Impact analysis is based on an attack tree. The indices are computed based on the historical data of intrusion, security countermeasures and password policies [16]. Meets SSC 1.

4.1.2 Quantitative methodology to assess cyber security risk of SCADA systems [17]

This model is based on power flow tracing and optimal power flow. Four SCADA system components (SCADA server, communication network, EMS server, and RTU), and fifteen types of threats are distinguished in this model. To define the vulnerabilities, there is a need to initially define the relevance between each threat with each component. Then assign a vulnerability index for each component in the system. This vulnerability index depends on the security characteristics and on historical data. To quantify the threat for each element of the SCADA systems, a normalised weighted index is allocated for each threat type. This is based on the applicability of the threat for each component, the vulnerability index of the component, and the extent of the component damage. Risk is computed in financial terms.[17]. Meets SSC 2 and 4.

4.1.3 Risk assessment in SCADA for railways [18]

Hierarchical Holographic Modelling (HHM) is a risk assessment framework, designed for GPS-based SCADA systems. HHM method works by "*capturing and representing the essence of the inherent diverse characteristics and attributes of a system"* [19]. HMM is used to model the complex defence and civilian systems, to assess risks among subsystems and reveal their impact on the entire system. There are three types of sub-models in HHM of ICS system; 1) hardware and software, 2) human supervisory, 3) environment. Each sub-model is decomposed into parts, and each part divided into subtopics. To assist in identification risk, HHM recommends to map the Control Objectives for Information and Related Technology (COBIT) to a holographic paradigm [18]. Meets SSC 1 and 4.

4.1.4 Digraph Model [20]

This model offers a formal description of the structure and behaviour of SCADA systems, and it can be used for risk impact assessment and fault diagnosis. The SCADA components are presented in the vertices of a graph. Fault diagnosis is defined as a process of revealing the components which could lead to failure in ICS systems or part of it. For this fault, a graph is used to identify the source fault in case a fault is detected in any of the components. Four steps for risk

identification and management include: 1) computing a reachability matrix, 2) computing partitions, 3) computing the separate parts partition, 4) finding the impact set for each partition. Meets SSC 2 and 4 [20].

4.1.5 Network Security Risk Model (NSRM) [21]

NSRM model is developed to represent attacks in a directed graph that allows formal, explicit representation of a SCADA system. The nodes in the diagraph describe the system components, and the edges the relationship between them. The main value of NSRM is to support selecting risk assessment controls by calculating the measure for a baseline version of the system and comparing to a 'secured' version. NSRM consists of eight steps: 1) identifying the dimensions of risk such as lost production, environmental damage, and supply chain, 2) analyse the infrastructure in a hierarchical model, 3) categorise the process to failure modes and impacts, 4) specify model processes and process disruption modes, 5) conduct an attack scenario, 6) categorise network security structure, 7) decompose the control network, 8) define the process interruption modes and resource needs. Based on the findings attack scenarios and associated risks will be identified [21]. Meets SSC 2,4 and partially 1.

From the analysis of SCADA risk assessment methods in terms of the special considerations as discussed in section 3.2, the selection of methods taken from the literature partially address the considerations. However, none of them addressed the non-digital aspect. The NSRM model developed by Henry & Haimes (2009) [21] appears to demonstrate the broadest coverage of the methods studied.

4.2 IoT and Risk Assessment Models

In this section we review existing risk assessment methods for IoT with a view to meeting the IoT Special Considerations (ISC) set out in section 3.3. Note this is not an exhaustive analysis due to page limitations. We propose future extensions could follow the same mapping process.

4.2.1 A Risk Assessment Methodology for IoT [7]

A risk assessment approach is developed to check the robustness of an IoT system using a method called NetwOrked Smart objects (NOS) [22]. It supports static and dynamic components of an IoT system. The risk analysis method considers the entire life cycle for an IoT platform. There are four major steps in this method; **1)** identify the vulnerabilities and develop an attack tree for a specific risk, **2)** identify the probable dependencies among the vulnerabilities, **3)** define exploitability values for identified vulnerabilities, **4)** present results to allow risk managers to view the outcomes of the risk analysis [7]. Meets ISC 1, 2, 3, and partially 4.

4.2.2 A novel risk assessment model in IoT [23]

An approach is proposed to manage probabilistic evaluation factors and discover the weight of effect in different propagation routes. The model considers the probabilistic interface and generates risk value probability in terms of the assets and propagation through using Bayesian Network (BN). Through BN, it is possible to reveal the risk propagation routes and compute weights by using DEMATEL. DEMATEL is employed to analyse relationships between factors such as threats and vulnerabilities, then convert the relationships into a comprehensive structure. The model helps to obtain countermeasure recommendations for decision makers, reduce risks to an adequate level, and evaluate the results [23]. Meets ISC 1 and 4.

4.2.3 Ontology development for run-time safety management methodology in Smart Work Environments using ambient knowledge[24]

This method is developed for run-time safety management of a Smart Work Environment (SWEs) as they employ IoT Services in safety and security. The approach consists of four main parts: (1) define the core methodology steps for run-time safety management, (2) create an ontological knowledge base for the safety in the work environment, (3) define the constraints based on safety protocols, (4) communicate information to each actor. The model contains a dashboard to support actors (risk managers) in making decisions on appropriate risk strategies. In addition, a safety expertise ontology is proposed based on the guidelines and directives in occupational safety, such as Occupational Safety and Health Regulations, and risk management standards such as ISO 31000:200. [24]. Meets ISC 1.

4.2.4 A Framework for Modeling and Assessing Security of the Internet of Things [25]

The framework is developed to represent all possible attack in IoT systems, assess the security degree using security metrics, and evaluate the effectiveness of the defence. The model consists of five steps:1) pre-processing: create IoT network from the required inputs such as number of nodes, network topology, and the vulnerabilities, 2) security model generation: compute the possible attacks towards an IoT network using the constructed network as input, 3) Visualise the generated attack paths, 4) security analysis: analyse the attack paths using a security evaluator, 5) the security analysis results show the most vulnerable aspects, helping decision makers to determine appropriate defence strategies [25]. Meets ISC 3 and partially 1.

From the analysis of IoT risk assessment methods in terms of the special considerations as discussed in section 3.3, the selection of methods taken from the literature broadly addressed the need to consider the dynamic nature of IoT devices; though the ability to address changing perimeter boundaries and heterogeneity within systems was limited. This could make it difficult to depict the risk of attacks among various devices in a single system. The only model that addressed the majority of the special considerations was developed by Sabrina et al., (2018) [7]. Therefore, this model represents the best fit for the special IoT requirements

4.3 Proposed Model

A comprehensive risk assessment model when converging IoT/ SCADA is required to help organisations to manage threats emerging from converged IoT and SCADA environments. From our analysis, the NSRM model

developed by Matthew & Yacov [21] best fits from an ICS/SCADA perspective (meets considerations 2,4 and partially 1), and Sabrina et al., (2018) [7] best fits from the IoT perspective (meets considerations 1,2,3, and partially 4). As these two methods best address the considerations as discussed in sections 3.2 and 3.3, it may be possible to merge them to form a hybrid approach for undertaking risk assessment when embedding IoT in SCADA, and future work will explore the possibility of this.

In addition to the potential for merging these approaches, we have suggested (below) some points within the general risk assessment process (as discussed in section 3.1) where the proposed special considerations could be addressed in the *context of converged SCADA and IoT systems*. Note, this is *not a complete process*, rather a subset of the overall risk assessment and management process with reflection on the special requirements for SCADA and IoT as discussed in sections 3.2 and 3.3. For a more complete overview of the risk assessment and management process study the established standards (e.g. NIST [5] and ISO/IEC 27005:2011), and guidelines (e.g. NCSC Risk Management Collection[1] and NIST IoT considerations [11]):

1.Preparation/Identification: The identification phase involves defining the scope of the risk assessment, ensuring the wider systems boundaries are considered where systems are interconnected (ISC 2). Identify all IoT and SCADA assets – ensuring non-digital assets are included (SSC 3). Categorise assets into data type, communication mode (e.g., discrete or streaming communication), and data flows in and out of the system. This must also be *performed and updated regularly* as systems may change dynamically with the inclusion of IoT devices (ISC1).

2.Analysis: Analyse the assets identified in phase 1 to identify likely vulnerabilities and possible attack surface. For IoT, it may be possible to use the NOS middleware from Sabrina et al., (2018) model [7] to understand the logical flows of data within IoT devices, which is a key requirement given devices are heterogeneous and therefore are prone to different risks (ISC3). Consider also safety aspects and physical impact of attacks both inside and outside the environment (SSC 1 and 2). It is important to consider dependencies between assets and processes also. It is unlikely they exist independently from other aspects of the system (SSC4)

3. Evaluate threat: Identify and evaluate threats that may exploit system vulnerabilities identified in phase 2. Threats to integrity, privacy, and confidentially for each of the data flows should be considered. Furthermore, define core process failure modes and their impacts on the interconnected systems, including impacts to and from supply chains (SSC 4). Consider how the threats may exploit system assets to launch further attacks – this means considering interconnected systems in anticipation of attacks pivoting onto connected networks. It also includes launching further attacks on wider Internet-connected systems (e.g. being used as part of a botnet) (ISC4). Threats need to be scored in terms of their potential impact so levels of expected disruption must be considered for each threat.

4. Treatments and Maintenance:
The following steps highlight some of the treatment and maintenance considerations with a particular focus on the special requirements:

1. Action Prioritisation: this is based on the threat levels from phase 3. For example, if the threat is very high this required immediate corrective action. A ranked list of actions ranking from high to low should result from the threats prioritisation exercise It is important to consider the propagation impact (SSC4) to systems which are connected with ICS systems whether these are internal or external the organisation, as this could impact physical and logical dependencies (SSC2).
2. Evaluate Recommended Response: Judge the feasibility (compatibility, user acceptance) and the effectiveness (level of protection) (SSC1) of the most appropriate control options to minimise the risks, including legal aspects (e.g. health and safety) (SSC2). The output should include a list of possible controls to prevent or reduce risk. In addition, risk should be managed for all system components including digital and non-digital assets (SSC3).
3. Cost Benefit Analysis: Evaluate the cost of potential controls against their threat level to support management in decision-making. The outputs of this should include costs of implementing or not implementing controls, bearing in mind that the cost may also propagate up or down a supply chain through interdependent processes (ISC4, SSC4) and impact human safety (SSC2).
4. On-going monitoring and Response: Management should decide the most effective controls to reduce the risk based on the analysis of the cost benefits. The selected controls must include technical, operational, and management controls to offer appropriate security for the organisation. This must be addressed regularly given the dynamic nature of IoT systems and management should ensure *continual reviews and updates to the risk assessment* take place (e.g. standing item at board level) (ISC1).
5. Assign Responsibility: Develop a list of responsible persons to enact and fulfil the duties of mitigating threats. In this case, it is essential for the organisations to consider all features of risk management related to safety and information security (SSC1) such as risk tolerances and risk framing. Furthermore, make sure the responsible persons are able to identify risk and are familiar with the potential physical impact that could effect (SSC2) and the potential for blurred boundaries between systems (ISC 2, ISC3).
6. Develop a security policy: this includes an action plan containing details on vulnerabilities and threats (including threats level), recommended controls and actions, responsible individuals or teams for supporting and implementing the controls, maintenance requirements –in this case ensuring regular review based on the dynamic IoT environment (ISR 1) and the fact new devices may

[1] https://www.ncsc.gov.uk/guidance/risk-management-collection

lead to exposure to interconnected systems (SSC4, ISC2, ISC4)

7. The policy should be implemented with residual risk made clear and regularly reviewed as new devices could be added (ISR1) or boundaries changed (ISR2).

4.4 Conclusion and Future Work

In this paper we presented special considerations for SCADA and IoT risk assessment based on existing literature, with a particular focus on risks emerging in converged SCADA/IoT environments. ICS/SCADA and IoT risk assessment methods were discussed and analysed. A hybrid approach was proposed, mixed with the inclusion of the considerations alongside standard risk assessment and management procedures. The aim is to support the risk assessment process in this context – on the SCADA side, by considering safety and security in SCADA systems, potential physical impacts of an ICS attack, consideration of non-digital assets, and propagation of impact between systems – including other Internet-connected systems. On the IoT side – the fact that periodic risk assessment may not be sufficient and the process may need to be continual; considerations of changing perimeter boundaries and that new interconnections may occur between systems when adding IoT devices, heterogeneity within systems, and as with SCADA - propagation of the impact to interdependent systems.

5 References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial Internet of Things," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, pp. 1–10.

[3] W. Xi and L. Ling, "Research on IoT Privacy Security Risks," in *2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII)*, 2016

[4] R. Hunzinger, "SCADA FUNDAMENTALS AND APPLICATIONS IN THE IoT," in *Internet of Things and Data Analytics Handbook, chapter 17*, Hwaiyu Geng, Ed. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2016

[5] NIST SP800-30, "Guide for Conducting Risk Assessments" Published 2012. [Accessed: 03-Feb-2019]. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[6] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Trans. Ind. Informatics*, vol. 9, no. 1, pp. 277–293, Feb. 2013.

[7] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "A risk assessment methodology for the Internet of Things," *Comput. Commun.*, vol. 129, pp. 67–79, Sep. 2018.

[8] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[9] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Prof.*, vol. 19, no. 5, pp. 20–26, 2017.

[10] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," 2015.

[11] NIST, "IoT Security and Privacy Risk Considerations," 2018.

[12] B. (An E.-T.-E. I. B. Solution), "IoT Technology Solution for Original Equipment Manufacturers." [Online]. Available: https://www.biz4intellia.com/oem/. [Accessed: 03-Feb-2019].

[13] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, 2011, pp. 1–5.

[14] G. Sorebo, "Managing the Unmanageable: A Risk Model for the Internet of Things Chief Cybersecurity Technologist Leidos @gibsorebo."

[15] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, 2017.

[16] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Trans. Syst. Man, Cybern. - Part A Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[17] P. S. Woo and B. H. Kim, "A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems," *Adv. Mater. Res.*, vol. 960–961, pp. 1602–1611, Jun. 2014.

[18] C. G. Chittester and Y. Y. Haimes, "Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures," *J. Homel. Secur. Emerg. Manag.*, vol. 1, no. 4, Jan. 2004.

[19] Y. Y. Haimes, "Hierarchical Holographic Modeling," *IEEE Trans. Syst. Man. Cybern.*, vol. 11, no. 9, pp. 606–617, 1981.

[20] J. Guan, J. H. Graham, and J. L. Hieb, "A digraph model for risk identification and mangement in SCADA systems," in *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*, 2011, pp. 150–155.

[21] M. H. Henry and Y. Y. Haimes, "A Comprehensive Network Security Risk Model for Process Control Networks," *Risk Anal.*, vol. 29, no. 2, pp. 223–248, Feb. 2009.

[22] A. Rizzardi, D. Miorandi, S. Sicari, C. Cappiello, and A. Coen-Porisini, "Networked Smart Objects: Moving Data Processing Closer to the Source," Springer, Cham, 2016, pp. 28–35.

[23] W. Tianshui and Z. Gang, "A Novel Risk Assessment Model for Privacy Security in Internet of Things," vol. 19, no. 5, 2014.

[24] M. Teimourikia and M. Fugini, "Ontology development for run-time safety management methodology in Smart Work Environments using ambient knowledge," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 428–441, Mar. 2017.

[25] Mengmeng Ge and Dong Seong Kim, "A Framework for Modeling and Assessing Security of the Internet of Things," in *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, 2015, pp. 776–781..