A Holistic Approach for Cyber Assurance of Critical Infrastructure with the Viable System Model

Theodoros Spyridopoulos, Ioanna-Aikaterini Topa, Theo Tryfonas, Maria Karyda

A holistic approach for Cyber Assurance of Critical Infrastructure with the Viable System Model*

Theodoros Spyridopoulos[1], Ioanna Topa[2], Theo Tryfonas[1], and Maria Karyda[2]

[1] Cryptography Group, University of Bristol, UK
[2] Department of Information and Communication Systems Engineering
University of the Aegean, Greece
th.spyridopoulos@bristol.ac.uk, icsdm12018@icsd.aegean.gr,
theo.tryfonas@bristol.ac.uk, mka@aegean.gr

Abstract. Industrial Control Systems (ICSs) are of the most important components of National Critical Infrastructure. They can provide control capabilities in complex systems of critical importance such as energy production and distribution, transportation, telecoms etc. Protection of such systems is the cornerstone of essential service provision with resilience and in timely manner. Effective risk management methods form the basis for the protection of an Industrial Control System. However, the nature of ICSs render traditional risk management methods insufficient. The proprietary character and the complex interrelationships of the various systems that form an ICS, the potential impacts outside its boundaries, along with emerging trends such as the exposure to the Internet, necessitate revisiting traditional risk management methods, in a way that treat an ICS as a system-of-systems rather than a single, one-off entity. Towards this direction, in this paper we present enhancements to the traditional risk management methods at the phase of risk assessment, by utilising the cybernetic construct of the Viable System Model (VSM) as a means towards a holistic view of the risks against Critical Infrastructure. For the purposes of our research, utilising VSM's recursive nature, we model the Supervisory Control and Data Acquisition (SCADA) system, a most commonly used ICS, as a VSM and identify the various assets, interactions with the internal and external environment, threats and vulnerabilities.

1 Introduction

Industrial Control Systems (ICSs), have been a fundamental part of Industry automation for many years. They are typically used to control industrial processes, such as power production, oil extraction, transportation, telecommunications etc. [1]. Those processes have a direct impact on the National Critical Infrastructure (CI) [2], making their protection against cyber-attacks a process of national significance. Effective Cyber-Security Risk Assessment methods are vital in order to manage security risks against the ICSs.

Assessing and managing cyber-security risks in traditional IT systems has followed certain well established techniques [3–6]. Nevertheless, the complexity and the interconnectivity of Industrial Control Systems (ICSs) hinder the application of traditional cyber-security risk management methods. In many cases though, the methods applied

* This work has been supported by the Univ. of Bristol's Systems Centre.

are adaptations of the conventional methods for managing cyber-security risks within the environment of an organisation [7], therefore addressing only part of the threat landscape and certainly mostly the traditional IT components, as opposed to sensor/actuator or other control elements [8]. For that reason, new methods are being developed. However, the majority of these lack the perspective of resilience [8], while in many cases the identification of the threats and vulnerabilities is conducted in each domain of the ICS separately, omitting the interactions between the various assets or threats. As a consequence they tend to protect the various domains of the system independently, applying overwhelming security measures driven by the worst case scenarios [8]. This way, even though the system is considered secure, cost-efficient risk mitigation strategies can not be identified. Therefore, novel holistic cyber-security risk assessment and management approaches that can overcome the drawbacks of past approaches have to be explored.

Towards this direction, we propose a conceptual framework for the enhancement of the cyber-security risk assessment in ICSs, adopting principles of the Viable System Model (VSM) [9]. We use the VSM to model the cyber-assets and functions within an ICS and identify the way cyber-threats against them affect the *viability* of the system, taking into account the various interactions that take place.

The rest of the paper is structured as follows. In Section 2 we discuss related work in the field of cyber-security risk assessment in Critical Infrastructure. Section 3 presents the basic background on the VSM. The description and analysis of our proposed model are given in Section 4. Finally, Section 5 discusses conclusions drawn from our work.

2 Related Work

Cyber-security risk assessment constitutes a fundamental element for the protection of ICSs. According to [8] , Critical Infrastructure risk assessment methods are divided into two distinct categories, the sectoral methods, which refer to those who treat each sector separately in the risk assessment process, and those that follow a systemic approach examining the CIs as interconnected networks. Most existing methods fall into the first category. In order to cope with ICS, those methods have been extended. Nevertheless, they have limitations when they are applied in cross-sectoral environments. Furthermore, in most methods of both categories resilience concerns are not addressed or exist only implicitly. Our model falls into the second category, utilising the VSM as a vehicle for the identification and description of the cyber assets and cyber-security risks. The inherent scalable nature of VSM ensures resilience while its systemic behaviour allows the investigation of the emerging interconnections.

The authors in [10] examine Critical Infrastructure as Complex Adaptive Systems. They represent ICSs as large sets of components that interact with each other while synergies emerge through those interactions. They introduce the notion of interacting agents where each agent carries data regarding its location, capabilities and memory. However, the modelling and simulation of such models poses significant challenges and thus has not been taken into account for the risk assessment process. Since our model is based on the VSM, a model that has already been tested against the viability management of an ICS, it poses no similar challenges. In [11] the authors present a simulation environment for SCADA security analysis and assessment. However, even

though their work takes into account the interdependencies to an extend and provides resilience, it is purely focused on the network communications between different parts of system, without taking into account several cyber-threats that are not network-driven.

In another approach [12] the authors combine Survivability System Analysis (SSA) with Probabilistic Risk Assessment (PRA) in order to develop a new approach towards risk management in power substations that inherits the strengths of both. The principles of survivability analysis used in their work resemble the viability concept adopted in the VSM that we use in our work. However, this work lacks the ability to thoroughly explore the emerging inter- and intra- disciplinary interactions.

3 Basic Background on the VSM

Our research mostly focuses on the risk assessment process in ICSs. We have combined the traditional risk assessment methodology with principles of the Viable System Model, providing a new way of thinking towards the "cyber-asset identification" and "cyber-threat assessment" steps within a typical cyber-security risk assessment process, as described e.g. in [3]. In this section we provide background information relevant to the Viable System Model and its application to the cyber domain. The Viable System Model was originally designed by Stafford Beer to model the viability of an organisation [13, 14]. Beer studied the human organism and constructed an organisational model for enterprises based on the methods used by the central and autonomic nervous systems to manage the operations of the organs and muscles. The model divides the organisation into three fundamental parts, i.e. Management, Operations and the Environment. The Operations part entails all the operations that take place inside the organisation while the management part controls the smooth operation of the system, ensures its stability, facilitates its adaptation to the future trends and structures the policies of the organisation. The environment entails all external entities that exchange data with the system. A general view of the model is shown in Figure 1. Beer suggests that we should model an organisation in the way the human body works, in a way that is not so strict and solid as the pyramid but flexible to adapt to changes caused by the environment. As seen in Figure 1, the VSM is composed of six different systems, each one of a distinct role.

System 1: Operational units within the organisation.
System 2: Attenuation of oscillations and coordination of activities via information and communication.
System 3: Management of the primary units. Provision of synergies.
System 3*: Investigation and validation of information flowing between Systems 1-3 and 1-2-3 via auditing/ monitoring activities.
System 4: Management of the development of the organisation; dealing with the future and with the overall external environment.
System 5: Balancing present and future as well as internal and external perspectives; ascertaining the identity of the organisation and its role in its environment; embodiment of supreme values, norms and rules of the system

Each operation in System 1 can communicate with the rest of the operations of System 1 and the external environment for exchange data. Their overall function is coordinated

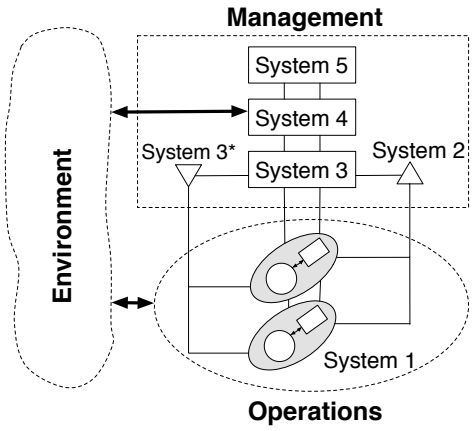

Fig. 1. The Viable System Model.

by System 2 and controlled by System 3 which is also responsible for the provision of synergies. System 3* is responsible to conduct audits upon System 1 to check if System's 3 directions and commands are implemented properly and address the existence of any issues to System 3. System 4 communicates with the external environment so that it can deal with the future trends and identify the various changes that take place in the external environment. It is in contact with System 3 in order to deliver the changes that have to be done and with System 5 which forms the upper level of management that deals with the system's policies and role inside the environment. System 5 is connected with System 3 since it monitors the homoeostasis between System 4 and System 3. Furthermore, System 5 has the responsibility to deliver the ethos of the organisation and take long term decisions that will be passed to System 3 in order to direct System 1 on how to implement them. Also, System 5 has to know the current state of the Organisation, through reports from System 3, in order to take a long term decision. An interesting characteristic of the VSM is its recursive nature. Each operation in System 1 forms a VSM subsystem with its own operational and management parts.

The VSM has already been used in the cyber-security domain, as a framework for examining the impacts of attacking organisations [15]. The authors utilised the VSM in order to identify the weak points within an organisation by modelling cyber-attacks as attacks against the various systems of the model. This way they managed to explore the impact of an attack based on the systems it affected. However, their work bears certain limitations as it only focuses on one VSM model, disregarding its recursive nature. Neither does it provide information regarding the VSM's relationship with the environment as well as other organisations.

In another approach [16] the authors use the VSM to model Information Security Governance establishing a baseline of the current information security operations system. In their work they model the cyber-security mechanisms of an organisation as a VSM, mapping the various protection mechanisms on the VSM depending on the

way they function. However, their research focuses exclusively on the protection mechanisms, omitting information regarding the cyber-assets and impact assessment of a cyber-attack. This is because they follow the implementation of a standard (ISO27001) and thus a checklist-based approach. In our work we use the VSM differently, modelling the cyber-assets of the system as operational or managerial components of a VSM, and examining the impact of a cyber attack upon it.

4 Proposed Model

In this Section we detail our model and its component and also an analysis of the VSM and how we utilise its features for the purposes of the risk assessment in ICSs.

4.1 Model Description

For the purpose of our research, we use VSM to model the assets of the system and the emerging relationships between those assets and the internal and external environment. Considering those relationships as another type of asset, we identify the threats against them and examine the vulnerabilities of the system that can be exploited by the identified threats. Since VSM was originally used to model the viability of a system, identifying the threats against the security of its system-components and their relationships equates to identifying the threats against the viability of the system. Therefore, in order to identify threats against the organisation we can do this by identifying the possible threats against the viability of the system as presented in [15]. In each of the six systems of the VSM we identify the threats that can:

- make the system unavailable to the rest of the systems disrupting its connection to them (Denial of Service attack),
- corrupt the connection of the system to the rest of the systems by sending false data to them (Man in the Middle attack),
- render the system unavailable to its external environment (Denial of Service attack),
- corrupt the connection of the system to its external environment (Man in the Middle attack),
- disclose or corrupt data transferred from/to the system to/from the external environment or another system inside the organisation (data theft, data tampering),
- disclose or corrupt data that reside within the system (data theft, data tampering),
- make its subsystems or suprasystem unavailable,
- corrupt the connection with its subsystems or suprasystem,
- alter or disclose the data transferred to its subsystems or suprasystem.

Afterwards we explore the vulnerabilities that can be exploited by the threats identified in the previous step. The rest of the risk assessment process follows the traditional methodologies. Figure 2 illustrates our proposed risk assessment process. The first step of the process includes the construction of the VSM of the upper level organisation and it is repeated for every subsystem until the lowest level of the organisation where operations are performed by hardware. This way, all the possible assets and interactions are taken into account. At this point it is important to note that in order to identify all

the assets and map them to the VSM as operational or management systems, knowledge from people within the ICS is also required. Managers form the upper management levels of the ICS along with engineers from the operational levels have to be consulted.

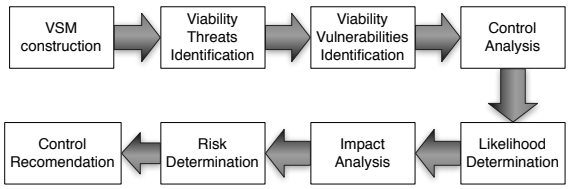

Fig. 2. VSM Risk Assessment Process.

4.2 Model Analysis

In general, the proposed process starts with the construction of the VSM of the upper organisational levels. A general VSM model addressing the most common upper level functions that can be found in an ICS, such as Finance, Sales and Marketing, Production, Legal Services, IT, Human Relations etc., can be seen in Figure 3.

All departments of System 1 are coordinated through regular meetings between the activities directors, an action that forms System 2, and organised by the executive director (System 3). The Quality Control Direction forms System 3*, which is responsible for the monitoring and auditing activities on the various departments. System 4 and System 5 are defined as the Marketing and Forward Planning Direction and the Management Board respectively. At a first glance, VSM at this level has nothing to offer to the cybersecurity risk assessment. However, the lack of a System (for instance System 3*) may result in significant effects to the subsystems of the various departments of System 1, or a less effective Forward Planning Direction may result in missing critical security news. Thus, even at this level certain threats against cyber security of the ICS that derive from poor organisation of the ICS can be identified. In the context of VSM, the viability of the whole system is inextricably linked with the viability of its subsystems, therefore, each unit should function as a VSM in itself. Applying recursively the VSM in every department of the ICS and delving deeper into the lower levels can reveal more threats against cyber security. In Figure 4, after applying VSM recursively we reach the SCADA system-level. At this level all operations consist of hardware components, known as *field devices*. The impact of a successful cyber-attack there is much higher, because it can affect directly the function of the whole ICS. The VSM helps us identify all the interactions between the various field devices and the control/management equipment/department. Furthermore, interconnections with the external environment can also be identified. For example cyber-threats can origin from trusted insiders carrying knowingly or not compromised equipment, e.g. a malware-infected flash drive, or

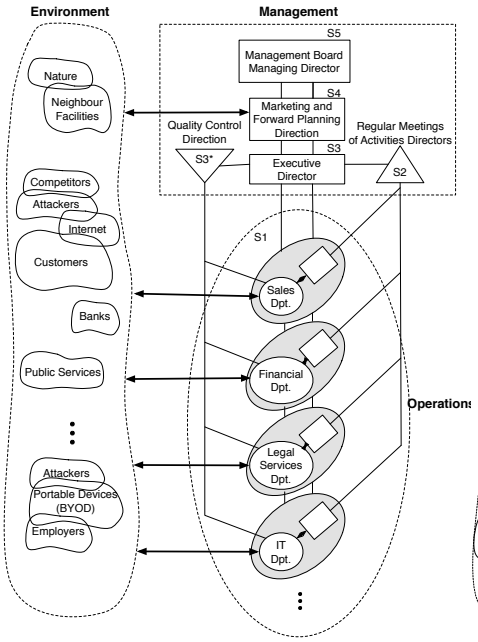

Fig. 3. VSM General Model of the Upper Organisational Level of an ICS.

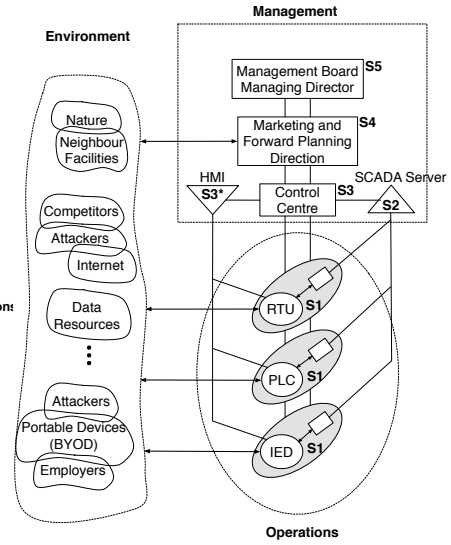

Fig. 4. Applying the VSM on the SCADA system.

a compromised mobile device etc. As part of the environment we can find other ICSs that exchange data or services with the ICS under attack. The investigation of those interconnections provides the ability to examine the impact of a cyber-attack on other ICSs.

5 Conclusion

Risk assessment is an essential part of the protection process of Critical Infrastructure. There is a wide variety of risk assessment tools that are currently being used, however the complexity of these systems poses major challenges to the traditional approaches. Existing methods struggle to manage the dependencies in such environments, and resilience remains in most cases an unsolved issue.

In this paper we have used the Viable System Model in order to identify the relationships between the different parts within and outside the Critical Infrastructure system, scope the area of concern with respect to 'cyber' and construct a whole-system view of the assets, threats and vulnerabilities within that scope. Our work enriches the identification steps of conventional risk assessment methods. The VSM approach yields improved results as a diagnostic tool and so combined with a risk management method it can provide system resilience at multiple hierarchical levels. This approach takes into consideration organisational issues (management, coordination etc.) that play a vital

role in the ability of a system to mitigate cyber-threats and could otherwise be overlooked.

As part of future work we are currently investigating agent-based modelling techniques where each agent embodies certain characteristics based on its position within the VSM. Furthermore, we aspire to develop novel risk management tools based on VSM, rather than using it as part of traditional methods. This requires the development of a quantitative risk evaluation process that will make use of the findings of the VSM to compute risks. Further work will focus on the development of a game theoretic model that tackles this issue.

References

1. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST Special Publication **800**(82) 16–16
2. Commission, E.: Council directive 2008/114/ec of 8 december 2008 on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union (2008)
3. Peltier, T.R.: Information security risk analysis. CRC press (2005)
4. Stoneburner, G., Goguen, A.Y., Feringa, A.: SP 800-30. risk management guide for information technology systems. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States (2002)
5. Alberts, C.J., Dorofee, A.: Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc. (2002)
6. Karabacak, B., Sogukpinar, I.: Isram: information security risk analysis method. Computers & Security **24**(2) (2005) 147–159
7. Stouffer, K., Falco, J., Kent, K.: Guide to supervisory control and data aquisition (scada) and industrial control systems security. Recommendations of the National Institute of Standards and Technology (NIST). Special Publication (2006) 800–82
8. Georgios, G., ROBERTO, F., Muriel, S.: Risk assessment methodologies for critical infrastructure protection. part i: A state of the art. EUR - scientific and technical research reports (2012) JRC.G.6-Security technology assessment.
9. Espejo, R., Harnden, R.: The viable system model: interpretations and applications of Stafford Beer's VSM. Wiley Chichester (1989)
10. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. Control Systems, IEEE **21**(6) (2001) 11–25
11. Chunlei, W., Lan, F., Yiqi, D.: A simulation environment for scada security analysis and assessment. In: Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on. Volume 1., IEEE (2010) 342–347
12. Taylor, C., Krings, A., Alves-Foss, J.: Risk analysis and probabilistic survivability assessment (rapsa): An assessment approach for power substation hardening. In: Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC. Volume 64. (2002)
13. Beer, S.: Brain of the firm: the managerial cybernetics of organization. J. Wiley New York (1981)
14. Beer, S.: The heart of enterprise. John Wiley & Sons Chichester (1994)
15. Hutchinson, B., Warren, M.: Information warfare: using the viable system model as a framework to attack organisations. Australasian Journal of Information Systems **9**(2) (2007)
16. Alqurashi, E., Wills, G., Gilbert, L.: A viable system model for information security governance: Establishing a baseline of the current information security operations system. In: Security and Privacy Protection in Information Processing Systems. Springer (2013) 245–256