Managing Cyber Security Risks in Industrial Control Systems with Game Theory and Viable System Modelling

Theodoros Spyridopoulos **Konstantinos Maraslis** **Theo Tryfonas** **George Oikonomou** **Shancang Li**

Crypto Group, Faculty of Engineering, University of Bristol, Bristol, UK

{th.spyridopoulos; k.maraslis; theo.tryfonas; g.oikonomou; shancang.li} @ bristol.ac.uk

Abstract – Cyber security risk management in Industrial Control Systems has been a challenging problem for both practitioners and the research community. Their proprietary nature along with the complexity of those systems renders traditional approaches rather insufficient and creating the need for the adoption of a holistic point of view. This paper draws upon the principles of the Viable System Model and Game Theory in order to present a novel systemic approach towards cyber security management in this field, taking into account the complex inter-dependencies and providing cost-efficient defence solutions.

Keywords: industrial control systems, risk management, game theory, asset evaluation, viable system model.

1 Introduction

Industrial Control Systems (ICSs) have been playing a major role in Industry for many years. They are used to control fundamental industrial processes such as power production, power distribution, transportation etc. [1]. Due to their national significance such systems can also be considered as Critical Infrastructure (CI), as defined by the 2008/114/EC European Directive on the identification and designation of European critical infrastructures [2]. The protection of those systems is of vital importance.

Traditionally ICSs have been operated as isolated systems, physically separated from the outer world with no connection to the Internet. However, the growing adoption of emerging network technologies in modern ICSs, such as wireless sensors and smart devices, has connected those systems to the Internet exposing them to various cyber threats. In addition, legacy devices used in many ICSs may bear a variety of vulnerabilities that are difficult or even impossible to be patched [3]. This, in conjunction with the critical nature of ICSs, makes them an attractive target for cyber-attacks. In order to mitigate such concerns, risk management techniques are used. These techniques assess the risks of cyber attacks against the system taking into account the characteristics of the system and the impact of a successful attack, and then provide recommendations for defence mechanisms that can minimise the risks. There is a wide variety of cyber security risk management methods used currently in the ICS domain, however most of them are adaptations of methods that have been used for assessing risks in an enterprise, and therefore are tailored to the particular threat landscape and the characteristics of a commercial enterprise, rather than a CI [1], [4]. Furthermore, most of the approaches tend to neglect the emerging dependencies between the components of an ICS and those between parts of different ICSs. Thus, the impact of a cyber-attack is not fully understood [4].

In this paper we introduce a novel approach towards the cyber security risk management in ICSs, utilising principles from the Viable System Model (VSM) and Game Theory (GT), two widely known methods for organizational management and strategic decision-making respectively. First, we use the VSM in order to evaluate the cyber components of an ICS. The 'value' of each component is proportional to the original price of the device and the type and number of its interconnections, as they are defined by the VSM following a system of systems approach. The results of the evaluation are then used in a game between the attacker and the defender, the strategies and payoffs of which reflect the risk assessment process, while the solution of the game provides cost-efficient protection solutions for the defender. In this way we present a cost-benefit risk management process for ICSs that requires minimum informational input.

The rest of the paper is structured as follows: In Section 2 we present the related work regarding cyber security risk management in industrial control systems. Section 3 describes the basic background of the VSM and GT and Section 4 presents the results of our game model. Section 5 presents the conclusions of our work.

2 Related Work

Managing cyber security risks in conventional IT infrastructures usually follows certain established approaches [5], [6]. In general, following the ISO/IEC 27005 standard on Information Security Risk Management, the methodology adopted by those approaches comprises four discrete phases and each phase consists of straightforward steps[7]:

Phase 1: Information Security Risk Identification

- Assets identification.
- Identification of cyber threats.
- Identification of existing security controls.
- Identification of vulnerabilities.

- Identification of consequences in case a vulnerability is exploited by an identified threat.

Phase 2: Information Security Risk Analysis

- Impact assessment.
- Assessment of cyber security incident likelihood.
- Level of risk determination.

Phase 3: Information Security Risk Evaluation

Risks are evaluated as the product of the impact of a cyber security incident and the likelihood of that incident.

Phase 4: Information Security Risk Treatment

The last step encompasses the proposal of risk mitigation mechanisms that will retain risks in acceptable levels or even avoid them.

Traditional approaches towards cyber security risk management in ICSs follow this methodology most of the times, adapting it to the needs of an ICS. However, as described by the authors in [1] and [4], the fact that this methodology originally focuses on IT infrastructures makes such approaches inapplicable in the complex environment of ICSs. Towards this direction many researchers have proposed methods that follow a holistic point of view in the ICS cyber security risk management process. More particularly, in [8] the authors adopt a mixed holistic-reductionist approach for the impact assessment of cyber attacks. The proposed conceptual methodology models heterogeneous systems and evaluates the impact of an attack through the definition of different agents and their dependencies. However, although it can identify emerging interconnections, its complexity due to the lack of a unified approach towards the definition of interconnections renders it un-manageable when more details are added. The complexity also rises from the fact that it models each attack separately.

Another approach is presented in [9] where the authors use the VSM in order to examine strategic cyber security attacks that an adversary could use in order to strike the viability of an organisation. By modelling traditional cyber attacks as attacks against the various systems that compose the VSM of the organisation, they managed to unveil the effect of a cyber attack on the system as a whole.

Authors of [10] build on the knowledge from models [11] and [12] about software assistants IRIS and ARMOR respectively, in order to come up with GUARDS, a novel game theoretic approach that is used by Transportation Security Administration (TSA) for security-related resource-limited allocation tasks regarding the protection of 400 airports of the United States. Unlike the previous two models, it can handle heterogeneous security activities and multiple diverse threats, with an almost decentralized method (meaning that headquarters do not plan a common strategy for all airports) that can take into account multiple security layers simultaneously while attempting to protect a set of targets. This project solves the game by finding its mixed Nash Equilibria. Although it is a robust model, it considers the airports almost autonomous to each other and not as systems within a larger system (TSA) making the adoption of a centralized solution that could respect the specificities of the airports, impossible.

Similarly, in [13], another airport (Los Angeles International Airport – LAX) is under investigation and ARMOR is adopted to convert the problem of optimally using their security resources (i.e. checkpoints on the roadways entering the airport and canine patrol routes) into a solvable one where mixed Nash Equilibria can be found. Although, the resources are composed of two factors, ARMOR can only focus on one of them per application.

A game theoretical approach applied to a Critical Infrastructure is demonstrated in [14]. The authors examine a scenario where, in a smart grid with state estimators that are supposed to accurately measure the price of electricity at any given time, an attacker tries to inject faulty data while a defender tries to withstand the attacks. Those behaviours are modelled as two-player, zero-sum games, the Nash Equilibria of which need to be found. The results are then validated with simulations. However, this method lacks the element of Risk Evaluation where the possibilities of a successful attack would depend on additional parameters that would make the model more realistic.

Game theoretic approaches are not new to Risk Analysis [15], however they are far from being used as state of art, despite various authors demonstrating how they can offer a deep insight into the problem, as they can be "mutually reinforcing" approaches [16].

3 Basic background on VSM and GT

The **Viable System Model** was firstly introduced by Stafford Beer in 1972 [17]. VSM models the organisational structure of viable and autonomous systems. The model initially divides the enterprise in three fundamental parts (Operations, Management and Environment), which are connected to each other in order to maintain the viability of the whole system.

As presented in Figure 1, an enterprise, composed of the operational and management parts, entails five different systems that communicate with each other and the environment. The presence of those systems along with the interrelationships between them and their communication with the corresponding environment, preserve the viability of the enterprise.

System 1 refers to the operational units within the enterprise. Each unit can communicate with other operational units and the external environment, transferring and receiving data. The overall coordination of System 1's operations is managed through System 2. The control of System 1 is carried out by System 3, while System 3* is responsible for auditing the operations in System 1. Each operational unit within System 1 has its own management system, exchanging data with it and forming a new VSM inside the initial VSM.

System 2 is responsible for the coordination of the activities of the operational units that form System 1. It also communicates with System 3 in order to transfer the results of its coordination actions.

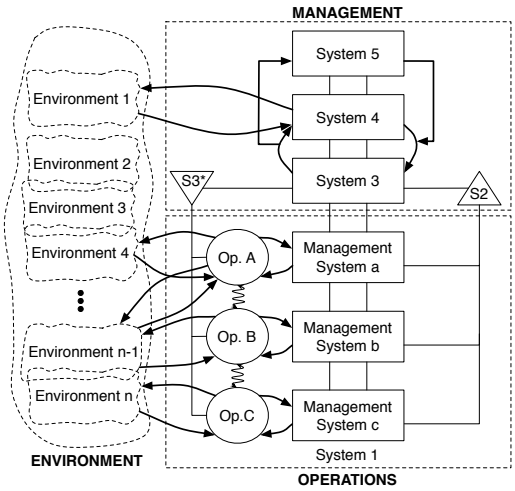

Figure 1 The Viable System Model

System 3 manages the units of System 1, controlling their behaviour by having access to all of them. It is also responsible for the provision of synergies among the operational units. It receives the coordination-related data from System 2 and the results of the audit conducted by System 3* in order to take new decisions regarding the management of System 1. It also communicates with System 4, which dictates the changes that should be made due to the ever-changing external environment.

System 3* audits the operational units of System 1 in order to identify whether System 3's management commands are followed by the operational units and whether changes should be made for the System 1's performance improvement.

System 4 communicates with the environment in order to identify changes in it and propose certain approaches to System 5 for the whole system's evolution. It also communicates System 5's decisions to System 3.

System 5 is the upper level of the management part of the VSM. It deals with the policies of the enterprise and its role within the environment. It communicates with System 4 in order to receive information regarding the changes in the environment. After deciding the changes that have to take place in the operational part of the enterprise, it delivers them to System 4. System 5 also monitors the homeostasis between System 4 and System 3 and receives information from System 3 regarding the current status of the system. Ultimately, System 5 is the one responsible for the long-term decisions.

In our proposed model we make use of the systemic approach that the VSM embodies in order to construct a formal method for the evaluation of cyber components in the complex environment of ICSs. Identifying the purpose of each cyber component and the dependencies that are created, according to the VSM structure, we unveil the real dimensions of the consequences of its disruption or destruction. In addition, its recursive nature that dictates a VSM to be composed of other VSMs and be part of a wider VSM in a system of systems way gives us the ability to explore interdependencies between various ICSs.

Game Theory is a mathematical tool that is used in situations (games) where participants (players) have conflicting interests. Every player can adopt a method of action (strategy) and for every possible combination of adopted strategies there is a reward/utility that occurs for each of them. Game theoretic implementations can "solve" a game by detecting the most effective strategy that each player should adopt in order to maximize their personal reward/utility (assumption of rationality of players). Although there are many kinds of games and many different concepts for defining a "solution" for a game, in this work we only construct two-player games where every player loses exactly as much as the other wins (zero-sum game). By solving the game we mean finding, before the game starts (static game), a strategy for each player such that none of them would be tempted to unilaterally deviate by because that would lead to a worse individual reward (the concept of Nash Equilibrium) [18], [19]. For the purposes of our research we have constructed a game where the defender aims at protecting a cyber component using cost-efficient strategies while the attacker tries to find the attack scenario that causes maximum possible damage.

Our work introduced in the next section uses Game Theory and VSM to provide the means of performing Risk Analysis on Critical Infrastructures.

4 Our proposed model - Analysis

For the purposes of our research we utilised the VSM to capture the relationships between the cyber components of an ICS and also those between the components of different ICSs. In that way, after the identification of the cyber components within the ICS, we assess the value of each component, taking into account the cascading effect of its failure to the rest of the components, within both the same and different ICSs. Assessing the value of each component through its interconnections helps us identify the impact of having it disrupted or destroyed.

In order to model the interconnections we adopt an agent-based approach. Each cyber component is modelled as an agent characterised by its market price, its input and output connections with other cyber component agents and with the environment, the type of its function in correspondence with the VSM structure (System 1, System 2 etc.) and the VSM level that it belongs according to its recursive feature. Figure 2 depicts how a cyber component within an ICS is modelled.

In order to compute each component's value we have to answer the following questions:

- What is the initial market price of the component?
- To which VSM Level does it belong?
- To which other ICSs is it indirectly connected?
- What is its role (System x) within the VSM (operational unit, coordination unit, auditing unit etc.)?

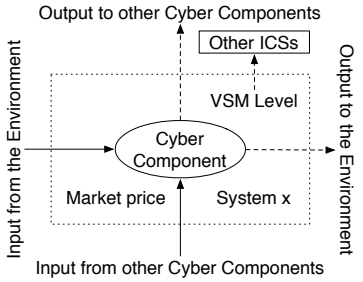

Figure 2 An ICS Cyber Component

- From how many environmental entities does it take input?
- To how many entities in its environment does it provide output?
- From how many other cyber components does it take input?
- To how many other cyber components does it provide output?

Answering those questions for every cyber component provides us with a way to determine their importance to the whole system. The number of total connections and the importance of the component's role form a factor, which multiplied by the initial market price of the component returns the ultimate value of the component. The VSM level refers to the recursion level that the cyber component belongs to and provides information on its purpose within the ICS and the way it affects other ICSs. For example, a Programmable Logic Controller (PLC), which is a control device used in many ICSs, is an operational unit (System 1) within a VSM of level *n*. Along with other field devices it may compose the production department of a power production station. The production department itself is the operational unit within a VSM of level *n*-1. Along with the other departments it may construct the organisational structure of the power production company. Considering this structure as a VSM of level 1, we now have *n*-1=1. Therefore, the PLC belongs to a VSM of level *n*=2. A power plant in its turn affects other ICSs since it provides the electricity they need to function. Therefore, the PLC has a level 2 effect on other ICSs. The magnitude of this effect is proportional to the role of the PLC (System 1) and the number of other devices with the same role in the same VSM level. The quantification of the role of each cyber component depends on the enterprise's perception of each role's importance. A quite simplistic yet acceptable, at this point of our work, way to compute the real value of a cyber component is by multiplying its various characteristics:

Value *= (Market price) x (Number of connections) x (Effect on other ICSs) x (Role of the cyber component)*

where,

Effect on other ICSs *= (Role of the cyber component) / (Number of devices with the same role and VSM level)*

To demonstrate how we embed GT in our model, we present a game scenario where an attacker (e.g. a hacker) plans an attack against a critical infrastructure while a defender is responsible for the best possible protection under limited resources. The attacker and the defender can be considered as players, the whole scenario as a game and all their possible actions as strategies.

Due to the structure of the model, in order for a game theoretical tool to be used, those strategies have to be identified, their impact has to be assessed and finally their probabilistic interdependencies to be evaluated. These steps are no other than Threat/Vulnerability Identification, Threat/Vulnerability Assessment and Risk Evaluation, respectively; steps that constitute the Risk Assessment of our scenario. As the outcome will be the proposal of specific strategies for the players, it is an integrated Risk Management use case.

The parameters that define attacker's strategies are the adoption or not of espionage, the core security attribute that the attack aims at (Confidentiality, Integrity or Availability), the inveteracy of the vulnerability that the attack targets at (less than one year which describes a zero-day threat or more than one year), the level of difficulty of the attack's detection (very difficult in case of multiple zero-day threats, difficult in case of a single zero-day threat or easy in case of attacks with older than one year threats) and the level of difficulty of the attack's recovery (very difficult if it requires a hardware replacement, difficult if it requires a system patch or easy otherwise). Similarly, the parameters that define defender's strategies are the employment or not of a Research and Development (R&D) department for security problems, the frequency that the patches are applied with (yearly, more than a year or never) and the existence or not of an Intrusion Detection System (IDS). Let's assume a scenario where the cyber asset under attack is a PLC device. We assume that the market price of the PLC along with its installation is 15000, the number of connections within the ICS is three, a sensor that feeds it with data, a mechanical device, such as a valve, that is controlled by the PLC, and the SCADA server that connects the PLC with the Control Centre. Its role is to control (System 3) the valve in the VSM level 3, and operate as a unit (System 1) in VSM level 2. Due to its dual purpose the value of the asset is increased by two. For space limitation reasons we will exclude the effect of interdependencies with other ICS. Thus, the ultimate value of the PLC is: $Value = 15000 \times 3 \times 2 = 90000$. The rest values attached to the parameters, presented in Table 1, represent our perception of the specific problem and can be easily adapted to the needs of any ICS.

Apart from the strategies, there are also the rewards of each player that need to be defined for any possible combination of strategies. Below are the formulas employed for attacker's rewards. We assume that the reward of a player is the loss of the other (zero-sum game), therefore the identification of one player's rewards is sufficient.

Table 1 Parameters That Define the Game's Strategies

Attacker's Strategies		
Espionage		30,000
Security Attribute	Confidentiality	0.33
	Integrity	1
	Availability	1
Inveteracy of Vulnerability	<1Year	1,000
	>1Year	10
Difficulty of Detection	Very difficult	4
	Difficult	1
	Easy	0.5
Difficulty of Recovery (Cost of Healing)	Very Difficult	101,000
	Difficult	1,000
	Easy	10
Defender's Strategies		
R&D		10,000
Patch Frequency	Never	0
	1 Year	1,000
	>1 Year	100
IDS		10
Value of Asset Under Attack		90,000

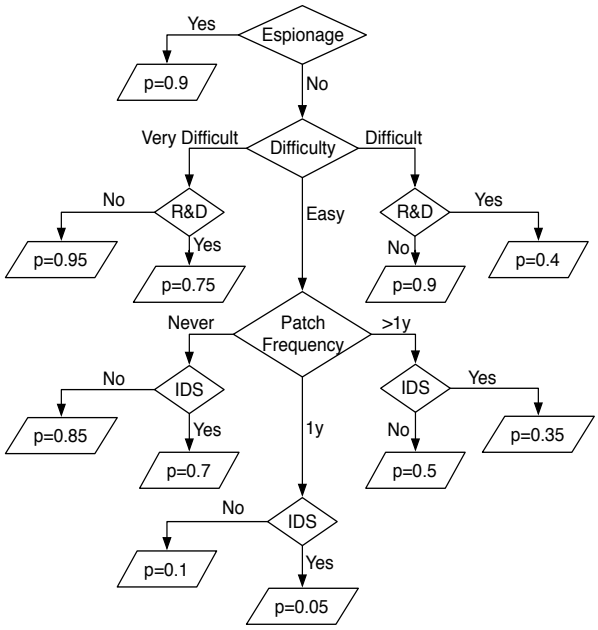

Figure 3 Flowchart of Probabilities of Successful Attack

Attacker's Reward = *Gain + Cost of Defence + Cost of Healing – Cost of Attack*

Where,

Gain = *Value of Asset × Security Attribute × Probability of Successful Attack*

for Probability of Successful Attack given by Figure 3.

Cost of Defence = *R&D + Patch Frequency + IDS*

Cost of Healing = *Difficulty of Recovery*

Cost of Attack = *Espionage + Inveteracy of Vulnerability × Difficulty of Detection*

Taking also into consideration the following rules

- Attack against C cannot be very difficult to recover
- Zero day attack cannot be easy to detect
- >1Years attacks can only be easy to detect

and adding also the case of not attacking within the strategies of the attacker's strategies[1], we end up with a 49×10 table of rewards. The game is solved by identifying its Nash Equilibria, which is a commonly adopted concept of a game's solution.

5 Results

This game was found to have two Nash Equilibria that are presented in the format:

A: (Attack, Espionage, Core Attribute, Inveteracy of Vulnerability, Difficulty of Detection, Difficulty of Recovery)
D: (R&D, Patch Frequency, IDS)

The Nash Equilibria are:

A: (Yes, No, Integrity, 1 Year, Very Difficult, Very Difficult)

D: (Yes, > 1 Year, No)

and

A: (Yes, No, Availability, 1 Year, Very Difficult, Very Difficult),

D: (Yes, > 1 Year, No)

Both lead to a payoff of 174,600 for the attacker, which is equivalent to 174,600 loss for the defender under our assumptions.

6 Conclusion and further work

This paper presents a novel approach towards cyber security risk management in ICSs. Combining the VSM with GT we created a method that provides cost-efficient defence strategies that take into account the proprietary and interconnected nature of an ICS. The proposed method requires the modelling of the ICS's cyber components as agents that represent systems in the VSM structure. In this way we quantify the criticality of an asset through its interconnections to other components. Then we construct a game between the attacker and the defender in order to compute the most cost-efficient strategies of both, when they compete upon each cyber component. Our model is generic and can be applied to any ICS, regardless of its

[1] the case of not defending is already included in the defender's strategies and it is equivalent to adopting no defence mechanisms out of the proposed ones

nature and function. Nevertheless, it can be further enhanced covering a wider range of defence and attack strategies, while validation against real data is also required.

7 Acknowledgments

This work was supported by the Systems Centre and the EPSRC funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1) and Frazer-Nash Consultancy.

References

[1] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," *NIST Special Publication,* pp. 800-82, 2011.

[2] E. U. Commission, "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," *Off. J. Eur. Union FEBBRARO Angela SACCO Nicola,* 2008.

[3] T. Spyridopoulos, T. Tryfonas, and J. May, "Incident analysis and digital forensics in SCADA and industrial control systems," in *System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International*, 2013, pp. 1-6.

[4] G. Georgios, F. Roberto, and S. Muriel, "Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art," *EUR - Scientific and Technical Research Reports,* 2012.

[5] T. R. Peltier, *Information Security Risk Analysis, Second Edition*: Taylor & Francis, 2005.

[6] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Computers & Security,* vol. 24, pp. 147-159, 2005.

[7] E. ISO, "IEC 27005: 2011 (EN) Information technology -- Security techniques -- Information security risk management Switzerland," *ISO/IEC,* 2011.

[8] G. Digioia, C. Foglietta, S. Panzieri, and A. Falleni, "Mixed holistic reductionistic approach for impact assessment of cyber attacks," in *Intelligence and Security Informatics Conference (EISIC), 2012 European*, 2012, pp. 123-130.

[9] B. Hutchinson and M. Warren, "Information Warfare: using the viable system model as a framework to attack organisations," *Australasian Journal of Information Systems,* vol. 9, 2007.

[10] J. Pita, M. Tambe, C. Kiekintveld, S. Cullen, and E. Steigerwald, "GUARDS: game theoretic security allocation on a national scale," in *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, 2011, pp. 37-44.

[11] J. Tsai, C. Kiekintveld, F. Ordonez, M. Tambe, and S. Rathi, "IRIS-a tool for strategic security allocation in transportation networks," 2009.

[12] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, "Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport," in *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, 2008, pp. 125-132.

[13] J. Pita, M. Jain, F. Ordónez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, "Using game theory for Los Angeles airport security," *AI Magazine,* vol. 30, p. 43, 2009.

[14] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," 2013.

[15] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica: Journal of the Econometric Society,* pp. 263-291, 1979.

[16] L. A. T. Cox Jr, "Game theory and risk analysis," *Risk Analysis,* vol. 29, pp. 1062-1068, 2009.

[17] S. Beer, *Brain of the firm: the managerial cybernetics of organization*: J. Wiley New York, 1981.

[18] T. Spyridopoulos, G. Oikonomou, T. Tryfonas, and M. Ge, "Game Theoretic Approach for Cost-Benefit Analysis of Malware Proliferation Prevention," in *Security and Privacy Protection in Information Processing Systems*. vol. 405, L. Janczewski, H. Wolfe, and S. Shenoi, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 28-41.

[19] M. Tambe and B. An, "Game Theory for Security: A Real-World Challenge Problem for Multiagent Systems and Beyond," *Association for the Advancement of Artificial Intelligence,* 2011.