View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Lancaster E-Prints

The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems

Alberto Zanutto, Ben Shreeve, Karolina Follis, Jerry Busby, Awais Rashid

Security Lancaster Institute
Lancaster University
United Kingdom
{a.zanutto, b.shreeve, k.follis, j.s.busby, a.rashid}@lancaster.ac.uk

ABSTRACT

Modern production processes are heavily reliant on industrial control systems (ICS) to help automate large-scale facilities. The security of these systems is paramount as evidenced by high profile attacks such as those against Iran's nuclear facilities and the Ukrainian Power Grid. Existing research has largely focused on technical measures against such attacks and little attention has been given to the security challenges and complexities arising from non-technical factors. For instance, cyber security workers need to maintain security whilst satisfying the demands of varied stakeholders such as managers, control engineers, enterprise IT personnel and field site operators. Existing ICS models, such as the Purdue model, tend to abstract away such complexities. In this paper, we report on initial findings from interviews with 25 industry operatives in the UK and Italy. Our analysis shows that the varying demands of various stakeholders in an ICS represent many complexities that we term *grey area*. Security workers often play the role of *shadow warriors* tackling the competing and complex demands in these grey areas while protecting themselves, their integrity and credibility.

1. INTRODUCTION

The geographic distribution of organisations is continuing to increase as improvements to both global infrastructure and IT systems enable new ways of working. Organisations are complex and traditionally follow a hierarchical model, from the shop floor through to CEO [1]. For many years, the industrial control systems (ICS) sector has doggedly followed this vision of organisational structure by adapting the Purdue model [2] as a basis for ICS security architectures (cf. Fig. 1). However, such models hide essential complexity arising from the interactions across the various layers that are a consequence of increasing inter-connectivity between the enterprise zone and the manufacturing zone. Such inter-connectivity has been exploited in a range of high profile attacks such as Stuxnet [17], German Steel Mill [18] and the Ukrainian Power Grid [19] where attackers pivoted from enterprise IT systems to critical control systems.

Existing security research has studied potential attack vectors [22] as a means to detect intrusions into ICS, e.g., [23, 24, 25]. Whilst research has focused on the role of human factors in ICS security, e.g., [3, 26], there is little work on understanding the complexities faced by security workers – arising from the demands of varied stakeholders such as managers, control engineers, enterprise IT personnel and field site operators.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12 -- 14, 2017, Santa Clara, California.

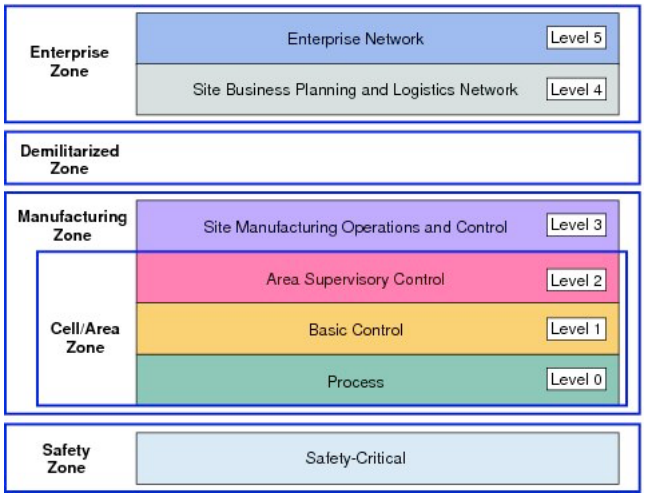

Fig. 1: The Purdue Reference Architecture for ICS [21]

This paper addresses this gap by reporting initial findings from a study of 25 industry workers in the UK and Italy. Our study highlights that ICS security is a *grey area* shaped by the often competing demands of a variety of stakeholders, e.g., managers, control engineers, enterprise IT personnel and field site operators. Security workers are the *shadow warriors* working continuously to address unexpected situations arising from the technologies in use, the supply chain as well as employees in different parts of the organisation. Their tasks are poorly understood by others in the organisation – other workers have to manage "real" things, like documents, or common production machineries and meet to prepare future product launches, address safety issues, and deal with countless other well-defined tasks. Against this backdrop, cyber security emerges as a relatively nebulous and intangible undertaking, not easily grasped by those who are not directly responsible for it. Security workers must, therefore, utilise disciplinary protocols, and rely on power delegated by the management. However, this often leads to lack of cooperation from other parts of the organisation. Security workers, therefore, don the role of shadow warriors tackling the competing and complex demands in these grey areas while protecting themselves, their integrity and credibility.

The novel contributions of this paper are as follows:

- We present insights into the grey areas of ICS security and the complexities faced by security workers.
- We propose the notion of security workers as shadow warriors tackling these complexities and report on their habits, beliefs and strategies.

The rest of this paper is structured as follows: first we summarise the method employed during the fieldwork including a summary of the individuals interviewed (Section 2). This is followed by a presentation of the key findings from our initial analysis (Section 3). We then discuss the implications of these findings (Section 4) before presenting a brief overview of related work (Section 5) and concluding the paper (Section 6).

2. FIELDWORK

We have completed 25 interviews, each lasting approximately one hour, collected over three years of fieldwork. Interviewees were from manufacturing, oil and gas industries both in Italy and the UK. These informants were selected for their role within security in these organisations. Their availability was a result of a snowball sample guided by our theoretical interest in access to people able to describe workplace practices about security in ICS. Therefore, we interviewed Managers, IT Managers, Security Managers, Engineers and Vendors of cyber security systems (see Table 1 for details). Our aim was to gather a range of stakeholder insights into organisational practices.

Table 1: Characteristics of 25 Informants

N	Role	ICS Sector	Organisation
10	Engineers in IT	Development of software for ICS: detecting, penetration test, mitigation, networks,	Various companies
3	Engineer	Maintenance	Utility companies
3	Security manager	Security policy and team in organizations	Utility companies
3	Vendor	Appliances for ICS	Industry
2	Security expert (ex-hacker)	Hidden market malware, post-event analysis, fixing	CEOs of their own companies
1	Technical Engineer	Network reliability, penetration test in industry	CEO of own company
1	Engineer	PLCs testing	Power company
1	Scholar	Risk & safety analysis	University
1	Scholar	ICS analysis	University

A series of five additional informal talks were conducted prior to these interviews in order to refine the interview questions. All the interviews were recorded, transcribed and coded for the analysis and supplemented with field notes collected during the interview process. The project received approval from our institution's research ethics committee.

Data analysis of interviews and fieldwork notes was carried out following a reflexive, grounded-theory approach focused on connecting concepts, emerging issues, labelling and commenting. We adopted a template analysis to assess the way that different stakeholders described their specific industry cyber security practices [16] following the framework of social construction in qualitative research [12]. Working with the templates we re-analysed the excerpts to understand if saturation of labels was reached. Then concepts were connected following a reduced number of templates that helped us to describe the characteristics of security work practices.

3. FINDINGS

The complexity introduced by the increased connectivity of ICS became apparent during our fieldwork. Every time we tried to "follow" the informant's description of his/her practices, we faced recurrent situations where professional boundaries, protocols and strategies used to manage security at the production level became blurred. This led us to the concept of a grey area – a description used by some informants to describe how organisational duty to provide security protocols and technical advice for all the staff did not sufficiently cover the multiplicity of situations that they actually had to resolve. The security workers often had to work in the shadows (following Morgan [20], we use the metaphor of "warriors") often fighting with incomplete instructions or coming up against barriers posed by organisational boundaries or role descriptions. In the following findings, we provide some examples of these grey areas and highlight their impact on ICS security. This is followed by a discussion of the shadow warriors' habits, beliefs and strategies regarding security.

3.1.1 Grey area and top-down approach

Informants described the complexity that occurs when organisations introduce a top-down approach to cyber security. The interviewees highlighted how management often request procedures that are not always applicable for dealing with *everyday exceptions*. Their accounts suggest that during any work day there are many situations and unexpected problems that need to be addressed. Security teams must therefore utilise disciplinary protocols, and rely on power delegated by the management to implement security controls. Nevertheless the accounts we collected show that their work and its implications are not easily understood by others. For example, a protocol may state that every person/item that enters a production plant must be detected and tracked. However, if a truck has to deliver a large number of parcels and props open a secured door then someone can enter undetected and untracked, hence potentially having physical access to information accessible via IT or SCADA workstations and HMIs (human-machine interfaces) for PLCs. In another example, if alarms are starting to sound excessively because of a routine maintenance program then staff may switch off the sound until the end of the day, without regard for the fact that such alarms may be the result of cyber security breaches. Alternatively, a valve may be replaced many times within a short period without anyone considering if the problem is the result of a cyber attack. Of course, if security staff remind personnel about how strictly they must observe these and other protocols then they are likely to receive a multitude of complaints from their colleagues about their integrity. So, sometimes they have to protect themselves from colleagues' remarks and from the risk of poor interactions that result from strict security policies.

3.1.2 Grey area and production's complexity

Some accounts collected from the informants reflected an image of the security team as a patrol continuously working in the shadow. As warriors, they develop internal codes to address unexpected situations. They fight everyday with the technologies, within the supply chain, as well as with employees in the different

sectors, but mainly in the production lines. Moreover, they are also continuously in negotiation with the management. Their tasks are poorly understood by others in the organisation. For example, if an operator is dealing with a SCADA system connected to a PLC and to a physical element of the process, and the physical element has unusual damage, it may take a long time to understand that it could be affected by a remote attack. But if the shadow warriors start to require strict access permissions and login check to every PLC, the operators become upset – as this requires them to change their practices and habits. Other problems come from legacy systems that are poorly protected and everything, from the cyber security point of view, must be handled with great care, as often they neither have the computational capacity nor the hardware/software necessary to implement relevant security controls.

3.1.3 Grey area and organisational knowledge

The work of the security teams is often restricted due to lack of visibility of information from various parts of the organisation. Despite the fact that work in ICS organisations mostly involves managing "real" things, like documents, production machineries, buying and selling things, the shadow warriors often have to work between teams and technical areas. As such they have to prepare a secure environment through a complexity that is hidden and blurred as seen from outside. The overlaps between security and other parts of the organisation are often poorly understood. An informant (an engineer) involved in maintenance in a power company reflected on the work of the security team as follows:

"They [security staff] tend to be a separate team, so they tend to do their own work, and I do my work. Yes, [I work in] physical security. I mean, there is an overlap, to our telemetry systems and that's a bit of a grey area – no direction as to who looks after certain [equipment], so, sometimes you don't know whether you should be touching it or not."

The situation is particularly acute at some peripheral sites where often technicians have a weak vision regarding security. In fact, if something unusual occurs within a production plant, it is simply considered 'strange' but often no further action is undertaken. Managing and implementing security in such situations requires contextual knowledge, responsibility and entitlement. More often than not, this requires an organisational effort and a communication commitment on part of the organisation. However, these efforts are not always strongly supported by the organisation and many aspects remain undefined.

3.1.4 Staff avoid mandatory behaviour

When security workers carry out assessments regarding possible attacks, and ask to perform any security testing which requires simple actions such as port scanning or switching off the PLC, the crew working with the [equipment] becomes (in the words of a security consultant) "crazy with fear". They are concerned about the potential safety impact of any security testing and ask the security teams to leave them in peace and in a safe situation. These safety concerns are often not completely unfounded; for instance, a penetration test could bring down significant parts of the system. An engineer noted the following with regards to the gap in security perception between the security team and production engineers:

"Well the system is working… Please don't give us much stress about it! Don't be so paranoid, please. It works!"

The engineers we have interviewed tend not to have faith in "real life" testing. They just want to follow their aims, to show how efficient they are with respect to production targets. Another problem is the lack of good documentation of devices at peripheral sites.

3.1.5 Shadow warriors: just workers among others

Security staff, like any other, have particular competencies, but again like any other, they are "employees" with typical concerns about disciplinary action or monetary rewards, e.g., a bonus related to the number of alerts managed in a year as suggested by one of our informants. Or may be they are under evaluation for a new post in the company. Or, again, they could be tired because of low wages and great stress that they face in the workplace. A security consultant highlighted how security workers can at times be more interested in *solving* the problem rather *analysing* the root causes so as to not be seen as doing a poor job:

"Once I have demonstrated that the temperature is coherent with what is compatible with these valves, then the question of what the cause is, if it isn't the temperature, will arise in the mind of whoever is in front of me."

We have to be aware of the idea that to deal with cyber security, is like to deal with any other job. It increases the complexity to pay attention to the possible link between unusual events, which can occur during production and possible cyber attacks. Therefore, security staff, like any other employee, often try to configure their tasks as a normal activity to reproduce organisational practices and habits.

3.2 The Shadow Warriors at Work

We have identified a number of key traits that the shadow warriors tend to exhibit when dealing with cyber security in ICS. They trust in their habits, try to stick to their beliefs and they follow a range of strategies to manage their work in the grey area.

3.2.1.1 Habits

The shadow warriors' habits are usually particular and help people involved in the security team to trust each other. As any organisational professional group they share practices, spaces, languages and a common labour culture. Warriors, from our findings, are highly motivated and are expected to be able to "protect" people from a wide range of situations. They must specialise in technological interventions, and are keen to adhere to international best practices when developing organisational protocols. They work (often behind the scenes) with vendors and technical consultants to improve security of the various hardware and software components deployed within the ICS. This enables them to achieve their security goals despite rigid organisational boundaries and lack of cooperation from others within the organisation. However, such "hidden work" further extends the grey area – in terms of a lack of visibility of security practices across the organisation. Asking about how communication can circulate between workers in a manufacturing company, an informant described how uncertain and untrained people may be:

"[If] you have this security person, and his job is to understand these things, he might know that Stuxnet happened or that the German Steel Mill got hacked, he might know these things, but it sounds like that information is not disseminated to people on the ground either."

3.2.1.2 Beliefs

As any warriors in history, shadow warriors believe that they are the only barrier, the last line of defence, against the enemy. They work with commitment and attempt to maintain security in the face of blurred boundaries and, at times, lack of resources and systemic documentation and communication across the organisation. An informant described how security can often be a handcrafted, solitary activity:

"We still don't have any internal protocols because, up until three years ago, I used to [do it all] by myself. Therefore, I would create a system, [and undo] it how I pleased. Now it is two people working together […] but there isn't anything written."

As highlighted by other research in organisational studies [13], all organisations deal with uncertain areas. The shadow warriors develop a special expertise to work in this space. They know that it is difficult to defend against all potential attacks but, through the power to configure every gate access, they do their best to secure the systems in their charge.

3.2.1.3 Strategies

Shadow warriors follow a range of strategies to manage their work in the grey area. When dealing with ordinary employees such as engineers, technicians, etc. this often involves power relationships, e.g., declining requests for additional privileges on local workstations, or enforcing particular security policies, e.g., password strengths and change frequencies. For interactions with management, as an informant explained, it is not so much about highlighting potential risk of attacks, but instead stressing the point about the business loss:

"But they [management] are not necessarily knocking on our door looking for solutions, but if we present issues, or issues that get close to their heart and they realise the danger to their operations, we would hope that they would react. You can't submit the bill of how much a technological solution might cost; what you should present is the bill of the total amount if you don't include certain things. In other words, how much would it cost you to implement a system and how much do you save […]? Even if this isn't totally understood, we need to use a bit of psychology so that the negative evaluation of the cost turns upside down."

The above quote shows that shadow warriors build particular coping strategies to manage the complexity of their work and acquire resources to enable them to carry on their task of managing security in the grey area. However, as noted previously, such (hidden) strategies further extend the "greyness" surrounding security in ICS settings.

4. DISCUSSION

The findings herein help to describe how organisational complexity in ICS settings affects cyber security. Our analysis suggests that, there are few investments in organisation-wide communication of security issues and awareness and that, consistent with previous work [15], companies are mostly considering the failure-model analysis and a positivistic approach.

Our findings also highlight that grey areas are crossroads of different professional interests and, within these, the organisations fail to work in a coherent manner. The fieldwork confirms that these places are a perfect environment for the shadow warriors. They follow a culture-based approach to organisational behaviour and work to become central to many internal policies. In doing so they act in contradictive relational fragmented ways [9, 10]. They use their knowledge of security issues and the danger posed by external attackers as differentiation tools to assess their relationships with other parts of the organisation and to maintain their relevance in the organisational labour divisions [7].

5. RELATED WORK

Ani et al. [14] propose three different organisational strategies to tackle cyber threats in ICS: technology-centred, process-centred and people-centred. However, these strategies are interconnected and often their complexities overlap. The original hierarchical vision – with clear division of labour, division of infrastructures and division of defence strategies – does not capture the real complexities [6, 7]. These systems are better represented as a continuum where at one end of the continuum there are mechanisms that tackle the problem through reliance on ICS security technologies and automated monitoring, while on the other are approaches focusing primarily on the human factor [4, 5]. If the former suggest that we pay attention to the evolution of the technology and its ability to measure the risk of intrusion, the latter show that people who interact with complex infrastructures and environments make the difference in protecting business and production, as is the case for the shadow warriors.

Cherdantseva et al. [15] suggest that most cyber security risk assessment methods for ICS are failure-oriented. They underline that a failure-oriented approach is not complete and highlight the need for a "positivist top-down perspective by identifying the elements and dependencies within a SCADA system that are required in order for a system to be operational, safe and secure" [15, p.22]. Unfortunately, such a positivistic top-down approach represents executives and senior management, middle managers, supervisors and workforce teams as differently involved in the process of security. In reality, they are in charge of many processes that can directly or indirectly affect the security of a plant. Despite this, security workers are usually tasked with providing security for all, regardless of the expectations of management, the complexity of technological systems or the non-compliant behaviour of non-technical users. These processes are rife with challenges and tensions, which require expert navigation in undefined territories. One common answer to this problem has been the improvement of design processes and (again) the top-down management of conflicts [25, 26]. Moreover, other researchers suggest that the answer should be mainly in the formation and use of strategic models and active monitoring [23, 24]. This creates a no-man's land, a shadow zone, apparently safe for business from potential attacks. However, we would stress that such territory lies between the complexities of technical expertise and social practices. Security staff often struggle to combine these two sides due to the strong division of labour by role that occurs within organisations [7]. The concept of *shadow warriors* describes the hidden but high stakes nature of the work that security personnel in ICS settings undertake. This label allows us to present some relevant issues, both on the technical side and on the social side, that affect security.

6. CONCLUSION AND FUTURE WORK

We have presented initial insights into the complexities faced by security workers in ICS environments. Our study highlights that these shadow warriors should not be left alone to fight these complexities. In fact, organisations can improve the security and resilience of their ICS if the knowledge from these shadow warriors is properly elicited and put to good use in improving

security practice across the organisation. Such a change will require a redefinition of the mission of security workers and indeed all employees to:

1. Bring cyber security out of the shadows to promote the idea that it is everyone's responsibility. Some operations, however, must necessarily remain in the shadows because of the inherent secretive nature of security work.
2. Organisations should enable their cyber security staff to operate less like warriors engaged in constant battles and instead support them to act more like officers engaged in community policing with the support and understanding of everyone around them.

Our future work (currently in progress) involves a more detailed analysis of the qualitative data collected in this study. This work will look at highlighting specific best practices used by successful shadow warriors and their wider organisations in managing ICS security effectively.

7. ACKNOWLEDGMENTS

This work is supported by UK Engineering and Physical Sciences (EPSRC) research grant, MUMBA: Multi-faceted Metrics for ICS Business Risk Analysis (EP/M002780/1), part of the UK Research Institute on Trustworthy Industrial Control Systems (RITICS).

8. REFERENCES

[1] Galloway, B., Hancke, G.P. (2013). *Introduction to Industrial Control Networks*, in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, 860-880, Second Quarter 2013.

[2] Jones, A.T., McLean, C.R. (1986). *A Proposed Hierarchical Control Model for Automated Manufacturing Systems*. Journal of Manufacturing Systems 5, no. 1, 15–25.

[3] Green, B., Prince, D., Roedig,U., Busby, J., Hutchison, D. (2014). *Socio-Technical Security Analysis of Industrial Control Systems (ICS)*. In Proceedings of the 2Nd International Symposium on ICS & SCADA Cyber Security Research 2014, 10–14. ICS-CSR 2014. UK: BCS, 2014.

[4] Rasmussen, J. (1983). *Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models*. IEEE Transactions on Systems, Man, and Cybernetics SMC-13, no. 3: 257–266.

[5] Piggin, R. (2014). *Industrial Systems: Cyber-security's New Battlefront [Information Technology Operational Technology*]. Engineering Technology 9, no. 8: 70–74.

[6] Dourish, P., Grinter, E., Delgado, J., de la Flor, Joseph, M. (2004). Security in the Wild: User Strategies for Managing Security As an Everyday, Practical Problem. *Personal Ubiquitous Comput.* 8, no. 6: 391–401.

[7] Busby, J. S., Alcock, R. E.. (2008). Risk and Organizational Networks: Making Sense of Failure in the Division of Labour. *Risk Management* 10, no. 4: 235–256.

[8] Luiijf, E. (2015). *Cyber In-security of Industrial Control Systems: A Societal Challenge*. In *Proceedings of the 34th International Conference on Computer Safety, Reliability, and Security - Volume 9337*, 7–15. SAFECOMP 2015. New York, NY, USA: Springer-Verlag New York, Inc., 2015.

[9] Boholm, Å., Corvellec, H. (2011). A relational theory of risk. *Journal of Risk Research*, *14*(2), pp. 175–190.

[10] Bruni, A., S. Gherardi, L. L. Parolin (2007). *Knowing in a System of Fragmented Knowledge. Mind, Culture and Activity* 14, no. 1: 83–102.

[11] Macaulay, T., & Singer, B. L. (2012). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press.

[12] Holstein, J. A., Gubrium, J.F. (2013). *Handbook of Constructionist Research*. Guilford Publications, 2013.

[13] Gherardi, S., Jensen, K., Nerland, M. (2017). Shadow Organizing: a Metaphor to Explore Organizing as Intra-relating. *Qualitative Research in Organizations and Management: An International Journal* 12, no. 1: 2–17.

[14] Ani, U. P., Hongmei M.D. He, Tiwari, A. (2016). Review of Cybersecurity Issues in Industrial Critical Infrastructure: Manufacturing in Perspective. *Journal of Cyber Security Technology* 1, no. 1, 2: 32–74.

[15] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K. (2016). A Review of Cyber Security Risk Assessment Methods for SCADA Systems." *Computers & Security* 56: 1–27.

[16] King, N., Brooks, M.J. (2015). Template Analysis for Business and Management Students. SAGE Publications.

[17] Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy* 9, no. 3: 49–51.

[18] Lee, R. M., Assante, M. J., Conway, T. (2014). German Steel Mill Cyber Attack. *Industrial Control Systems* 30 (2014). http://ics3.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

[19] Liang, G., Weller, S. R., Zhao, J., Luo, F., Dong, Z. Y. (2017). The 2015 Ukraine Blackout: Implications for False Data Injection Attacks." *IEEE Transactions on Power Systems* PP, no. 99: 1–1.

[20] Morgan, G. (1997). *Images of Organization by Gareth Morgan (26-Feb-1997) Paperback*. 2nd Revised edition. SAGE Publications.

[21] Automation, Rockwell. (2011). Converged Plantwide Ethernet (CPwE) Design and Implementation Guide." Accessed May 28, 2017. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.352.6198&rep=rep1&type=pdf.

[22] Chandrasekaran, S., Cooper, O., Deshpande, A., Franklin, M.J., Hellerstein, J.M., Hong, W., Krishnamurthy, S., Madden, S.R., Reiss, Samuel R., Shah, M.A. (2003). TelegraphCQ: Continuous Dataflow Processing. In *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data*, 668–668. ACM. http://dl.acm.org/citation.cfm?id=872857.

[23] Hadžiosmanović, D., Sommer, R., Zambon, E., Hartel, H.P. (2014). Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes. In *Proceedings of the 30th Annual Computer Security Applications Conference*, 126–135. ACM, 2014.

[24] Jardine, W., Frey, S., Green, B., Rashid, A. (2016). "SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection." In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 23–34. ACM, 2016. http://dl.acm.org/citation.cfm?id=2994496.

[25] Urbina, D. I., Giraldo, J.A., Cardenas, A.A., Tippenhauer, N. O., Valente, J., Faisal, M., Ruths, J., Candell, R., Sandberg, H. (2016). Limiting the Impact of Stealthy Attacks on Industrial Control Systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1092–1105. ACM, 2016. http://dl.acm.org/citation.cfm?id=2978388.

[26] Frey, S., Rashid, A., Zanutto, A., Busby, J. S., Follis, K. (2016). On the role of latent design conditions in cyber-physical systems security. In Proceedings of the 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems, SEsCPS@ICSE 2016, Austin, Texas, USA, May 14-22, 2016 (2016), pp. 43–46.