Towards Real-Time Assessment of Industrial Control Systems (ICSs): A Framework for Future Research

William Knowles, Daniel Prince, and David Hutchison
Security Lancaster
School of Computing and Communications
Lancaster University
Lancaster, LA1 4WA, UK
{*w.knowles, d.prince, d.hutchison*}*@lancaster.ac.uk*

Jules Ferdinand Pagna Disso, Kevin Jones
EADS Innovation Works
Quadrant House, Celtic Springs, Coedkernew
Newport, NP10 8FZ, UK
{*JulesFerdinand.Pagna, kevin.jones*}*@eads.com*

This paper outlines a general framework for future research into the real-time cyber security assessments of industrial control systems (ICSs). A proof-of-concept real-time assessment framework is also introduced.

Industrial Control System, ICS, SCADA, Real-Time Risk Assessment, Risk Management

1. INTRODUCTION

According to a report on industrial control system (ICS) security by ICS-CERT (2012), the number of incident reports in 2012 had multiplied to five times their 2010 level. The etiology of this rise is the integration of open and standardised technologies that are traditionally found in IT environments into ICS components, and the interconnection of ICSs to corporate networks and the internet. Although there are similarities in technologies, the approaches to securing them can not be directly translated. For ICSs, availability rather than confidentiality is the primary security goal. This incongruity led to the development of ICS-specific standards, guidelines and best practices (henceforth standards). Despite an increasingly rigorous ICS cyber security ecosystem, three predominant issues remain.

First, standards that address risk management do so in terms of the traditional snapshot in time, and continuous improvement (where it is addressed at all) is typically in terms of cyclic snapshot processes over long timescales (e.g., yearly re-assessments). This approach to risk management has proven to be easily implementable and relatively effective, and is likely to always maintain relevancy in any cyber security program. However, compared to non-ICS systems, there is an absence of mechanisms to address risk in these intermittent periods, especially in real-time. As ICSs seek to ensure availability and safety, perpetual risk awareness becomes highly beneficial.

Second, the majority of these standards lack detail on the practical processes involved in conducting risk assessments. One of the reasons for this limitation is arguably due to the lack of ICS security metrics. Without a foundation of appropriate metrics, risk assessment can not be effectively conducted.

Third, they provide limited information on implementing security controls in order to mitigate risk. Outlined security controls are typically highly generic guidelines of best practice and do not address the complexities of implementing controls in ICS environments (e.g., due to the requirements of real-time monitoring and control). This limitation includes those standards that are industry-specific.

This paper addresses the first and second limitations, and introduces a general framework for research into the real-time risk assessment of ICSs. Section 2 outlines areas of related work. Section 3 introduces the framework and its three elements: system (3.1), expert (3.2), and human (3.3). Section 4 introduces a proof of concept real-time assessment framework, and section 5 concludes the paper.

2. RELATED WORK

Security and safety are distinct concepts, although they are often erroneously used interchangeably. An example of this distinction is illustrated in the

following example. Most safety-focused frameworks work through anomaly detection of returned sensor values from monitored systems. A manufacturing system could potentially be compromised and intellectual property stolen, but this would unlikely be reflected in process outputs. Safety then is not synonymous with security, although the monitoring of process outputs can be a potential indicator that something is wrong with the security of the system. There is a large quantity of literature on real-time safety frameworks, which are almost exclusively centred around power systems. The approaches in these frameworks include decision trees (e.g., Diao et al. 2010), machine learning (e.g., Xu et al. 2011), predictive control theory (e.g., Jin et al. 2010), multiobjective optimization (e.g., Xiao and McCalley 2009), K-means clustering (e.g., Kalyani and Swarup 2011), and pattern discovery (e.g., Xu et al. 2012).

Work that specifically addresses real-time cyber security risk assessment for ICSs is relatively sparse. The largest body of publications has come from the EU project MICIE . MICIE produced a real-time risk assessment framework that combines risk indicators from interdependent ICSs and visualised them in an alert system. An ongoing project, COCKPITCI, is extending MICIEs alert system and intends to develop a software layer that will enable ICS components to autonomously react to identified threats. There is a considerable body of literature addressing static ICS cyber security assessments. Utilised techniques include attack trees (e.g., Byres et al. 2004) and vulnerability trees (e.g., Patel et al. 2008) which could potentially be extended to real-time use in full or in part.

Although not real-time risk assessments, there have been attempts to retro-fit traditional protection technologies such as intrusions detection systems (IDSs) into ICS environments. Examples include Quickdraw IDS signatures (Peterson 2009) and the multitude of academic papers addressing IDS integration (e.g., Verba and Milvich 2008; Morris et al. 2012). Both the approach to this integration and the technologies themselves could play some role in developing real-time risk assessment frameworks.

3. ICS REAL-TIME ASSESSMENT FRAMEWORK

This section outlines a general framework for future research into the real-time assessment of ICSs. This general framework consists of three elements, which represent the entire chain of operation for ICSs: the physical retrieval of system state, an analysis of this state, and the initiation of a behaviour based upon this state. These elements are named system, expert, and human respectively.

The purpose of subdividing the framework into three elements, is to provide broad yet distinct areas that require further research in order to produce a usable real-time assessment system that could survive real-world deployment. Elements are interdependent, and success of the framework is therefore dependent upon a holistic approach to research. This general framework is illustrated in Figure 1. Dotted lines represents research feedback loops, while solid lines represent data flow in implementations. Each element is discussed in further detail in the following subsections.

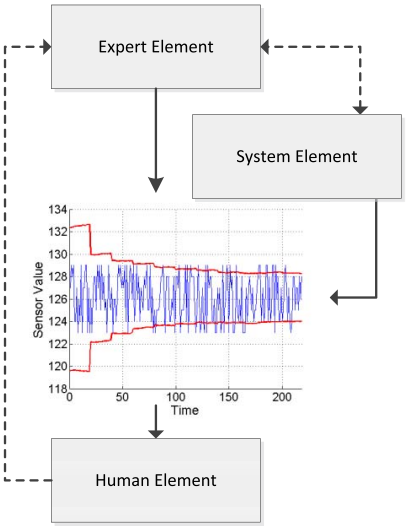

Figure 1: *Interdependent Elements in Real-Time Risk Assessments of ICSs*

3.1. System Element

The system element is concerned with both the physical and logical characteristics of ICS components. Fundamentally, all system element future research within the real-time risk assessment space is concerned with a single issue: data integrity. Integrity is the often forgotten security goal. Information security reveres confidentiality, while ICS security reveres availability; however, integrity plays a central role in a robust risk assessment framework. Future research in ICS security must tackle two issues.

First is the ability to reliably retrieve true values from field devices (e.g., sensor values). This requirement provides an obvious link to the aforementioned dichotomy between safety and security, and therefore constitutes a broader challenge for ICS research. This challenge is not purely academic, and vendors are now frequently striving to integrate integrity assurance into their offerings; however, the focus is predominantly directed towards safety. For example, the evaluation of products against IEC 61508 and IEC 61511 safety integrity levels (SILs).

In broader terms it remains an open research question as to whether these improvements are enough to guarantee reliable functionality for real-time risk assessment. Components are required to not only prevent dangerous failures, but to return reliable and accurate data to security monitoring systems. It is plausible that to obtain the level of integrity required it would require large scale architectural changes, which in practice may not be possible due to the monolithic nature of ICSs (e.g., due to the long amortisation periods for ICS investments).

Second is the ability to return reliable data on the current system state. State in this instance does not refer to monitored processes (e.g., sensor values), but the operating parameters of ICS components (e.g., software configurations). For example, the US Department of Homeland Security's Control Systems Security Program (CSSP) framework (2009) outlines seven dimensions of security and ten technical metrics to evaluate them. To compute many of these metrics, information from the end-system is required. Research is required into whether this can be achieved independently of end-systems, or some form of trusted platform module (TPM) is required to collect and return state data. If a TPM-style component is required, further research is required to identify which ICS components must be monitored to provide a comprehensive overview of risk, and how to appropriately evaluate their heterogeneous risk posture (e.g., as operating system and software differs between HMIs, PLCs, etc).

3.2. Expert Element

The *expert* element is concerned with ensuring the collection of appropriate ICS state data through the system element, and its conversion into a real-time representation of risk. It has two broad issues.

First there is the dearth of ICS security metrics. Metrics are the foundational blocks for determining risk, and although there are many standard publications, the definition of ICS security metrics remains almost universally unaddressed in comprehensive terms. Exceptions exist which typically focus on standards compliance (e.g., ISA/IEC 62443-1-3); however, whether they could be adapted to real-time assessments is unclear. Security metrics must have a low computational overhead in order to a have minimal impact on the real-time nature of ICSs.

Second is the use of defined metrics to compute risk. Section 2 highlighted various approaches for real-time safety analysis, but a limited number for addressing cyber security. However, safety-focused frameworks could potentially be adapted to the cyber security paradigm. Furthermore, there are various static analysis approaches that could be potentially expanded into hybrid or purely real-time frameworks. This issue is also concerned with a number of other factors including how to weight and combine metrics, and the manifestation of risk to be represented (e.g., monetary, uncertainty, compliance).

3.3. Human Element

Risk is not an objective construct, but rather a subjective one that differs widely between individuals. Through representing risk in real-time, the aim is to enable rapid identification and response to potential threats by stakeholders. Potential subjectivity in risk judgements, therefore necessitates consideration of a *human* element.

An overview of the role of subjective risk perception in the risk assessments of computer networks was addressed by Knowles et al. (2012); however, the focus on was static assessments. The demands of real-time environments (e.g., time-pressure and stress) are further variables that must be considered, along with various other dimensions of the human element. For example, research is required to determine the best *manifestation* of risk to represent in real-time. Risk can represent many things, but whether that can provide meaningful information to those charged with monitoring the system in real-time is a separate issue. Furthermore, it is necessary to determine the most appropriate way to *visualise* risk, which has two related issues: First, the act of representing risk accurately and determining what impact this has upon behaviour. For example, individuals have been shown to innately create intervals of estimated (true) values for observed values (e.g., a sensor value). Using the example of confidence intervals based upon system security, if you explicitly make this information available, how does it influence these innate perceptions and the resulting behaviour? Second, this must be achieved across the stakeholders that will use the system (e.g., executives and control engineers will likely perceive risk differently).

4. PROOF OF CONCEPT

A proof-of-concept real-time risk assessment framework has been created called the *uncertainty framework*. It extends the CSSP framework (2009), by addressing some of its limitations (outlined in general terms in section 1), while adding the ability to conduct real-time assessments. The uncertainty framework included a trusted on-system component for end-devices (e.g., PLCs) that collected and returned CSSP metric scores, and a further centralised component that could be integrated as part of the human-machine interface (HMI). CSSP metric scores were

combined using a multi-dimensional Pythagoras theorem to produce a measure of confidence in security, which was then used to create an interval of potentially safe values of monitored sensors. Figure 1 shows an example output of the centralised component. Over time the system under evaluation shows increasing signs of being compromised, and confidence in its security is reduced, leaving some monitored values lying outside of the interval. Assessments were conducted to determine the efficacy of the uncertainty framework when a test-bed ICS is challenged. The results of this assessment will be outlined in a future publication. No human element assessments have yet been conducted.

5. CONCLUSION

This paper introduces a general framework for future research into real-time cyber security assessments of ICSs. This framework identified three interdependent elements (areas) for future research: First, the *system* element which deals with the ability to retrieve the security state of ICS components. Second, the *expert* element which deals with metric definition, computation and evaluation. Third, the *human* element which deals with human behaviours based upon the output of the assessment. Finally, a proof-of-concept real-time risk assessment framework was introduced.

6. ACKNOWLEDGMENT

This research is funded through an Industrial CASE PhD studentship (IW201340) supported by EPSRC and EADS.

REFERENCES

Byres, E. J., M. Franz, and D. Miller (2004). The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. In *International Infrastructure Survivability Workshop (IISW '04)*.

COCKPITCI (2012). Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures.

Diao, R., V. Vittal, and N. Logic (2010, May). Design of a Real-Time Security Assessment Tool for Situational Awareness Enhancement in Modern Power Systems. *IEEE Transactions on Power Systems 25*(2), 957–965.

ICS-CERT (2012). ICS-CERT Year in Review 2012.

Jin, L., R. Kumar, and N. Elia (2010, May). Model Predictive Control-Based Real-Time Power System Protection Schemes. *IEEE Transactions on Power Systems 25*(2), 988–998.

Kalyani, S. and K. Swarup (2011, September). Particle swarm optimization based K-means clustering approach for security assessment in power systems. *Expert Systems with Applications 38*(9), 10839–10846.

Knowles, W., D. Prince, and D. Hutchison (2012). Perceptual Influences on Risk Assessments and the Challenges for Information Security and Network Management. In *Proceedings of the 13th Annual Post Graduate Symposium on the Conservence of Telecommunications, Networking and Broadingcasting (PGNET2012)*.

MICIE (2011). Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures.

Morris, T., R. Vaughn, and Y. Dandass (2012). A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems. In *45th Hawaii International Conference on System Sciences*, pp. 2338–2345. IEEE.

Patel, S. C., J. H. Graham, and P. A. Ralston (2008, December). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management 28*(6), 483–491.

Peterson, D. (2009, March). Quickdraw: Generating Security Log Events for Legacy SCADA and Control System Devices. In *2009 Cybersecurity Applications & Technology Conference for Homeland Security*, pp. 227–229. IEEE.

U.S. Department of Homeland Security (2009). Primer Control Systems Cyber Security Framework and Technical Metrics.

Verba, J. and M. Milvich (2008, May). Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS). In *2008 IEEE Conference on Technologies for Homeland Security*, pp. 469–473. IEEE.

Xiao, F. and J. McCalley (2009, February). Power System Risk Assessment and Control in a Multiobjective Framework. *IEEE Transactions on Power Systems 24*(1), 78–85.

Xu, Y., Z. Dong, K. Meng, R. Zhang, and K. Wong (2011). Real-time transient stability assessment model using extreme learning machine. *IET Generation, Transmission & Distribution 5*(3), 314.

Xu, Y., Z. Y. Dong, L. Guan, R. Zhang, K. P. Wong, and F. Luo (2012, August). Preventive Dynamic Security Control of Power Systems Based on Pattern Discovery Technique. *IEEE Transactions on Power Systems 27*(3), 1236–1244.