DOI: http://dx.doi.org/10.14236/ewic/ics-csr2014.2

Socio-Technical Security Analysis of Industrial Control Systems (ICS)

Benjamin Green
Lancaster University
Lancaster, Lancashire, LA1 4WA
b.green2@lancaster.ac.uk

Daniel Prince
Lancaster University
Lancaster, Lancashire, LA1 4WA
d.prince@lancaster.ac.uk

Utz Roedig
Lancaster University
Lancaster, Lancashire, LA1 4WA
u.roedig@lancaster.ac.uk

Jerry Busby
Lancaster University
Lancaster, Lancashire, LA1 4YW
j.s.busby@lancaster.ac.uk

David Hutchison
Lancaster University
Lancaster, Lancashire, LA1 4WA
d.hutchison@lancaster.ac.uk

Focusing on technical security can lead to shortfalls in the understanding of social and organisational security challenges. This paper proposes a method for analysing social, technical, and organisational security challenges, in regard to industrial control systems (ICS). This method is applied to a target organisation dependent on ICS, to validate the approach and gain initial insight into the organisation's perspective on security for ICS.

Keywords: Industrial Control System, ICS, SCADA, Security, Social, Technical, Organisational, Survey

1. INTRODUCTION

Industrial Control Systems (ICS) are used within various industries on a global scale, for the automation and control of operational plants. Example industries include, electricity, water, wastewater, food, and transportation (Stouffer et al. 2013). A number of these industries form part of the United Kingdom's critical national infrastructure (CPNI 2014), and while recent events, most notably the discovery of Stuxnet in 2010, and Flame in 2012 (Miller and Rowe 2012) have raised the awareness of technical issues/vulnerabilities found within ICS, even acted as a catalyst for further technical research (McLaughlin 2011), a gap remains in understanding social and organisational challenges across such systems. The two core contribution of this paper are:

1. A method for which technical, social, and organisational challenges can be analysed.
2. An empirical dataset, used to validate the proposed method, and providing insight into social and organisation perspectives.

Sections 2 and 3 propose a method for defining individual subsections of ICS, and workforce role groups. Sections 4 and 5 outline the survey and results, used for validation of the proposed method. Section 6 provides a conclusion and the direction of future work.

2. A SIX LEVEL APPROACH

A common approach when analysing ICS security, is to consider the system in its entirety. However we believe that a more detailed definition of ICS is required to analyse independent ICS subsections, such that greater detail may be obtained on how and where technical and non-technical issues are exposed. Summarisations such as "the CIA triad is reversed for control systems" (Fenrich 2007) provide little detail, and are too high-level for remediation and mitigation techniques to be employed. Furthermore, in such complex systems, it is unlikely every individual working across each independent subsection would hold this view. Understanding each subsections interdependencies, alongside system wide organisational and social structure will provide a holistic view of security challenges. However, this can only be achieved once a clear definition of system subsections and role groups have been established. We believe that by understanding system challenges at a low-level (individual subsections), a foundation is formed, on which further holistic (system wide) analysis can be conducted.

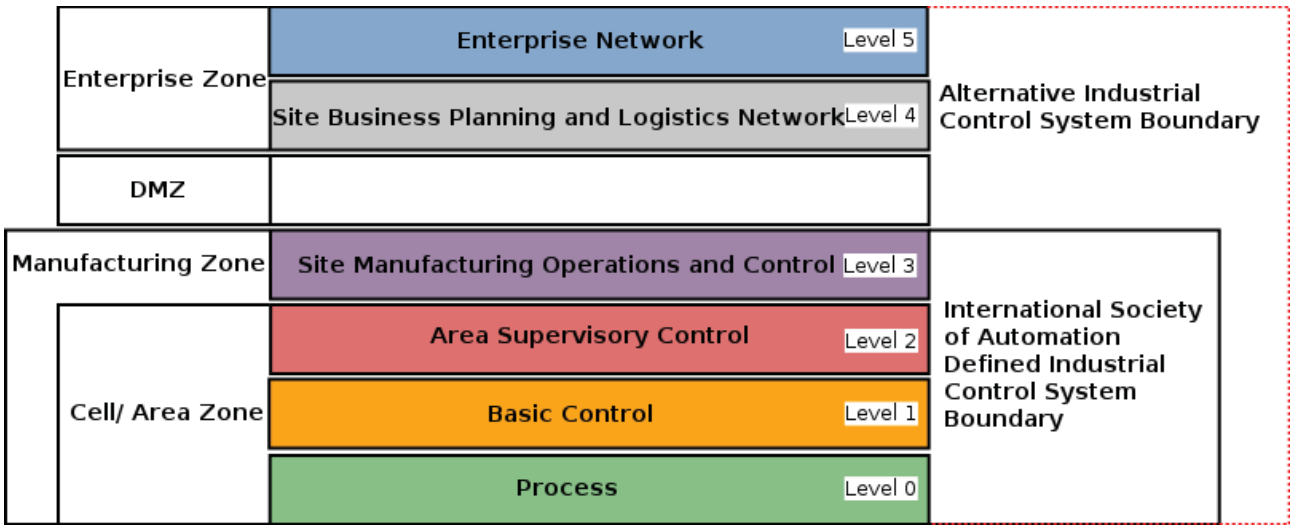

Figure 1: *ICS Levels (Adaptation of Didier et al. (2011))*

Figure 1 provides an adaptation of Didier et al. (2011) Perdue model diagram, depicting the basic construct of a Six Level ICS. While the ISA define a ICS boundary as levels zero to three (Cosman 2007), we suggest an alternative definition, which considers inclusion of the demilitarised zone (DMZ), and levels zero to five (see Figure 1). Due to the ever-expanding ICS functionality provided within enterprise networks, their inclusion is essential when assessing security challenges.

This method for identifying ICS subsections provides the foundation for detailed analysis, technically and from a social and organisational perspective. Not only do devices residing within each level rely on one another to function at a technical level, but also on those who operate and support/maintain them. Although operational and support/maintenance structures will differ from organisation to organisation, the six level structure will remain. Rather than treating ICS as a single entity, this approach will allow for a clear, more concise analysis to be conducted across each defined level.

3. ROLES RESPONSIBILITIES AND ACCESS

The complexity of a typical enterprise network, requires the adoption of access controls. Based on Authentication, Authorisation, and Accounting (AAA), access controls underpin the ability to control users privileges (access to systems and services), while simultaneously providing a method by which logging of activities can be conducted. Restrictions are often enforced based on an individual's job role, via role-based access controls (RBAC) (Sandhu 1998). The same principles apply to physical access to specific buildings, rooms, etc. The management of digital and physical restrictions applies to ICS environments. However this goes beyond the scope of this paper. Importantly, due to the size and complexity of ICS, there are likely to be clear distinctions between access levels (digital and physical) granted to individuals working within each ICS level, and across varying job roles. This is both a social and organisational issue, one that must be reviewed in conjunction with technical challenges.

Roles vary between organisations; however within ICS a role typically falls within one of six categories; Junior Operator, Senior Operator, Supervisor, Instrumentation Technician, Engineer, and Manager (Singla and Khosla 2012). Taking a higher-level view of these six roles, they fall within one of two categories; operator, and support/maintenance. Although the two role groups outlined here do not guarantee an individuals access restrictions, they provide a baseline, and clear indicator of an individuals core function. Importantly for the assessment method, they provide a simple abstract way to classify workers. The six previously listed role groups could be mapped effectively into either higher-level group.

3.1. Operator

The operator category is defined as those who use ICS within their daily duties. Based on ICS level, this could include physical access to sites and control rooms. The operator role may not modify or configure ICS devices in any way. A typical access control level would be read-only. Operators can be described much the same as End-Users within conventional IT systems.

3.2. Support/Maintenance

The support/maintenance category is defined as those who provide support for, and maintain,

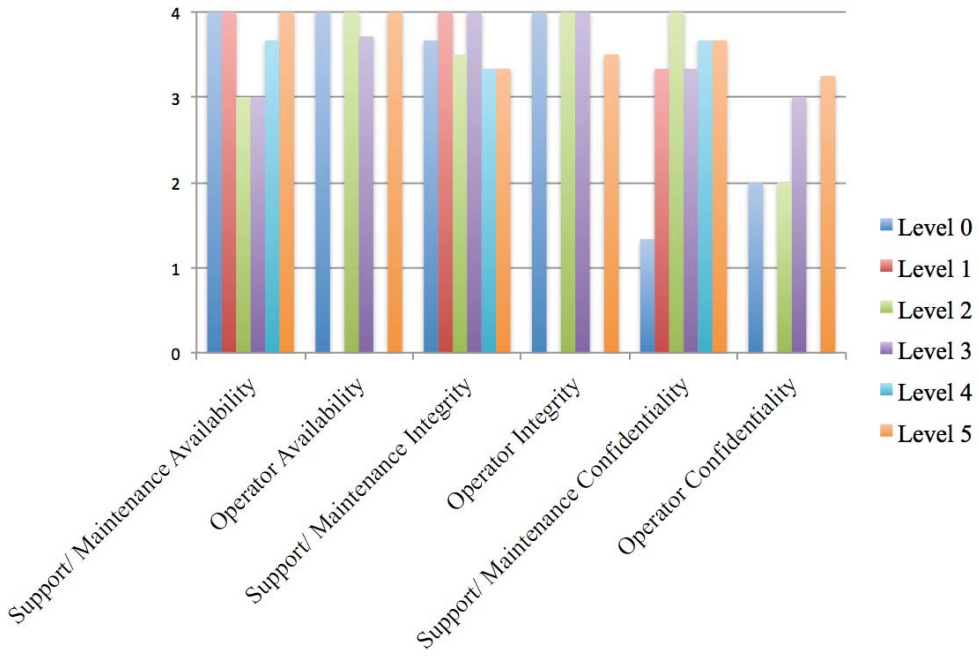

Figure 2: *Average Importance Ratings*

ICS. Based on ICS level, this could include physical access to sites, control rooms, and datacentres. Unlike the operator group, modification, configuration, and replacement of ICS devices is conducted by this group. It is likely administrative access, and full control rights, are available to this group. A typical access control level would be read-write-execute.

4. SURVEY DESIGN AND QUESTIONS

Having provided a method, by which individuals working within ICS can be separated based on the level in which they work (Section 2), and their core role (Section 3), the following survey adopts this method and applies it to a real-world ICS operator for validation, and to gain insight into social and organisational views.

Based on the method outlined in Sections 2 and 3, the first two survey questions are used to establish which level, and job role, each participant is linked with:

1. Which level (0-5) do you most frequently work with?
2. Do you operate, or provide support/ maintenance for this level?

In conventional IT systems, use of the Confidentiality, Integrity, and Availability (CIA) triad is common practice. Categorised as “Security Basics” constituting the “hallmarks of security we all strive for” (Walker 2011). Stewart et al. (2011) identifies that CIA is used to assess the completeness of security controls or approaches. Although other models are used in the analysis of ICS (e.g. Safety, Reliability, and Availability (SRA)), they often focus on safety related risks. The CIA triad should normally be adopted when analysing systems and their data, not associated safety risks. The CIA triad has been chosen here, as the core focus of this survey is to better understand social and organisational perspectives associated with systems and data, not safety. However, we believe the basic approach could be extended to include these.

Using the CIA triad as a basis for this survey, involves understanding how individuals working with ICS prioritised each tenant. The following four questions provide basic prioritisation details, and importance ratings for each tenant, using a 0-4 scale, ranging from “not at all important” (0), to “very important” (4):

3. Please prioritise availability, integrity, and confidentiality. (Place in order of highest priory first)
4. How important is availability?
5. How important is integrity?
6. How important is confidentiality?

5. SURVEY RESULTS

In total, thirty participants completed the survey. Across each level, with the exception of one and four,

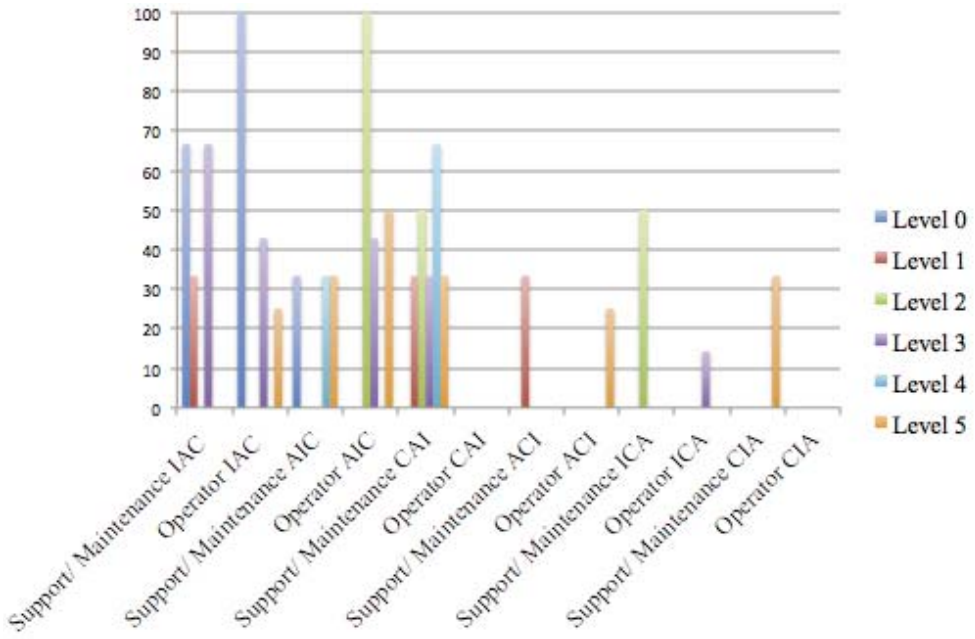

Figure 3: *Average CIA Prioritisation*

results were obtained from both role groups. The failure to obtain results for operators within levels one and four, was due to device limitations (no human machine interface). Also, for the purpose of this survey we incorporated DMZ devices into level four. This was due to the DMZ and level four environments being shared within the organisation surveyed.

Key finding are displayed in Figures 2 and 3. Both Figures highlight results across every level, and role group, established through separation of results based on the responses provided to questions one and two. For each subset of results, and average has been calculated. Calculating the average, allows for a clear picture to be formed of the overall group (e.g. Level zero operator, Level three operator, etc.).

What these results show, is that disparity exists in the views of individuals working across each ICS level, and in varying roles. Therefore demonstrating validity in the proposed method. In viewing these results from a social and organisation perspective, we can see individuals surveyed at level zero, have less concern for system and data confidentiality than those working in all other levels. Also, the operator role prioritises availability and/or integrity above confidentiality 100% of the time, compared to the support/maintenance role, which prioritises confidentiality above integrity and/or availability 53% of the time. This diverse set of results indicates that the ICS workforce surveyed here, have level and/or role specific, priorities, challenges, and goals. Although it is important operationally for each level/role to have a core focus, it should allow for flexibility, particularly where confidentiality is concerned. Although confidentiality within some levels/roles is prioritised lower than others, it must be seen as an important factor, for the protection, and long-term success of any ICS.

6. CONCLUSION AND FUTURE WORK

The results show that our method is able to highlight social and organisational characteristics based on operational level and role. Therefore, having proven a research method by which division of ICS can be achieved, and applied to the collection of data through the use of a survey, we are confident that if used in parallel with technical evaluation, a holistic view will be formed, allowing for social and/or technical mitigation techniques to be employed.

While this survey only provides a small cross-section of results, the varying opinion of CIA could be an indication of a fragmented approach to system and data security. If an organisation fails to provide a coherent message to its entire workforce, the potential for successful vulnerability exploitation could be heightened. For example, the survey results here could be seen as an indication of vulnerabilities within level zero i.e. having a lower concern for confidentiality, and with the adoption of Ethernet-based devices at level zero, technical vulnerabilities are introduced. Akerberg and Bjorkman (2009) show how it is possible to gain control of Ethernet-based devices operating over the Profinet protocol. With this, an organisation's lack of guidance from a security perspective at level zero, could lead to the

technically unsecure adoption of Profinet devices, and the added potential for social engineering, further aiding attackers.

We recognise that the number of survey participants was relatively low for such a large system. However, it has provided a basis for further methodological refinement, while gaining early insight into social and organisational challenges. It also demonstrates our fundamental belief, that ICS security analysis needs to be fine-grained (level and role based). Statements made summarising CIA within ICS provide very little detail, and may be factually inaccurate depending on the role, and ICS level in question.

We intend methodological improvements in order to gain a more detailed understanding of the challenges ICS face. While maintaining the six level approach, and role division, our future work looks to develop a series of questions allowing us to align individuals with levels, and more detailed roles. While detailed role descriptions are unlikely to be comparable between organisations, the identification of roles based on these questions will provide greater detail, and allow for cross system/organisation analysis to be conducted.

7. ACKNOWLEDGEMENTS

The authors are grateful to GCHQ for their funding of this work, and to Airbus Group for their continued support and valued input.

REFERENCES

Akerberg, J. and Bjorkman, M. (2009) Exploring security in PROFINET IO. In: *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International*, 406–412.

Cosman, E. C. (2007) An overview of ISA99 Part 1 ISA99 Part 1 Security for industrial automation and control systems: Terminology, concepts and models. In: *ISA EXPO*, 28.

CPNI (2014) *The national infrastructure.* Available from http://www.cpni.gov.uk/about/cni/

Didier, P. et al. (2011) *Converged plantwide ethernet (CPwE) design and implementation guide*, CISCO Systems. Available from http://scholar.google.co.uk/scholar?q=cisco+Converged+Plantwide+Ethernet+design+and+implementation+guide&btnG=&hl=en&as_sdt=0,5#0

Fenrich, K. (2007) Securing your control system. In: *50th Annual ISA. POWID Symposium/17th ISA POWID/EPRI Controls & Instrumentation Conference*.

McLaughlin, S. (2011) On dynamic malware payloads aimed at programmable logic controllers. In: *Proceedings of the 6th USENIX Conference on Hot Topics in Security. HotSec*. 10.

Miller, B. and Rowe, D. (2012) A survey SCADA of and critical infrastructure incidents. In: *Proceedings of the 1st Annual Conference on Research in Information Technology, RIIT '12*. New York, NY, USA, 51–56.

Sandhu, R. S. (1998) Role-based access control. *Adv. Comput.*, 46. 237–286.

Singla, R. and Khosla, A. (2012) Intelligent security system for HMI in SCADA applications. *Int. J. Modeling Optim.*, 2 (4). 444–448.

Stewart, J. M., Tittel, E., and Chapple, M. (2011) *CISSP: Certified information systems security professional study guide*. 5th ed. New York: John Wiley & Sons.

Stouffer, K., Falco, J., and Scarfone, K. (2013) Guide to industrial control systems (ICS) security. *NIST Special Publication*, 800. 82.

Walker, M. (2011) *CEH certified ethical hacker all-in-one exam guide*. 1st ed. New York: McGraw-Hill Osborne Media.