"How Long is a Piece of String": Defining Key Phases and Observed Challenges within ICS Risk Assessment

Benjamin Green, Daniel Prince, Jerry Busby, David Hutchison
Lancaster University
InfoLab21, Lancaster, LA1 4WA, United Kingdom
{b.green2,d.prince,j.s.busby,d.hutchison}@lancaster.ac.uk

ABSTRACT

The numbers and severity of global cyber security attacks on Industrial Control Systems have increased over recent years. However, there are also significant efforts to improve defensive capabilities. While comprehensive reviews of risk assessment efforts exist, little detail is currently available on how they are being applied by security practitioners. This paper provides a summary of the approaches adopted by security practitioners, outlining key phases applied to risk assessment, application of existing predefined methodologies, and challenges faced throughout the overall process.

KEYWORDS

Industrial Control Systems; ICS; SCADA; OT; Cyber Security; Risk Assessment

1 INTRODUCTION

Industrial Control Systems (ICSs) are applied to the monitoring, control, and automation of operational processes across a range of sectors, some of which can be considered critical national infrastructure (CNI) [7]. Cyber attacks targeting ICSs have become more prevalent and widely publicised, the latest of which being an attack targeting the Ukrainian energy sector [8]. These can, however, be seen as a catalyst towards the development of defensive actions.

One key stage required in the development of defensive capability is an understanding of existing risk, which can be used to better educate and promote discussions on appropriate mitigation strategies. This in an area which has seen coverage from both academia and industry, with a range of risk assessment approaches. However, the application of these activities within the security practitioner (SP) space has seen little coverage. This work presents the findings from interviews conducted with SPs, all of whom are actively engaged in the assessment of ICS risk.

2 RISK ASSESSMENT

Risk management is the strategic approach to understanding and pre-emptively reducing the impact of risk realisation against a target under consideration. Typically encompassing four distinct domains: risk framing, assessment, response, and monitoring [18]. Here we focus specifically on risk assessment. Designed to provide an improved understanding of risk, which if realised, could impact organisational objectives. In addition, risk assessments can been used to evaluate existing controls and their adequacy [2].

While there are a number of established approaches to the assessment of risk, particularly within the standards community [2], it can be seen that their application to ICSs poses a challenge. Therefore, the development of tailored ICS specific approaches have been witnessed across both academic [3] and industry contexts [17]. Our previous work summarised a handful of approaches within existing industry standards and guidelines (S&G) [13], with the work of [20] and [6] providing more comprehensive discussions. However, existing works have provided little to no discussion from real-world SPs. More specially, how is the assessment of risk achieved, including core phases, application of existing approaches, factors of importance, and common challenges.

3 INTERVIEWS

The following questions can been see as core to our interviews. For a more complete view of the applied interview protocol/guide see Green et al. [16]. For a more complete view of the methodology applied to data collection and analysis see Appendix A.

- Do you work for an ICS operator?
- Do you work for a Cyber Security consultancy firm?
- Do you conduct Cyber-Security risk assessments?
- What do you understand the term ICS to include?
- At a high level, what are the core phases you go through when conducting an assessment?
- What are your design/implementation influences in the described phases?
- Which of the defined phases is the most important, and which proves the most challenging to accomplish and why?
- Please can you summarise the process you go through for (Read back phase 1, then phase 2, etc.)?
- What do you think of currently available standards and guidelines?
- Is there anything you would like to add?

4 RESULTS

The following subsections present an aggregated summary of salient points raised across all interviews. As described in Appendix A, this focuses more towards a discussion of captured data, as opposed to a statistical summary. Relevant quotations are included where possible to further highlight findings.

CPS-SPC'17, November 3, 2017, Dallas, TX, USA

ACM ISBN 978-1-4503-5394-6/17/11…$15.00
https://doi.org/10.1145/3140241.3140251

4.1 Phases of a Risk Assessment

Ten core phases were identified across all interviews, a summary of which is provided here. As we have aggregated interview data, not all SPs feature in each of the described phases, nor do they align directly to points made within the discussion of each phase.

4.1.1 Scope/Understand the System. Described by some SPs as two separate streams of activity, the processes applied to scoping and understanding the system often overlapped, and ran in a cyclic manner.

Basic scoping exercises were described as a starting point for engagement with an organisation. The length and depth of scope was mostly associated with constraints placed on time and financing, with sector context also playing a role. Although scope was considered a point to which both parties must agree from the beginning, this could be seen as a starting point with levels of flexibility required. Understanding what it is the organisation is trying to protect, what aspects of the systems are most critical, who is responsible for decision making around security, which operational sites to sample, etc. all impact scope. Throughout an engagement knowledge across these areas builds, further impacting scope. For example, where an inventory is provided of devices and systems in/out of scope, should critical relationship between devices across these two groups be discovered, addition to in-scope could occur.

"Well, it's how long is a piece of string, really...."

A number of resources were discussed across this phase, these included access to relevant people, network diagrams, organisational structures, operational design documents, historian configuration, asset inventories, purchase orders, operational/procedural documents, network traffic, physical security parameters, safety documentation, etc. While obtaining resources such as these was described as an important process within the phase, often achieved in an office based environment, its validation was almost always described as a core requirement. Most validation was conduced on-site (the operational facility in question). Exceptions to this included the use of question sets related to network and physical security, procedures, governance, staff training activities, etc. used in both office/on-site exercises with workers across different areas of the business.

"You are massively dependent on the system owner's and the system operator's knowledge at that stage...."

In order to extract the information require, SPs relied heavily on the knowledge and experience of system owners and operators. In relation to more technical details, subject matter experts were also called upon (e.g. PLC engineers, mechanical engineers, etc.). When criticality and interdependency of systems was established, the level of questioning was adjusted. If a system were considered less critical, fewer questions, and therefore time, was consumed in fully understanding it. This level of flexibility can be seen to reduce the involvement of those responsible for system operation and maintenance.

"You need to add that context to it...."

Across SPs, the level of understanding discussed varied. However, to summarise it can be considered as a broad picture of how the system is architecture and operated, including a mix of technical operational process characteristics, integrated safety functions, failure modes, etc.; technical details related to the network, including the location of computational resource and function; existing controls (physical, technical, procedural, etc.); processes for recovery, including details of relevant backup procedures; and general maturity with regards to cyber security, including any training activity, policies, etc. and their prevalence/acknowledgement across multiple business areas.

The use of spreadsheets and relational databases were discussed as methods by which data could be recorded. In addition to these, some SPs organisations had developed their own tools, these were considered intellectual property (IPR) and not discussed in any detail. Given the diversity of context, and variance in scope, some SPs felt that standardising the approach to documentation was unrealistic. Instead opting for a more ad-hoc approach, with previous techniques adapted to fit the system under review.

4.1.2 Understand Risk Appetite. Those responsible for instigating an exploration into existing risk can provide some initial insight into organisational risk appetite. However, engagement with the wider business was discussed as a more useful exercise in understanding risk appetite. Used to gauge the level of detail required within the assessment process, this phase was described as an aid in scoping and contextualising risk.

"What the initial risk appetite levels were in terms of from a corporate perspective and from a national perspective...."

Understanding risk appetite presented an interesting view, with inclusion of human resource from technical, operational, and managerial backgrounds, providing more holistic details, covering organisational processes and what constitutes risk. Furthermore, the suggestion of providing a national perspective was proposed. Where some ICSs form part of a countries CNI, obtaining this additional viewpoint and feeding it back into the organisation, could be of value where risk is not fully understood within a cyber context.

4.1.3 Cyber Security Community Engagement. Engagement with the cyber security community was considered within the risk assessment process as a form of information gathering. Used to gain a greater understanding of threat actors, developing capability (offensive and defensive), and likelihood of the organisation under review being targeted. Example sources included the UK's national cyber security centre (NCSC), Idaho National Labs, and general media outlets with articles focused on cyber security.

4.1.4 Understand Threat Actors. Understanding who is likely to target the organization under review, their capabilities, and motivation, was used as a method of contextualising risk. Example actors discussed included nation states, organised crime, amateur hackers, lobby groups/activists, and insiders. Difficulties around quantification of risk posed by threat actor groups was acknowledged, yet having a basic view of expertise, tools/techniques used, level of persistence, etc. were all described as useful in understanding existing risk posture in the current climate.

"As far as I am aware, there is no perfect accepted methodology for this. I mean, I've created a few myself where you allocate numerical scores for different aspects of capability and intention...."

The use of historical attack data was described as one approach for obtaining a greater level of understanding, particular where

systems of a similar nature have been targeted in the past. Even where direct parallels cannot be found, should certain tools and techniques be attributed to a specific threat actor, expansion of those towards the system under review can be used as an indicator capability extension.

4.1.5 Understand Vulnerabilities and Impact. Described by some SPs as two separate streams of activity, the collation of information derived through understanding vulnerabilities and impact presented an overlap, hence their collation here. This phase considered system attributes extended beyond conventional IT system, therefore the application of existing IT based methodologies can't always be easily adopted. In terms of a defined methodology, some SPs believed a concrete formalised approach was not available. However, a systematic view of identifying vulnerabilities was applied, focusing on equipment and the operational process as a two-stranded approach.

"Slightly different from just a control system down to an enterprise system, hence why you can't always easily adopt the enterprise methodologies...."

Discussion on relevant data to inform this phase was typically split between technical and operational/procedural factors. The output of which was captured through use of spreadsheets, custom tools (IPR), databases, etc. These would be used to understand how a defined impact could occur, building links between likelihood of vulnerability leading to impact given the existence of current security controls/practices.

"Sitting down and going through an awful lot of cups of tea with the people who run the system and saying, what are the impacts if this item or this part of the process were to go wrong and what are the mitigations that are already in place...."

Data captured from a technical perspective covered several points. Logical analysis of system components was conducted, for example, should a valve be IP enabled, and can be remotely accessed with no protection/authentication, a vulnerability is present. This can be considered a theoretical exercise, however other SPs made use of tools (NMap, Nessus, and bespoke IPR) to identify known vulnerabilities. Factors related to device support frameworks (e.g. is the vendor still releasing updates) were also discussed. Technical points mostly related to what connections exist to and from a device, and subsequently the likelihood of it being accessed by unauthorised parties. Questioning/Reviewing logic code of certain devices (PLCs and RTUs) presented a greater depth of review, however this was not broadly adopted by all SPs.

"The essential but slightly tedious thing of just you go through the elements of the system and look at whether each element is vulnerable to what you believe is the significant threat to it...."

Data captured from an operational/procedural perspective also covered several points. These discussions included understanding how operational processes can exceed accepted parameters, and what states they cannot fall into. This typically involves numerous discussions with stakeholders across the operational environment. As part of these discussions, taking note of electro-mechanical mitigations was another important point, alongside physical access restrictions (sign-in sheets, cameras, vetting, etc.). Understanding supplier relationships presented an addition consideration for some SPs, this included discussion on how/where PLC and RTU logic code was handled and stored.

"An awful lot of attacks, let's call them malicious attacks, at the moment may not simply occur because the safety systems will prevent that...."

In providing meaning around potential impact observed, engagement with the broader business was sought. This was seen to allow for a more comprehensive view with regards to impact on overall business objectives. With the categorisation of impact typically aligned to simple high, medium, and low metrics, additional confirmation of this kind was therefore seen as highly valuable. Furthermore, where prioritisation of impact was conducted, additional viewpoints can again prove highly valuable.

"We just did a simple three tiered model of high, medium, low and what are the, essentially what are the impacts that you are not willing to accept...."

4.1.6 Assess Maturity. The assessment of cyber security maturity was discussed, however the level of detail provided was limited. The Cybersecurity Capability Maturity Model (C2M2) was applied as one option. The decision to assess maturing using this model was described as a good way to depict security posture and impact. It was noted that this approach does not go as far as understanding engineering safeguards, but can be helpful when conveying business risk, aiding in the understanding of maturity across the organisation under review.

"C2M2 shows the posture and approach to security and the technical assessment shows you what the impact of that is...."

4.1.7 Assess and Prioritise Risk. Assessment and prioritisation of risk forms the core component of most methodologies discussed. A number of approaches to this were described. Some of which applied pre-existing techniques from S&G, or internally developed approaches from the organisation under review, with others described as more informal discussions based on professional judgement.

"The organisation will have their own health and safety risk assessment matrix, which is likelihood against a consequence and it's health and safety, business loss, reputation loss, for example...."

Some described this phase as a blend of art and science, requiring flexibility and a degree of imagination. Putting yourself in the mind of an attacker, and thinking in a non-liner fashion provides a foundation to this narrative. This can be further emphasised by consideration of dependencies between system components, no matter how subtle.

"It is a blend between art and science...."

The approaches adopted by most SPs was adapted on a client-by-client basis. A one size fits all approach was considered to be incompatible given the scope and complexity of systems across varying sectors. Understanding where a client is currently, and where they are looking to go, aids in selection and delivery of a given approach.

"Every situation is different, you know, what may be absolutely brilliant for Client A may be not really relevant so much to Client B...."

A number of external resources were discussed in relation to the allocation of risk level. Examples include risk matrices from the

likes of ISA 62443. Based on a selection of vulnerability and impact data, Low, Medium, and High, risk categories could be defined. The use of a scoring matrix from existing S&G was considered a positive approach by some, allowing for a level of repeatability, and added credibility to any provided output ("Not just pulled from thin air"). CVSS data could also be used to feed into vulnerability calculations. Additional tools, such as compliance models, were also considered useful, acting as a reminder to explore forgotten factors. Where clients employed existing approaches to the quantification of risk, with examples related to health and safety, reputational damage, etc. their adoption within the process was conducted.

"I think it's quite handy to have some of the compliance models because it reminds you that you've got to, you know, look at certain areas. But you need to keep an imaginative open mind...."

Some SPs felt providing clients with detail exceeding "Low, Medium, and High", or "Green, Amber, and Red", was unnecessary and unhelpful, further complicating the output of an assessment. On occasion the use of "Very High or Very Low" could prove to be a valuable addition.

"It would generally be simply low, medium and high.. if you try and do any more than that, you always up using three numbers anyway, you always end up feeling that it's going to be low, medium, or high...."

The use of spreadsheets across this phase was prevalent. Applied not only to documenting relevant data, but also in feeding that data into a form of matrix or metric. Some SPs considered this to allow for a tick box process/exercise to be conducted. Others developed custom tools/software packages, considered IPR. Fault tree analysis was also briefly discussed by one SP as an option used on occasion to aid in the understanding of risk and better inform the client.

"Normalise that information, use the base information we got initially from our interview as to where the base level of risk acceptance is, and then we use that to help develop what we feel will be their actual risk exposure...."

Where risk is presented as the assessor understands it, returning back to various stakeholders within the business to further contextualise and priorities risk was required. Activities around the normalization of data towards initial discussions on risk tolerance/appetite was considered useful in providing a more meaningful output. This was also described as useful in the identification of additional procedures/processes which had not been accounted for during earlier phases.

4.1.8 Penetration Test. Briefly discussed as part of the "cycle back" phase, penetration tests were also considered as a phase in their own right. Where information had been gleaned throughout the process with regards to a systems susceptibility to attack, on occasions a penetration test was conducted to provide additional validation of risk prior to the consideration of appropriate mitigation.

4.1.9 Discuss Risk. The discussion of identified risk in parallel to standard paper based reporting was raised as an important phase, ensuring all points were understood by both parties. The identification of relevant stakeholders within this phase was essential, as they may not always be directly involved in associated activities. Typically, stakeholders would be included from across the business, coving a broad range of technical and managerial viewpoints. Dependent upon sector, regulators may also be involved. Inclusion of a broader stakeholder base was seen as a positive step for the assessor, on occasion providing additional detail with regards to business direction (e.g. asset x will be decommissioned in six months).

"Sit down with the appropriate stakeholders, say, normally the service owner and normally the risk owner. So then you've got someone who is ultimately responsible for whatever that technology is, whatever the outcome the business and/or organisation is trying to drive from it...."

Due to the background of some clients, presentations and reports provided for use during discussions were described as suitable/designed for management. Discussion of risk mitigation was also provided, again using high-level terminology suitable for a non-technical audience. These discussions could include the use of S&G to emphasis use of certain security controls. Furthermore, road-maps for future evolution could be provided here. The application of bronze, silver, and gold levels was just one example of how the aforementioned roadmap could be conveyed to a non-technical audience (e.g. bronze = 4 controls, silver = 7 controls, and gold = 10 controls).

4.1.10 Cycle Back. Once the risk assessment process had been completed, some SPs went back to the start and cycled through for a second time. This was done at differing stages. For example, some cycled back immediately to confirm all risk had been captured and assessed accordingly, others once security controls had been considered to measure hypothetical risk reduction, or post selection and physical implementation of security controls.

"You need to do the refresh because, actually, by the time you've taken those steps, or planned them, you may find that actually the threat has slightly changed...."

This activity was considered import for a number of reasons. Change in threat landscape was one such reason, with understanding of capability and intent providing a constantly changing picture. Induction of risk was another, where security controls were suggested or implemented post-assessment, their inclusion could induce risk. Where the latter point was of greatest consideration, use of vulnerability and penetration testing services were also considered.

4.2 Most Challenging

When considering which stages within the risk assessment process present the greatest challenge to accomplish, understanding the system was of highest prevalence, with scoping, understanding risk appetite, and understanding threats also discussed.

Challenges related to understanding the system were largely directed towards reliance on system operators and their engagement within the assessment process. Where matching physical and logical characteristics is discussed as a key task, it can be seen that understanding individual aspects of an operational process, and their importance within the bigger picture, is of great importance. Across these points are sets of procedural requirements one must take into consideration with regards to the systems ongoing operation and maintenance. To gain the level of detail required across

these, finding appropriate teams and individuals was considered a significant challenge. One might be able to ascertain nine of the ten pieces required to build a coherent picture, yet without appropriate resource acquiring all ten becomes impossible. Furthermore, it was noted that some individuals can prove hostile, viewing the assessment as a threat to their way of working/trying to catch them out. As most engineers are not focused on cyber security, it was noted significant effort to extract relevant information and relay it back to develop clarity of baseline understandings was required.

"It's not a witch hunt...."

Additional challenges raised related to supplied resources. These included IT related documentation, outdated diagrams, and continuing evolution of systems, all leading to a lack of one single comprehensive resource (individual or document set) with any real understanding/detail. These were in part attributed to the continued use of system integrators, and lack of clear hand-over processes. It is for these reasons teams are sent into operational environments, validating any details provided within off-site engagements. However, this process instigates further challenges an assessor must overcome.

"A lack of real understanding of how the systems work..network diagrams if they exist are often inaccurate. A lot of these systems are built by systems integrators, so the knowledge of how they work and so on, stays with the systems integrators...."

Challenges related to scoping can be predominantly described as managing expectations. Assessments can be limited by time and funding, therefore agreement in terms of output must be managed. Input from the organisation under review in relation to where the focus should be is critical, and often shifts throughout the process.

"The hardest thing to achieve was to really define what the focus of interest was from a sensible, a practical point of view...."

Challenges raised in relation to understanding risk appetite, highlighted deficiencies in an organisation's understanding of cyber security and its link to operational assets. Points raised around risk appetite included limited detail on criticality of operational assets, and the impact of their failure to wider business operations. Without engagement from management, understanding wider business impact is often limited. Therefore, obtaining a solid understanding of acceptable risk, and subsequent conveyance of risk can be arduous.

"You raise awareness of them understanding what the risks are in their systems, because, you know, people are not born thinking about security...."

Challenges raised in understanding relevant threats was limited. However, examples included the behaviour of malware, being relatively straightforward to map with a given context, compared to that of threat actors and their evolving capabilities. The use of perimeters firewall logs was proposed as a solution, used to give an indication of the techniques attackers deployed against the organisation in question.

4.3 Most Important

When considering which stages within the risk assessment process are of greatest importance, understanding the system and what to protect was of highest prevalence, with dialogue, and understanding risk appetite also discussed.

The importance of understanding the system and scope were driven by a view that you are not working to assess a single computational resource, e.g. PLC, RTU, etc., but what that resource is responsible for, overall system nuances, and possible avenues for failure. As ICSs are highly complex, one small element could enable unauthorised access to primary operational processes. Assessing risk posed to operational processes was considered the end goal, therefore understanding what they are connected to, and in-turn what that is connected to, is a fundamental requirement. This can be summarised as an understanding of devices, processes, and impact of failure. Furthermore, it was noted that operation and maintenance staff are considered components of the system, in the same way as a PLC or RTU. Subsequently, understanding their numbers and perception of risk feeds into one's ability to adequately assess risk. Once a high-level understanding is achieved, a more abstract view can be used to define a clear boundary of scope. Without this, inclusion of unnecessary systems could occur, reducing time spent in other areas. All of which requires continual dialogue, with client expectations managed and scoping extended or retracted where required.

"You are not protecting a piece of hardware, you are not protecting the PLC, a PLC is £100, you are protecting a system that it is controlling...."

When considering criticality of operational assets, and the impact their failure has on the business, understating of risk appetite is considered of high importance. This related not only to scoping and requirements for understanding the system, but also towards dissemination of findings. Therefore, risk appetite should be linked with operational processes in parallel to broader business objectives.

4.4 Use of Standards and Guidelines

Opinions of existing S&G was mixed amongst SPs. Largely considered a positive starting point, taken as inspiration, and built on to provide a more comprehensive tailored offering. The following subsections provide a summary of discussions in relation to their use.

4.4.1 Example Standards and Guidelines Discussed. While some examples are not individual S&G within their own right, they relate to a standards body/scheme/catalogue/information source, discussed in more generic terms. "ISF", "ISO 23301", "C2M2", "NESA", "NIST 800 Series", "10 Steps to Cyber Security", "IS2", and "ANSI" were discussed once. "CESG Good Practice Guides", "NIST 800-53", "HMG", and "SANS Top 20" were discussed twice. "IS1", "Cyber Essentials", and "NERC" were discussed three times. "ISO 27001", "NIST Frameworks", and "CPNI Guidance" were discussed four times. "ISO 27000 Series" was discussed five time. "ISA 62443" was discussed six times. No approaches derived from academic works were discussed.

4.4.2 Opinion of Standards and Guidelines. Where existing S&G were viewed in a positive light, highlighted attributes focused on their clear well throughout logical approach to a problem. Their use was mostly described as a good starting point for multiple sectors, allowing for customisation based on variables seen to change across

organisations, include size, sector, maturity, and budget. Their development over recent years was described as maturing, being more open to diverse minds (individuals with expertise in multiple related areas). The variety of available S&G was also considered a positive attribute by some, allowing for less mature organisation to begin their journey into cyber security (e.g. CPNI guidelines), and more mature organisations to continually re-evaluate and evolve their existing posture (e.g. ISA 62433). The output of existing IT focused assessments (ISO 27001, ISO 22301, etc.) was considered to be a useful resource within a more ICS focused assessment.

"I also think that organisations will need to just pick sections of 62443 depending on the type of organisation that they are...."

Where existing S&G were viewed in a negative light, a variety of points were raised. The most common criticism related to compliance against a standard failing to deliver a more secure environment. Other criticisms referred to the prevalence of numerous S&G, leaving end users confused on what to use and where, all with varying scale and scope. This point extended to the feeling of some S&G being too large and complex, attempting to cover too many areas within a broad non-sector specific approach, resulting in a less than ideal fit to specific sectors. Other more generic points raised included too much of an IT focus, lack of clear direction on how far one should go in assessing and mitigating risk, focus on an idealised end state, and inadequacies in addressing CNI risk given the resources of some threat actors (e.g. nation states). Committee participants were also considered as questionable, for example ISA 62443's use of the zones and conduits, derived through discussions with committee members from "firewall companies", and how its use lends itself towards the procurement of products which directly benefit the committee. Due to the points discussed here, one SP concluded "you can just tear them up and throw them away".

"I'm sure the Titanic was compliant with all the engineering and flotation standards when it sailed from Belfast...."

In more general discussions, a handful of interesting points were raised. Continuation beyond an initial assessment and subsequent mitigation was heavily emphasised. Some system owners were described as failing to understand a continuing evolution of threat landscape, requiring regular validation of defensive strategy. Suggestions around future development was also common, with some believing governments should provide clear guidance on the line between organisation vs. government responsibility for cyber security, concepts related to the collaboration of multiple bodies to create a single standard given existing approaches can be mapped across one another anyway. The use of ISA 62443 or NIST catalogues were considered to be the best options going forwards.

"I think that one of them will start winning out, my feeling it will either be you know some form of NIST or 62443...."

5 CONCLUSION AND FUTURE WORK

Across these interviews, ten key phases to a risk assessment were identified. Forming part of one initial phase, "understanding the system", was considered not only to be the most challenging to accomplish, but also the most important. The use and opinion of existing approaches defined in S&G was mixed. Where used, S&G often provided an initial base, from which more customised approaches are applied. ISA 62443 was the most prevalent across all interviews, with six of the ten SPs referring to it as a known, applicable standard.

Where we see "understanding the system" to be a key phase within the overall assessment process, it also presents a challenge to assessors. This is a salient point to which we experienced a similar reaction during some of our previous work [3, 15]. Also, we see from the broader literature that this phase receives little attention from within the academic community [6]. Therefore, our future work will seek to further develop prior concepts [13] in an effort to address this gap. Through the use of interview data discussed here, and Lancaster's ICS testbed [12, 14, 22], a practical approach will be developed and evaluated. Ensuring it can be used to bolster concepts from ISA 62443 [17], we feel, is of importance given the observed popularity.

REFERENCES

[1] Hilary Arksey and Peter T Knight. 1999. *Interviewing for social scientists: An introductory resource with examples.* Sage, London.

[2] British Standards Institute. 2010. BS ISO/IEC 31010 - Risk Management - Risk Assessment Techniques. (2010).

[3] Jeremy Simon Busby, Benjamin Green, and David Hutchison. 2017. Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk. *Risk Analysis* (2017).

[4] Donald Thomas Campbell and Julian C Stanley. 1963. *Experimental and quasi-experimental designs for research on teaching.* Ravenio Books.

[5] David Canter, Jennifer Brown, and Michael Brenner. 1985. *The research interview: Uses and approaches.* Academic Press, New York.

[6] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. 2016. A review of cyber security risk assessment methods for SCADA systems. *computers & security* 56 (2016), 1–27.

[7] CPNI. 2017. Critical National Infrastructure. (2017). https://www.cpni.gov.uk/critical-national-infrastructure-0

[8] Dragos. 2017. *CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations.* Technical Report. https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[9] James H Frey. 1983. *Survey Research by Telephone.* SAGE Publications, Beverly Hills.

[10] Deianira Ganga and Sam Scott. 2006. Cultural" insiders" and the issue of positionality in qualitative migration research: Moving" across" and moving" along" researcher-participant divides. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, Vol. 7.

[11] Barney Glaser and Anselm Strauss. 1967. Grounded theory: the discovery of grounded theory. *Sociology The Journal Of The British Sociological Association* 12 (1967), 27–49.

[12] Benjamin Green, Sylvain Andre Francis Frey, Awais Rashid, and David Hutchison. 2016. Testbed diversity as a fundamental principle for effective ICS security research. In *SERECIN*.

[13] Benjamin Green, Marina Krotofil, and David Hutchison. 2016. Achieving ICS Resilience and Security Through Granular Data Flow Management. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy.* ACM, 93–101.

[14] Benjamin Green, Anhtuan Lee, Rob Antrobus, Utz Roedig, David Hutchison, and Awais Rashid. 2017. Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17).* USENIX Association.

[15] Benjamin Green, Daniel Prince, Jerry Busby, and David Hutchison. 2015. The Impact of Social Engineering on Industrial Control System Security. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy.* ACM, 23–29.

[16] Benjamin Green, Daniel Prince, Jerry Busby, and David Hutchison. 2017. Interview Protocol/Guide. (2017). https://tinyurl.com/ybo9r9bk

[17] ISA/IEC. 2017. *Security for Industrial Automation and Control Systems: Security Risk Assessment, System Partitioning and Security Levels.* Technical Report. ISA/IEC.

[18] Joint Task Force Transformation Initiative. 2012. *Guide for Conducting Risk Assessments.* Technical Report.

[19] Nigel King, C Cassell, and G Symon. 1994. Qualitative methods in organizational research: A practical guide. *The Qualitative Research Interview* 17 (1994).

[20] William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, and Kevin Jones. 2015. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection* 9 (2015),

52–80.
[21] Grant McCracken. 1988. *The long interview*. Vol. 13. Sage, London.
[22] Ben Paske, Benjamin Green, Daniel Prince, and David Hutchison. 2014. Design and Construction of an Industrial Control System Testbed. In *PGNET*. 151–156.
[23] Michael Quinn Patton. 1990. *Qualitative evaluation and research methods*. SAGE, London.
[24] Janet Powney and Mike Watts. 1987. *Interviewing in educational research*. Routledge & Kegan Paul, Ablingdon.
[25] Herbert J Rubin and Irene S Rubin. 2011. *Qualitative interviewing: The art of hearing data*. Sage, London.
[26] Robert Philip Weber. 1985. *Basic Content Analysis* (first ed.). Sage Publications, Beverly Hills.

A METHODOLOGY

The following subsections outline our methodology, applied to the capture and analysis of interview data.

A.1 Interviews

Ethnographic observation would be challenging and time consuming, particular when considering the sensitive nature of ICSs, and would likely fail to yield detailed perspectives of SPs. Interviewing was therefore selected as an appropriate alternative [23], enabling non organisation-specific discuss. The ability to explore meanings, routines, etc. [25] all adds towards focusing, and confirmation of meaning from both parties when required [5].

We opted for a semi-structured interviewing approach, often seen as the most common form of qualitative research methods. This provided adequate flexibility with a predefined core question set, options to include improvised follow-up questions, and explore meanings should they be required [1].

A.1.1 Sample. In selecting an appropriate sample, we aimed to obtain an understanding from all relevant perspectives. To achieve this, a dual approach to the targeting of SPs was applied. The first category of SPs work for organisations who operate ICSs, i.e. information security officers. The second category of SPs provide cyber security services to organisations who operate ICSs, i.e. cyber security risk assessors.

Although ten interviews were conducted, it is noted a sample size of eight is often sufficient [21]. This extension ensured all relevant points were uncovered, adding to the sample until little additional information was provided, and ensuring the data set was large enough to make generalisations with confidence.

A.1.2 Validity. There exist sets of common threats to the validity of interview data [4]. To address these, attention was initially focused on our sample. From this, interviewing techniques applied to build rapport, trust, and openness were adopted. Questions were drawn from initial understandings achieved through a review of existing literature.

Emergence of interesting content upon completion of interviews is common [24]. These were noted and added to the interview protocol/guide as additional prompts, useful for future and potential re-interviews. This approach allowed the interview process to evolve in a structured and managed way, while eliciting pertinent information.

A.1.3 Reliability. Of primary concern to data reliability is interviewer bias i.e. the ability to trust findings are not derived from research instruments, or as a result of an interviewers quirks and improvisations. In relation to this is the perspective of "insiders", defined as interviewers who share similar cultural, ethnic, linguistic, national and religious heritage [10], or where the interviewer and interviewee are part of the same organisation. This can prove highly valuable when seeking additional participates, understanding organisational structures, etc. [1]. However, it can also impact data reliability, with an increased probability of assumptions based on personal perspective. Neutrality beyond the aforementioned "insider" bias was also considered throughout the interview protocol/guide design process, and during each interview. Acknowledging personal background, age, class, etc. as a potential influence in the direction and output of interviews. Positive attributes of our past experiences were utilised in the interview protocol/guide, and interview process, however to account for the possibility of negative attribute inclusion, this document and subsequent transcripts were reviewed by the team.

A.1.4 Practical Technique (Telephone Interviewing). Telephone interviewing was selected due to cost and time saving, compare to an in-person approach. However, unique challenges do exist. For example, fixed-response questions are recommended, as open-ended questions are harder to manage in this setting [9]. While this is acknowledged, open-ended responses were necessary to achieve the required level of detail. Additional challenges based on interviewee focus were noted and addressed in designing the interview protocol/guide, e.g. reduction in technical depth.

A.2 Analysis

Template analysis was selected for its highly flexible approach to the analysis of qualitative data [19]. Sitting between content analysis [26], and grounded theory [11]. It has seen an increase in popularity since the work of King, Cassell, and Symon [19].

Although harbouring fewer specified procedures, recommendations for its use are proposed [19], these have been followed within the analysis of our data. For example, through use of our interview protocol/guide, an initial code set (data categorisation) was constructed. This code set was hierarchical, limited to allow for further granularity or abstraction if required. Too many pre-defined codes may constrain/confuse analysis, too few may cause a lack of direction. Upon a brief review of two transcripts, additional codes were added. These codes were reviewed by a separate researcher for validation.

Additional codes were added throughout the codification process. Existing codes were deleted and re-scoped, and changes were made to the hierarchical construct. Use of parallel coding was also applied, useful in identifying key themes appearing across multiple areas of discussion. These are all considered common practice [19].

In the interpretation of coded data, we started by reviewing all codes present across the range of transcripts. This allowed for the identification of code frequency, providing a view on commonality of approached adopted by each SP. Where a particular code was prevalent across a significant proportion of interviews, and was missing from few, we sought to better understand the reasoning behind this. As the "why" is not always considered [19], additional reviews of codes captured within the few, along with a secondary review of specific transcripts was conducted.