Assurance Techniques for Industrial Control Systems (ICS)

William Knowles, Jose M. Such, Antonios Gouglidis, Gaurav Misra, Awais Rashid
Security Lancaster
Infolab21, School of Computing and Communications
Lancaster University
Lancaster, LA1 4WA, United Kingdom
{w.knowles,j.such,a.gouglidis,g.misra,a.rashid}@lancaster.ac.uk

ABSTRACT

Assurance techniques generate evidence that allow us to make claims of assurance about security. For the purpose of certification to an assurance scheme, this evidence enables us to answer the question: are the implemented security controls consistent with organisational risk posture? This paper uses interviews with security practitioners to assess how ICS security assessments are conducted in practice, before introducing the five "PASIV" principles to ensure the safe use of assurance techniques. PASIV is then applied to three phases of the system development life cycle (development; procurement; operational), to determine when and when not, these assurance techniques can be used to generate evidence. Focusing then on the operational phase, this study assesses how assurances techniques generate evidence for the 35 security control families of ISO/IEC 27001:2013.

Categories and Subject Descriptors

K.6.5 [**Computing Milieux**]: Management of Computing and Information Systems—*Security and Protection*

General Terms

Security, Evaluation, Performance, Standards

Keywords

ICS, SCADA, Risk Management, Assurance Techniques

1. INTRODUCTION

Industrial Control System (ICS) security has seen a deluge of research activity over the past decade. Much work has been conducted in the field of risk management; in particular the development of new methodologies. However, minimal attention has been paid to the techniques used within these processes, which are used to generate evidence to make claims of assurance. This paper examines these "assurance techniques" within the context of ICSs.

Critical infrastructure such as that of utility industries (e.g., oil and gas) is a frequently cited example of an ICSs, although their usage is far more diverse and widespread. Service industries (e.g., logistics), and manufacturing industries (e.g., aerospace) make heavy use of ICS technologies. The technologies that support ICSs are largely similar in concept, and in many cases, identical. The technological similarity can be further expanded to small-scale installations, such as Building Automation Systems, although they are not addressed here.

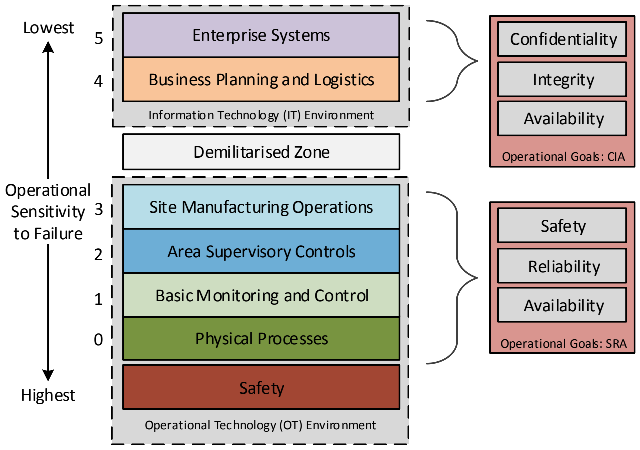

Lowest
5
4
Enterprise Systems
Business Planning and Logistics
Information Technology (IT) Environment
Confidentiality
Integrity
Availability
Operational Goals: CIA
Demilitarised Zone
Operational Sensitivity to Failure
3
2
1
0
Site Manufacturing Operations
Area Supervisory Controls
Basic Monitoring and Control
Physical Processes
Safety
Operational Technology (OT) Environment
Safety
Reliability
Availability
Operational Goals: SRA
Highest

Figure 1: A Conceptual Model of an ICS: Safety and Security Goals (Adapted from [3, 8])

At a conceptual level, an ICS can be seen as a series of layers, split into two areas (Figure 1). Layers 0-3 constitute the "Operational Technology (OT) environment". Present in layers 0-2 are safety systems, the sensors and actuators that monitor and manipulate physical processes, and the devices enforcing the intended logic of such processes. Multiple instances of layers 0-2 may exist, which may be geographically clustered or dispersed (e.g., a utility network may have many thousand "field sites"). In both cases, they have been conceptually labelled "Cell Zones". Layer 3 manages OT environment wide functions. Layer 3 systems capture and archive cell zone process data, monitor these processes, and take managerial action as necessary. Layers 4-5 are known as the "IT Environment" where enterprise functions are traditionally found. Centralised IT services are found here (e.g., business-to-customer services). Both the OT and IT environments may be physically isolated from each other, in what is known as an "air gap" which can act as a security feature. However, these networks in contemporary ICSs are frequently interconnected, due to the potential to facilitate core business functions (e.g., to enable automation in a manufacturing system, through linking the consumer purchasing system to the production line). The terms OT and ICS are frequently used synonymously; however, here ICS refers more holistically to all layers of the conceptual model to account for components and processes that span this boundary (often in both directions).

It is through the diversity in the operational requirements of ICSs that challenges in the appropriate and effective use of assurance techniques can be seen to emerge. Yet it is these techniques that allow us to generate claims of assurance about security. This paper addresses their application within ICSs, and makes the following key contributions:

1. Examining "how" security assessments are conducted within ICS environments and establishing guiding principles (PASIV) for safe and effective assurance technique use.
2. Assessing "when" assurance techniques can be used at different phases of the System Development Life Cycle (SDLC).
3. Assessing "where" these assurance techniques provide evidence of (non-)conformity about security control implementation within ISO/IEC 27001:2013.

Assurance techniques and related concepts are introduced in Section 2, along with existing literature in this domain. A methodology is outlined in Section 3. Section 4 then focuses on the use of assurance techniques within ICS environments. Section 4.1 examines current approaches to security assessments and derives five principles for using assurance techniques. Assurance technique use within three phases of the ICS SDLC are examined in Section 4.2, while Section 4.3 examines their contribution to ISO/IEC 27001:2013.

2. BACKGROUND AND RELATED WORK

Assurance techniques are merely activities with particular characteristics. The appropriate time of their use, their effectiveness, and the implications surrounding their outputs form part of the wider ecosystem of assurance. Previous work established terminology to describe the major concepts within this ecosystem [14]. Each component is described below, and their relationships collectively illustrated in Figure 2.

Assurance Scheme - This encompasses formal publications for organisations (e.g., standards) and individual qualifications, which establish a "level" of assurance that is to be met. For both, at least one assurance target is set. In some assurance schemes, there are explicitly defined assurance techniques that should be used to assess targets. For others, these are set and enforced through an external body (e.g., an accreditation body).

Assurance Target - An assurance target may be either a security control (e.g., asset management) or the competence requirements to assess such security controls (e.g., an individual must possess a certain qualification).

Assurance Technique - A method of assessing an assurance target. There are two types of assurance techniques. Those which assess security controls (e.g., penetration testing) and those that assess the competence requirements for using those assurance techniques (e.g., a multiple choice or lab-based exam). In some assurance schemes, the use of particular assurance techniques is explicitly defined.

Audit and Assessment Evidence - The use of an assurance technique to assess an assurance target generates audit or assessment evidence. Such evidence is used to assess conformity to an assurance scheme.

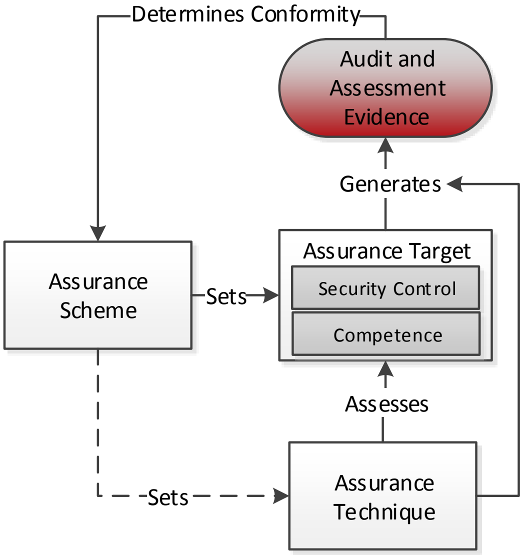


Figure 2: The Terminology of Assurance

All components of the ecosystem are not mandatory in the assurance process. An absence of an assurance scheme is a conspicuous example of where this may occur. Assurance techniques may assess the security controls of a product and generate assessment evidence, which is not used as audit evidence within an assurance scheme. Instead, this contributes to the "perception" of assurance and associated risk. An assurance scheme is then an established baseline for the level of perceived assurance. This paper, however, focuses on scenarios where all components are present, to understand how assurance techniques can be used within security evaluation criteria for future assurance schemes for ICS.

The extent of the implications of audit evidence (positive or negative) is dependent upon the assurance scheme. For example, in what is best seen as a spectrum, at one end, in some assurance schemes a "high risk" vulnerability discovered through penetration testing may be indicative of a major non-conformity. At the other end, this may not be the case. Instead, an holistic review of organisational risk posture is considered. ISO/IEC 27001 is an example of a risk-based assurance scheme, which in ISO terminology is termed a Management System Standard (MSS) [1]. A common misperception of such assurance schemes is that they establish strict requirements for security controls. However,

[1] ISO/IEC 27001 has been adapted for ICS environments in the energy sector through ISO/IEC 27019.

in practice system owners opt-in or opt-out of broadly defined security controls based on their chosen risk posture [2]. The security controls themselves are not mandatory; the clauses which mandate the supporting processes for making such decisions are. An auditor's role is not to dictate personal perceptions of what security should look like; it is to verify that the client has, amongst other requirements, clearly established processes for risk assessment (a process which itself may use assurance techniques as inputs), risk treatment (i.e., the modification of risk if required, for example, through implementing additional security controls), and risk acceptance (i.e., an informed decision to accept retained risk) in an ongoing fashion. A system owner will implement security controls based upon this process (reducing the broad category down to a specific type and extent of implementation). Audit evidence can then be used to verify that the processes are established and that the security controls that have been implemented are consistent with this risk posture. This is visualised in Figure 3.

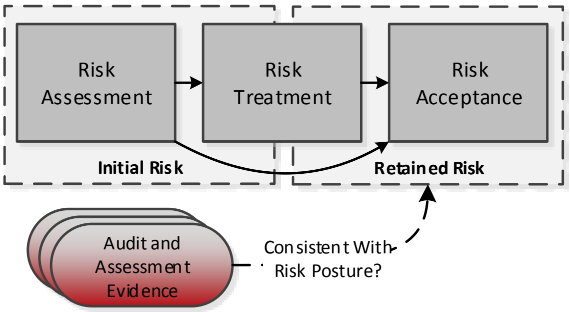


Figure 3: Audit Evidence Determines Conformity Based on Organisational Risk Posture

Such assurance schemes have the core feature of accounting for the particulars of organisational context when determining conformity. This has notable benefits for ICS environments. There exists industry-wide and system-specific operational challenges which create risk generating scenarios. For example, inadequate security considerations during product development may create insecure components, and depending upon ongoing vendor support, patches may not be available within reasonable time scales (or at all). Even with patch availability there remains the challenge of patch management for high-availability safety-critical systems. This approach to assurance schemes allows such risk inducing scenarios to occur, and does not deal a deadly blow to the certification of an organisation's efforts to provide assurance. However, it does this on one provision: a robust risk management process is in place to assess, treat, and accept risks. Therefore, although audit evidence generated by a particular assurance technique may indicate risk, an auditor can use other assurance techniques to verify that risk treatment has occurred, and that what remains, is consistent with the system owner's risk posture. In practice, such a risk treatment process may involve a defence-in-depth approach through the implementation of mitigating security controls. These controls may be technical (e.g., monitoring systems), non-technical (e.g., additional administrative controls for the use of vulnerable systems), or both (e.g., risk-based segmentation, such as with IEC-62443's Zones and Conduits model).

The dynamic of technical and non-technical security controls arguably mandates the use of technical and non-technical assurance techniques in their assessment. In practice, however, audits rely heavily on non-technical assurance techniques [14]. Multiple reasons for this exist. Notably, due to the process-focus of many assurance schemes, but also because it is unrealistic to expect auditors to also have the skill sets required for highly technical assurance techniques. What is reasonable, however, is the expectation for system owner or third party security assessments to contribute as audit evidence. A report by the British Standards Institution (BSI) [7] has highlighted the need for this to occur with greater frequency within security-based assurance schemes, and made recommendations for additional standardisation in the form of auditing guidelines for the use of simulated security assessments (e.g., penetration tests) as audit evidence. The intention being that such assurances techniques generate *demonstrable* audit evidence of whether security controls are consistent with risk posture.

Through the conceptualisation of the components of assurance, one can see how assurance techniques are a fundamental tool of the assurance process. Despite this, they have largely escaped the focus of existing research. A significant body of literature exists on assurance schemes, both within and outside ICS security; however, the focus has predominantly fallen on the operational challenges and benefits of using such schemes and not the assurance techniques contained (explicitly or implicitly).

Where existing literature exists on assurance techniques, the focus has largely fallen on their role within software assurance. In particular, assurance techniques and their use within the software development life cycle [2]), or in rare cases, their use within specific product-focused assurance schemes (e.g., the classification of assurance techniques for use within Common Criteria [6]). The predominant body of work in this area has been instigated by the National Institute of Standards and Technology (NIST) project, Software Assurance Metrics And Tool Evaluation (SAMATE)[3], which is sponsored by the U.S. Department of Homeland Security (DHS). An abundance of publications have been produced under this umbrella; notably around the topic of source code analysis, with a particular focus on static analysis[4]. A comprehensive review of existing *software* security assessment tools is presented in [18], focusing on when they can be used, their required skills, and their benefits and drawbacks.

To the authors' knowledge there is no existing academic literature examining the use of assurance techniques within ICS environments. There is, however, ad-hoc industry-led literature on specific assurance techniques. The UK Centre for the Protection of National Infrastructure (CPNI) have produced a procurement guide for ICS penetration testing [1]. One section of this report highlights high-level risks and potential mitigations. A more detailed report on the practical assessment was produced by CPNI in partnership with

[2] This is known as the Statement of Applicability (SoA).

[3] `http://samate.nist.gov/Main_Page.html`

[4] A list of SAMATE publications can be found at: `http://samate.nist.gov/index.php/SAMATE_Publications.html`

the U.S. DHS [17]. Engagement design is the core focus, and consideration, at a high-level, is provided on potential risks. At the time of submission, this report had just entered a period of review. A more detailed ICS assessment methodology is outlined in NESCOR [13], which categorises attack types by systems affected (but not at the level of assurance techniques) and the level of relative expertise required to assess each. In each publication, the risks of assessments are raised, but not discussed in depth, and no principles to underpin assurance technique use have been defined. Furthermore, such guidance is placed under the umbrella of "penetration test" or "security assessment", and there is no consideration of wider assurance technique use within the SDLC, or their contribution within assurance schemes.

3. METHODOLOGY

This study was conducted as a special use case within a wider project around the economics of assurance activities [14]. As part of this process, a period of desk research established the components of the assurance ecosystem, along with contextualising the fundamental role of 20 assurance techniques in IT systems. Assurance technique definitions can be found in Appendix A.

After the process mentioned above, a series of interviews was conducted to establish context on real-world security risk management practices of ICS operators (the framework in which assurance techniques provide value), and the approaches and challenges to conducting ICS security assessments. The latter is the focus of this paper, although the former influenced this study's design along with related literature in this domain (e.g., see Knowles et al. [8] for a recent survey). To maximise the contribution of interviews, four non-operator security practitioners were targeted. A benefit of this approach is that these are the individuals conducting security assessments within ICS environments in a consultancy (or quasi-consultancy) role. However, a secondary benefit is that these individuals have experience within a multitude of operator environments (one stakeholder stated this figure was over 100). Interview questions are outlined in Appendix B.

A grounded theory approach was utilised in the analysis of interview data. Approaches to current security assessments were analysed, and recurring themes in cautionary warnings and practices led to the derivation of a set of principles for conducting security assessments — i.e., "how" to conduct assurance techniques within ICS. The principles along with descriptions of practitioner experiences were then used to analyse "when" assurance techniques can be used within three phases of the SDLC. A separate analysis was then conducted for *operational systems* to determine "where" assurance techniques generate evidence within an assurance scheme (with respect to security controls). Both the choice of phases and assurance scheme were influenced by the risk management findings.

4. ASSURANCE TECHNIQUES FOR ICS

Understanding the potential opportunities for assurance technique use has significance, as it is through these techniques that the concept of risk is sculpted and opportunities for claims of assurance to be made. This section examines the current approaches for assessing ICS environments. A set of principles is presented based upon the findings of practitioner interviews. These principles are then applied to the assurance techniques defined within this study to examine their use within three phases of the ICS SDLC and their contribution as audit evidence within ISO/IEC 27001:2013.

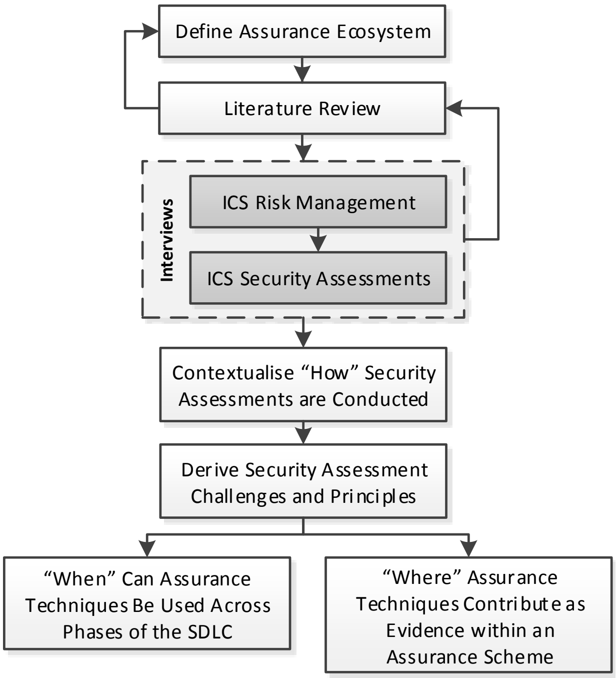

Define Assurance Ecosystem
Literature Review
Interviews
ICS Risk Management
ICS Security Assessments
Contextualise "How" Security Assessments are Conducted
Derive Security Assessment Challenges and Principles
"When" Can Assurance Techniques Be Used Across Phases of the SDLC
"Where" Assurance Techniques Contribute as Evidence within an Assurance Scheme

Figure 4: Study Methodology

4.1 Approaches to ICS Security Assessments

To what extent are ICS operators conducting security assessments? Results of a 2013 ENISA survey [5] show high variation: only ~15% are "always" testing, 30-35% "often" and 60% "sometimes". A 2014 SANS survey [12] has similar findings, but refers to how many operators use broad techniques, and does not quantify their frequency. Neither study considers non-response bias; therefore, caution should be taken in extrapolating results.

More interesting, perhaps, is *who* is conducting these security assessments when there is third party involvement. Practitioners interviewed within this study described heavy involvement of governments, primarily for critical infrastructure, which may come as no surprise; however, private sector involvement varied highly. For example, within the UK context, security assessments are predominantly government-led for critical infrastructure, either by CESG (the information security arm of GCHQ) or government departments (in some cases, facilitated with CESG involvement). Commercial assessments of ICSs in the UK were described as significantly less prominent than in other countries; notably the US. As the UK ICS security industry matures, commercial involvement may increase, as it has the secondary benefit of reducing the burden on government assessments. Indeed, the UK government has initiated schemes for such a reason in the past: notably "IT Health Checks"[5] for penetra-

[5] `http://www.cesg.gov.uk/servicecatalogue/service_`

tion tests of public sector systems. Furthermore, CREST[6], the leading UK body for penetration testing, is currently seeking to expand its STAR scheme, which provides threat intelligence-led red team exercises for critical infrastructure. Such reasoning may be applied to explain the extensive commercial sector involvement within the US, as one considers the logistical challenges of delivering security assessments across the US' extensive geographical scale.

Practitioners were asked about their experiences of what types of assurance techniques are used within ICS security assessments. The perception was that for security assessments of ICS environments, there was one of two approaches (Figure 5), which may be considered technical and non-technical (in relative terms, referring to their form of validation, rather than the individual competence of their users). Most widespread were security assessments that were in effect risk assessments that used the *non-technical* "big three" audit techniques: Review of Documented Policies, Procedures, and Processes; Observe; Interview. In-house *technical* security assessments were rare, as many ICS operators do not yet have appropriately trained individuals to conduct these tasks. Third party commercial (*technical*) security assessments, widely marketed as penetration tests, were increasing for the critical infrastructure sectors, but infrequent, and highly rare for non-critical environments. For IT networks, the frequency of security assessments was deemed to parallel those of non-ICS systems, although OT components within the IT network would often be out of scope. It was the general consensus of practitioners that current modes of assessing such environments were limited and greater effort should be placed on ensuring security controls are not only in place, but are effective in their objectives.

Practitioners felt the service model for commercial security assessments of OT environments was largely consistent: a fully white box engagement (i.e., full system awareness by the attacker) in collaboration with the ICS operator (e.g., to prevent operational impacts). In essence, the approach was one of a traditional security consultancy approach, rather than the scenario-based penetration testing model that they were marketed as. However, these services do contain a degree of the "penetration" element, but theorised rather than practically demonstrated. Commercial security assessment providers described methodologies for assessing the *operational* OT environments. Such assessments unsurprisingly shied away from the active and found passive alternatives to what would be conducted in a typical IT engagement. Highly cited assurance techniques included configuration reviews, architecture reviews (including passive network monitoring and mapping), physical inspections, and threat assessments. Supplementary test-bed assessments were sought to allow for greater active assessment, but few ICS operators were found to have this capability (either owned or shared with other operators), and many were not representative of operational networks. Other forms of simulated security assessments (e.g., red team exercises and social engineering audits) were not considered to be widely conducted, due to a limited appetite from procuring operators. However, practitioners believed their usage would increase as the security risk management practices of ICS operators mature.

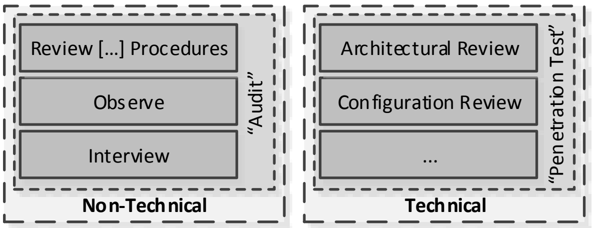


Figure 5: Two Approaches to Security Assessments

Third party involvement in the assessment of security during procurement was rare, although one practitioner stated its popularity is slowly increasing, and that they encourage ICS operators to include security testing clauses within their procurement contracts. For example, to state that if a device fails a security assessment, a discount is received, or there are other contractual requirements for patches within an established time frame.

For operational ICS environments, the lack of security assessments was suggested to lie with the lack of risk management processes or business requirement for such tests. A technical assessment would create a de-facto obligation to address issues found. Security assessments exist to push organisations to a higher level of security. Vulnerabilities in assessments of any infrastructure are frequently found; ICS are no exception, and arguably present greater opportunity for vulnerability (e.g., due to legacy equipment). A security assessment in effect is the purchasing of a problem. For operators that have invested heavily in security risk management there is a benefit of such an assessment; however, without the basic organisational competency for assessing and managing security risk, any issues found will be challenging to address, which may act as a deterrent. The dominance of the "audit-approach" was seen to encourage risk management behaviours.

A recurring theme in practitioner opinions was that the paradigm of ICS security assessments differs considerably from its IT counterpart. For some practitioners, the lack of a skilled workforce with an understanding of the peculiarities of assessing such environments posed a risk as security assessment providing organisations increasingly target the growing ICS security market. The fear being that the lack of domain-specific knowledge could lead to undesirable consequences for operators and potentially wider stakeholders.

Based upon the findings of practitioner interviews, five principles were derived for ICS security assessments of operational environments: PASIV. Here, PASIV is a homophone for *passive*, the guiding principle of assurance techniques use within ICS environments.

PROXIMITY requirements. Assurance techniques should be used when the assessor is in physical proximity to the system under evaluation. Remote assessment should be avoided, but if a scenario necessitates this, it should only conducted with alternative personnel present on-site.

assurance/IT-Health-Check/Pages/IT-Health-Check.aspx

[6] http://www.crest-approved.org/

Accessibility limitations. Assessments should consider to what extent claims of assurance can be made and addressed due to the wide accessibility limitations that restrict assurance technique usage (e.g., proprietary, closed source systems create little opportunities for the use of some assurance techniques).

Safety requirements. Ensuring that the use of an assurance technique does not negatively impact human and environmental safety should be the primary goal of an assessment.

Impact of the assurance technique. Assurance techniques should not impact the core operational goals of the operator, nor cause faults in live environments.

Value generated by using an assurance technique. A cost-benefit trade-off must be considered in assurance technique use and its implications for aiding the management of organisational risk (e.g., considering the extent to which a system under evaluation represents the wider system due to the infeasibility of testing many thousands of field sites).

4.2 Assurance Techniques and the ICS SDLC

To illustrate the limitations placed upon assurance technique usage within ICSs, the application of assurance techniques defined within this study to three phases of the SDLC is examined. The phases focus specifically on the role of assurance techniques in product assurance within ICS environments. Phases were selected based upon pressing sources of risk identified based on practitioner responses within the interviews: assurance technique use during product development; during procurement; once operational. These phases are defined below below:

Development During the supplier's development process, what assurance techniques can the *supplier themselves* use to ensure that a product has been designed in a secure manner? To illustrate the wider range of potential assurance techniques that can be used in this scenario, the focus is on applying assurance techniques within the product development process itself, rather than the wider organisational security that supports it. However, in practice, both are necessary to ensure resilient products (e.g., to mitigate against supply chain threats). The focus of this phase is at the component level (although communication capabilities fall under scope), and the broad process may culminate as a Factory Acceptance Test (FAT) [16].

Procurement When a product is being procured, what assurance techniques can the *procuring operator* use to gain assurances of a product's security? This phase is again focused on the component-level, and may form part of a pre-commissioning Site Acceptance Test (SAT) [16].

Operational Once a system is operational, what assurance techniques can be used in a security assessment? Operational is split into two parts: First, the assessment of products and the manner in which they are deployed within a representative testbed setting. This sub-phase considers the component and architectural levels. Second, a broader review of how assurance techniques can be used within live environments, while also considering an organisation's wider security processes and controls. This sub-phase considers the component, architectural, and human levels.

The assurance techniques defined within Appendix A were chosen based upon their relative frequency of use within IT environments, while trying to establish a consolidated collection that still covers the breadth of security assessment scenarios. Within the ICS security assessment paradigm, however, this frequency requires adjustment. Based upon the interviews, it was determined that two additional assurance techniques must be added: radio frequency analysis and hardware analysis. Both are defined below.

Radio Frequency Analysis - The assessment of the security of a communications channel that uses radio frequency bands as its transport medium. This may be passive (e.g., analysing captured traffic to discover modulation techniques) or active (e.g., replay attacks). This includes standardised implementations (e.g., 802.11 and 802.15), but also encompasses a wide variety of other technologies (e.g., licensed radio and microwave).

Hardware Analysis - The process of assessing security through hardware attack vectors, with or without powering the device, and using either passive mechanisms (e.g., reading data buses) or active mechanisms (e.g., modifying or replaying signals).

The application of assurance techniques to phases is described in Table 1. The mapping is based on a *typical scenario* for an ICS operator, and follows the principles of only mapping what is *feasible* and of *benefit* in such a case. Mapping uses three labels. "✓" indicates an assurance technique has widespread application, while "×" means it is unlikely for most cases. "P" indicates a possible application but is limited by certain factors, which are indicated by one of two suffixes. "(I)" when limited by concerns surrounding operational impact, and "(C)" when the application is case dependent (e.g., whether the operator has the resources to fund a testbed, or has bargaining power during procurement).

The mapping aids in illustrating the importance of a robust product development lifecycle as it at such a stage where there is greatest opportunity not only for remediating security faults, but also conducting in-depth assessments. Once operational the use of demonstrable assurance techniques, such as penetration testing, becomes limited and is marred by the PASIV principles imposed upon the process. Testbed assessment aids somewhat in addressing this, but as discussed, representative testbeds are a rarity.

One limitation of such a mapping is that it highlights only potential uses of assurance techniques, and the need for further review with respect to three factors. First, on *where* these assurance techniques are used. For example, as shown in Figure 1, operational sensitivity increases at lower layers of ICSs, and this mapping does not consider the opportunities for assessing ICS components that bridge the IT network boundary. Second, *how* they are used. The enforcement of PASIV principles requires assumptions not explicit in the mapping. A conspicuous example of this is for architecture review. Part of this process requires the mapping of current assets and communications channels. Active tech-

Assurance Technique	**Development**	**Procurement**	**Operational (Testbed)**	**Operational (Whole)**
Review of Documented Policies, Procedures, and Processes	P(C)	×	×	✓
Review of Client-Completed Self-Assessment Form	P(C)	P(C)	×	✓
Threat Assessment	×	×	P(C)	✓
Architectural Review	P(C)	×	✓	✓
Configuration Review	✓	×	✓	✓
Source Code Review	✓	×	×	×
Observe	P(C)	×	×	✓
Interview	P(C)	P(C)	×	✓
Red Team Exercise	×	×	×	P(IC)
Penetration Testing	✓	P(C)	✓	P(IC)
Vulnerability Scan	✓	P(C)	✓	P(IC)
Social Engineering	×	×	×	✓
Static Analysis	✓	×	×	×
Dynamic Analysis	✓	×	×	×
Fuzzing	✓	P(C)	✓	P(IC)
Formal Verification	✓	×	×	×
Cryptographic Validation	✓	P(C)	✓	P(IC)
Emanation Security Analysis	P(C)	×	×	×
Witnessed Test	P(C)	P(C)	✓	✓
Public Review	×	×	×	×
Radio Frequency Analysis	✓	P(C)	✓	P(IC)
Hardware Analysis	✓	P(C)	✓	P(IC)

Table 1: The Feasibility of Using Assurance Techniques for Three ICS Lifecycle Phases

niques that may be used in IT environments to facilitate this such as port scanning can not be used. In OT environments this mapping involves alternative approaches such as passive traffic analysis, which is supported by other assurance techniques (e.g., physical inspection, which is defined here as "Observe"). Third, on how effective these assurance techniques are. Perceptions of effectiveness can be assessed independently, but effectiveness is also related to the particular security control being assessed. Establishing this relationship is also a requirement to understand how particular assurance techniques might be used to generate demonstrable claims of assurance within schemes.

4.3 Assurance Techniques and the Security Controls of ISO/IEC 27001:2013

Assurance schemes exist for multiple phases of the SDLC. However, it is those targeting operational systems that are the focus of the majority, as it is at such a stage where there is the greatest demand for evidence that security risk is being managed, and therefore, it is the operational phase that will be the continued focus of this paper. In order to make a claim of assurance, understanding which assurance techniques can be used at this stage needs to be supplemented by an understanding of which security controls they relate to, as not all assurance techniques are equal in this regard. Furthermore, this will aid in the understanding of which assurance techniques can potentially provide supplementary evidence, or act as substitute evidence (e.g., when there is a restriction on assurance technique use due to PASIV).

Some assurance schemes clearly dictate the assurance technique to be used to assess the processes and security controls it mandates. In some assurance schemes, this requirement is highly specific (e.g., PCI DSS's security evaluation criteria [11] is a notable example, although of unlikely relevance to ICS security); in other schemes a general direction towards a particular assurance technique is established (e.g., NERC CIP-007-3 R8 for "Cyber Vulnerability Assessment" [9] which precedent has established as, in large, a vulnerability scan). However, there are many other assurance schemes in which the choice of assurance technique is intentionally not mandated, unclear, or ambiguous.

A mapping of assurance techniques to the high-level security families of ISO/IEC 27001:2013 has been produced. It is believed that such a mapping will aid in the development of an holistic compliance evaluation criteria for the security controls outlined in future assurance schemes. As such, this mapping may be of potential use to a wide variety of stakeholders. First, to international bodies developing standards in this space (e.g., ISO/IEC JTC1/SC27), such as those for MSS. Second, to private/consortia bodies that contribute to the development of assurance schemes (e.g., technical bodies for penetration testing). Third, for clients and third parties in designing and assessment and audit programmes.

The choice of ISO/IEC 27001:2013 was driven by the findings of industry surveys, along with the experiences of ICS operator practices by the interviewed practitioners. Industry surveys such as that of ENISA [4] (EU-centric) and SANS [12] (US-centric) have both highlighted that for standards where conformity can be assessed (i.e., rather than guidelines), ISO/IEC 27001 has popularity beyond or on-

Security Clauses	Security Categories	Review of Documented Policies, Procedures, and Processes	Review of Client-Completed Self-Assessment Form	Threat Assessment	Architectural Review	Configuration Review	Source Code Review	Observe	Interview	Red Team Exercise	Penetration Testing	Vulnerability Scan	Social Engineering	Static Analysis	Dynamic Analysis	Fuzzing	Formal Verification	Cryptographic Validation	Emanation Security Analysis	Witnessed Test	Public Review	Radio Frequency Analysis	Hardware Analysis
A.5 Information Security Policies	A.5.1 Management Direction for Information Security	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.6 Organisation of Information Security	A.6.1 Internal Organisation	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.6.2 Mobile Devices and Teleworking	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	✓	✓
A.7 Human Resource Security	A.7.1 Prior to Employment	✓	✓	×	×	×	×	✓	✓	✓	×	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.7.2 During Employment	✓	✓	×	×	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.7.3 Termination and Change of Employment	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.8 Asset Management	A.8.1 Responsibility for Assets	✓	✓	✓	✓	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.8.2 Information Classification	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.8.3 Media Handling	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
A.9 Access Control	A.9.1 Business Requirement of Access Control	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓	×	✓	×
	A.9.2 User Access Management	✓	✓	×	×	×	✓	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	✓	×
	A.9.3 User Responsibilities	✓	✓	×	×	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.9.4 System and Application Access Control	✓	✓	×	×	✓	✓	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	✓	×
A.10 Cryptography	A.10.1 Cryptographic Controls	✓	✓	✓	×	✓	×	✓	✓	✓	✓	×	×	×	×	×	×	✓	×	✓	×	✓	✓
A.11 Physical and Environmental Security	A.11.1 Secure Areas	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.11.2 Equipment	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	✓
A.12 Operations Security	A.12.1 Operational Procedures and Responsibilities	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	✓	×
	A.12.2 Protection from Malware	✓	✓	×	×	✓	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.12.3 Backup	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.12.4 Logging and Monitoring	✓	✓	×	×	✓	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.12.5 Control of Operational Software	✓	✓	×	×	✓	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	✓	×	×	×
	A.12.6 Technical Vulnerability Management	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	A.12.7 Information Systems Audit Considerations	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.13 Communications Security	A.13.1 Network Security Management	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	×	✓	×
	A.13.2 Information Transfer	✓	✓	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	✓	✓	✓	×	✓	×
A.14 System Acquisition, Development, and Maintenance	A.14.1 Security Requirement of Information Systems	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	×	✓	×
	A.14.2 Security in Development and Support Processes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	A.14.3 Test Data	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.15 Supplier Relationships	A.15.1 Information Security in Supplier Relationships	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.15.2 Supplier Service Delivery Management	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.16 Information Security Incident Management	A.16.1 Management of Information Security Incidents and Improvements	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.17 Information Security Aspects of Business Continuity Management	A.17.1 Information Security Continuity	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
	A.17.2 Redundancies	✓	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×	×
A.18 Compliance	A.18.1 Compliance with Legal and Contractual Requirements	✓	✓	✓	×	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	✓	×	✓	×	×	×
	A.18.2 Information Security Reviews	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2: Assurance Techniques and ISO/IEC 27001:2013 Security Control Families

part with ICS-specific standards such as ISA/IEC 62443 and NERC CIP. For the purposes of this study, NERC CIP was considered too US-centric, and ISA/IEC 62443, while considered a future de facto ICS standard, is in its current form perceived by practitioners as "drafty" which deters adoption[7]. ISO/IEC 27001:2013 in contrast, likely owes its popularity to its maturity and widespread adoption for IT systems in general, and while some criticisms may be attributed to its application within ICSs, these have been diminished to some extent by the development of ISO/IEC TR 27019:2013. This standard provides guidelines on how ISO/IEC 27001:2013 should be adapted to suit the requirements of ICS environments (specifically those of energy utilities). The current popularity of ISO/IEC 27001:2013 was therefore a key contributor to the choice of assurance scheme for this mapping; however, two further factors were also considered: First, ISO/IEC 27001 standards are widely used as a framework on which to build other standards. This may be a strict mapping (e.g., as with the CESG Assured Service Telecoms CAS(T) standard within the UK[8]), or an informal or advisory one (e.g., Appendix H of the NIST 800-53 guidelines [10] provides a mapping of ISO/IEC 27001 to NIST 800-53, and then from NIST 800-53 to ISO/IEC 15408); Second, ISO/IEC 27001:2013 was deemed to be of interest to the wider cyber-physical system audience, beyond ICS.

Table 2 outlines the mapping between 22 assurance techniques and the 35 ISO/IEC 27001 control families (outlined in the standard's Annex A and in more detail within ISO/IEC 27002:2013). Observant readers may note that ISO/IEC 27001:2013 is an assurance scheme for operational systems, yet the assurance techniques included within Table 2 go beyond those outlined as being capable of use for operational ICS systems in Section 4.2. A design decision was made to conduct a more expansive analysis, because while these restrictions may apply for ICSs, they may not apply for other cyber-physical systems.

Assurance techniques within ISO/IEC 27001 broadly fall into two categories: First, those used by a client (i.e., the auditee) or procured (i.e., from a third party) which generate audit evidence. Second, those used by an auditor. In some cases, assurance techniques may bridge the two categories (e.g., for internal audits). It is important to clarify for the reader, that in standards such as ISO/IEC 27001, auditors are free to use any assurance technique they deem adequate for assessing an assurance scheme's requirement, although exceptions to this occur in other schemes, where particular requirements mandate certain assurance techniques be used in their assessments.

The following mapping is not intended to dictate assurance technique usage in either category. Instead, it is intended to provide guidelines on the most appropriate assurance techniques for particular security controls, with the intention of facilitating the design of security evaluation criteria for future assurance schemes. To provide a robust framework for this analysis, a set of principles was defined.

Core Principle: An assurance technique contributes directly to an audit and is conducted by the auditor, or the assurance technique is used by the auditee or a third-party to generate audit evidence. Sub-principles:

1. Where possible, assurance technique usage is pragmatic (i.e., they provide a valid contribution, or can be seen to provide one in the design of future assurance schemes, while ignoring "potential" or "abstract" inclusions).

2. An assurance technique may provide audit evidence while not being a direct assessment of a security control. An example is a threat assessment. This may include the definition of organisational requirements and identification of assets, which can contribute to control families such as "A.6.1 Internal Organisation".

3. Relationships between the assurance techniques of Appendix A were defined in Such et al. [14]. If an assurance technique is set which has "optional contributing" assurance techniques, it does not mean they also must be enabled in this mapping, and vice versa. An example is penetration testing, where multiple sub-techniques can contribute, and may or may not be used depending on the assessor.

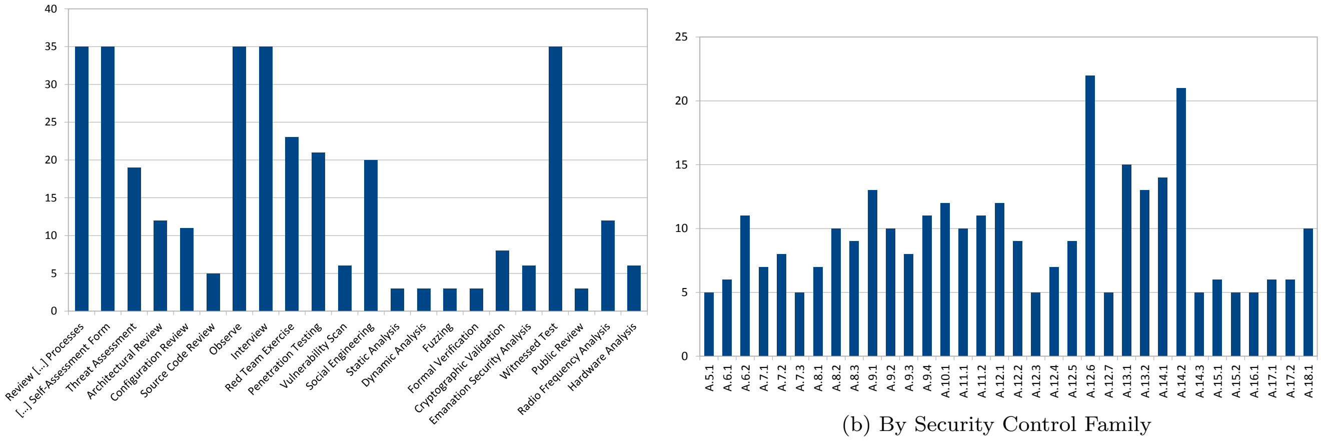
4. Assurance techniques are associated with control families, based upon their potential to assess that control family. A more granular level of effectiveness exists beyond this; the mapping does not dictate that two assurance techniques are equally effective for assessing that control family.

A review of the frequency of assurance techniques within each security control family was conducted. Figure 6a and Figure 6b illustrate the results of this review. A clear trend can be seen in Figure 6b of 5-12 assurance techniques per security control family. A qualitative review of these assurance techniques highlighted the dominance of the "big three" audit techniques (Review of Documented Policies, Procedures, and Processes; Observe; Interview). Their adaptability is more clearly visualised within Figure 6a. This, however, is not surprising given that ISO/IEC 27001 is used to enforce an ISMS, where processes have historically reigned over the specifics of security controls. Furthermore, the two techniques appearing with equal frequency are closely related to the audit process. Witnessed tests are widely used for third party validation within audits, and Reviews of Self-Assessment Forms are increasingly being used as an audit-"lite" technique when a full audit is not viable (more widely, in particular for assurance schemes that provide a form of entry-level certification such as with Cyber Essentials [15]).

For the security control families where assurance techniques appear with higher frequency, we begin to see greater use of assurance techniques where an element of user behaviour is considered in the security controls contained. For example, Social Engineering appears frequently here, along with meta-techniques that rely on it heavily, such as Red Team Exercises. Security control families where there are technical

[7] Certification schemes such as ISASecure (`www.isasecure.org`) exist; however, they have so far been limited to products and the product development life cycle, rather than operational systems.

[8] `https://www.cesg.gov.uk/servicecatalogue/service_assurance/CAS/Pages/CAS.aspx`



(a) By Assurance Technique

(b) By Security Control Family

Figure 6: Frequency of Assurance Techniques Within ISO/IEC 27001:2013 Security Control Families

controls are a minority within ISO/IEC 27001:2013. However, where such security controls exist, there is as would be expected, a large number of assurance techniques that could potentially be used in their assessment. In practice, however, the constraints of real-world environments may restrict the use of some of these (e.g., due to the limitations imposed by PASIV).

5. CONCLUSIONS

This paper establishes assurance techniques as the fundamental tool of the security risk management process, and the mechanism by which assurance is measured. The use of assurance techniques within the context of ICS environments was the subsequent focus of the paper. A series of interviews was conducted with ICS security practitioners which culminated in three key contributions.

First, the contextualisation of “how” assurance techniques are used within real-world ICS security assessment including the approaches taken by governments and commercial security assessment providers. Findings of practitioner interviews were used to derive the PASIV principles for the safe use of assurance techniques within ICS engagements.

Second, an analysis was conducted to determine “when” assurance techniques may be used within three phases of the SDLC. This highlighted the restriction on the types of assurance techniques that can be used once a system is operational, and that the greatest opportunity for diversified approaches to assessing security were found during the development process. Such findings have two implications. First, it establishes the importance of strong security risk management to make a business case for security during procurement to encourage vendor improvement. Second, that the call for greater validation of the efficacy of implemented security controls is hindered by the operational challenges of assurance technique use. It does, however, provide a preliminary step in identifying what assurance techniques may apply within particular assurance schemes for different phases of the SDLC.

Third, it provides the first step towards overcoming the criticism of many assurance schemes: that there is inadequate technical validation of the implemented security controls [7]. This paper does this by promoting an holistic approach to the design of security evaluation criteria, by mapping the 22 assurance techniques outlined here to the 35 security control families of ISO/IEC 27001:2013. As such, it answers the question of “where” assurance techniques can generate evidence of conformity within assurance schemes.

One limitation of this work is that the opportunity to use an assurance technique says nothing of its effectiveness. The authors have addressed this within a separate publication [14] which outlines the findings of a survey of over 100 security practitioners on their perceptions of the attributes of the assurance techniques listed within Appendix A. This work, however, is for IT systems in general, rather than ICS specifically, and based on this study’s findings of the challenges of applying assurance techniques in ICS environments, this will be addressed as future work. Furthermore, as outlined in Section 2, individual competence has a integral role in assurance ecosystem, and therefore contributes to the measure of effectiveness. Future work will also consider assurance techniques that assess the competencies of individuals for conducting ICS security assessments.

6. REFERENCES

[1] CPNI. Commercially Available Penetration Testing: Best Practice Guide. Technical report, 2006.

[2] N. Davis. Secure Software Development Life Cycle Processes. Technical report, Software Engineering Institute, 2013.

[3] P. Didier. *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*. Cisco Systems and Rockwell Automation, 2011.

[4] ENISA. Protecting Industrial Control Systems: Annex II. Survey and Interview Analysis. Technical report, 2011.

[5] European Network and Information Security Agency (ENISA). Survey and interview analysis. For the Report :Good practices for an EU ICS testingcoordination capability. Technical report, 2013.

[6] D. Jackson and D. Cooper. Where do Software Security Assurance Tools Add Value. In *Workshop on*

Software Security Assurance Tools, Techniques, and Metrics. SSATTM05, pages 14–21, 2005.

[7] W. Knowles, A. Baron, and T. McGarr. Analysis and recommendations for standardization in penetration testing and vulnerability assessment: Penetration testing market survey. Technical report, British Standards Institution (BSI), 2015.

[8] W. Knowles, D. Prince, D. Hutchison, J. Pagna Disso, and K. Jones. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9:52–80, 2015.

[9] NERC. Standard CIP-007-3 - Cyber Security - Systems Security Management. Technical report, 2013.

[10] NIST. Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, 2013.

[11] PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures (Version 3.0). Technical report, 2013.

[12] SANS. Breaches on the Rise in Control Systems: A SANS Survey. Technical report, 2014.

[13] J. Searle. NESCOR Guide to Penetration Testing for Electric Utilities. Technical report.

[14] J. Such, A. Gouglidis, W. Knowles, G. Misra, and A. Rashid. The Economics of Assurance Activities. Technical Report SCC-2015-03, Security Lancaster, Lancaster University, 2015.

[15] UK HM Government. Cyber Essentials Scheme: Summary. Technical report, 2014.

[16] U.S. Department of Homeland Security. Cyber Security Procurement Language for Control Systems. Technical Report September, 2009.

[17] U.S. Department of Homeland Security. Cyber Security Assessments of Industrial Control Systems. Technical Report April, 2011.

[18] D. Washington Navy Yard and B. A. Hamilton. Software security assessment tools review. *Mar*, 2:145, 2009.

APPENDIX

A. ASSURANCE TECHNIQUES

The following subsections outlines 20 high-level assurance techniques organised in 5 categories that were defined within [14]. A further category outlines assurance techniques for assessing individual competencies, but was omitted here.

A.1 Review

Review of Documented Policies, Procedures, and Processes - The process of analysing the documented specifications (e.g., procedures and security properties) and processes (e.g., managerial) for a component or system under assessment.

Review of Client-Completed Self-Assessment Form - An analysis of a client submitted review of their implementation of assurance targets as set out within an assurance scheme. Self-assessment forms typically consist of a multitude of questions that a client must answer is multiple choice or narrative form.

Threat Assessment - A multi-stage process used to identify and rank the threats to computer software, a component, or IT system. Threat analysis builds upon the analysis of sub-processes such as asset identification and architectural reviews against a security policy.

Architectural Review - An analysis of the components (type, quantity, configuration, etc.) and their relationships within a piece of software, component, or system to determine if their implementation meets a desired security policy.

Configuration Review - A review of the way a system or its software has been configured to see if this leads to known vulnerabilities. Configuration reviews can be passive (e.g., manually checking software versions for known vulnerabilities) or active (e.g., automated build review scanners).

Source Code Review - The examination of source code to discover faults that were introduced during the software development process. Source code reviews are predominantly manual; however, they may be supplemented with automated techniques (e.g., using static analysis tools).

A.2 Observe

Observe - The process of watching a live, operational system to identify real-world deviations from documented assurance targets.

A.3 Interview

Interview - The process of questioning one or more individuals about security-related matters within the organisation being assessed through any medium (e.g., in person or virtually).

A.4 Test

Red Team Exercise - A simulated attack on a system that is given more freedom than is available during a penetration test, in order to more realistically simulate a real-world malicious attacker. This freedom is given in terms of the engagement's duration (e.g., often months in duration), available human resources (e.g., large teams built around individuals with different specialisms), allowed use of tools (e.g., a heavy use of social engineering is common), and restriction of defender knowledge to test their day-to-day responses to cyber threats.

Penetration Test - A simulated attack on a component or system using similar techniques to that of a real-world malicious attacker. A penetration test may build upon a vulnerability assessment; however, it differs in having an implicit or explicit goal that the assessment attempts to realise (e.g., compromise sensitive data or obtain a certain level of network access). Typically this requires vulnerabilities to be exploited, which would not be undertaken within a vulnerability assessment.

Vulnerability Scan - The process of using an automated scanner on a web application or network to identify vulnerabilities. Discovered vulnerabilities are not exploited.

Social Engineering - An attempt to manipulate one or more human users into performing an action that does not conform to operational procedures. This can be conducted in a manner that is goal-based (e.g., access data) or audit-based (e.g., the percentage of a department vulnerable to a spear phishing attack).

Static Analysis - Without executing computer software, static analysis attempts to debug and identify potential software vulnerabilities through an analysis of its source code. Static analyses are predominantly automated; however, they may contain some elements of manual interaction (e.g., in order to understand the context and implications of the results). Human-led analyses fall under source code review.

Dynamic Analysis - Once computer software has been executed, this technique attempts to debug and identify potential software vulnerabilities through active methods (e.g., inputting unexpected data through fuzzing) and passive methods (e.g., memory analysis).

Fuzzing - The process of injecting erroneous and unexpected data into an input field in order to trigger faults (e.g., crashes and exceptions) that could be leveraged to discover software vulnerabilities. Fuzzing may be dumb (i.e., random) or intelligent (i.e., with a knowledge of the protocol being tested).

Formal Verification - The use of mathematical techniques for assessing functional properties of information and communication systems.

Cryptographic Validation - A method used to analyse a cryptographic algorithm and/or its implementation within a component or system (e.g., entropy testing).

Emanation Security Analysis - One or more methods used to assess device emanations (e.g., electromagnetic or sound emanations) for the unintentional leakage and disclosure of information.

A.5 Independent Validation

Independent validation occurs when a third party is used to verify the assessment methodology of an assurance technique, or otherwise validate the results of its assessment of assurance targets.

Witnessed Test - The use of an independent witness to provide a second level of verification that the results of an assurance technique are as described.

Public Review - The process of opening a technology, component, or system to wider review by the public. Public reviews may be of documents (e.g., drafts of future cryptographic algorithms) or live systems (e.g., bug bounties).

B. INTERVIEW STRUCTURE

1. Risk management and standards:
   (a) Do OT environments have clear strategies when it comes to assessing and treating risk relating to security? Are public methodologies used? Robust processes?
   (b) How does this differ to the IT network?
   (c) How is risk assessed at the boundaries between these two networks (e.g., responsibilities for systems that lie in other aspects of the network, such as OT systems in the IT network)?
   (d) Is there a clear strategy for linking safety and security requirements in the OT environment?
   (e) Are you seeing standards being used in these environments (at both the OT/IT levels)? As cursory references, guidelines or for certification?
   (f) Are ICS operators enforcing security requirements on their supply chain?
   (g) (General then specific) What about in terms of: (a) contractors working in these environments?; (b) the products they procure (e.g., ensuring they've had security assessments - basic or with more advanced schemes such as with the Common Criteria or ISASecure).
   (h) Do operators embed security and safety requirements into the full lifecycle of their ICS system?
2. Risk perception:
   (a) How do organisational cultures differ between OT and IT networks when it comes to security?
   (b) Challenges created for securing these systems?
   (c) Organisational support for security management (e.g., from board level)?
   (d) How is security risk communicated in these organisations?
   (e) Is the security community communicating ICS risks effectively to those that matter (e.g., to those at board level)? How?
3. Security assessment:
   (a) To what extent is the government's involvement in ICS assessments? Extent of private sector assessment?
   (b) What assurance techniques are involved in the assessment of an OT and IT environment? Reasons for choices? Holistic or fragmented? Usage considerations? Logical, social (e.g., social engineering), and physical assessments (e.g., physical pentests)?
   (c) In your experience, how well are the boundaries defined defined between the OT and IT network?
   (d) Do you think the current methods of assessment are enough to prove that controls are robust enough to mitigate against most cyber threats? Clarify if necessary: lack of evidence of attacks is not evidence of good security posture.
   (e) What metrics are used during assessments?
4. The future of ICS security:
   (a) How can the state of ICS security be improved going forward (e.g., standards, regulations, cultural shifts)?