Achieving ICS Resilience and Security through Granular Data Flow Management

Benjamin Green
Security Lancaster Research Centre
Lancaster University
Lancaster, United Kingdom
b.green2@lancaster.ac.uk

Marina Krotofil
Honeywell Industrial Cyber Security Lab
Atlanta (GA), USA
marina.krotofil@honeywell.com

David Hutchison
School of Computing and Communications
Lancaster University
Lancaster, United Kingdom
d.hutchison@lancaster.ac.uk

ABSTRACT

Modern Industrial Control Systems (ICS) rely on enterprise to plant floor connectivity. Where the size, diversity, and therefore complexity of ICS increase, operational requirements, goals, and challenges defined by users across various sub-systems follow. Recent trends in Information Technology (IT) and Operational Technology (OT) convergence may cause operators to lose a comprehensive understanding of end-to-end data flow requirements. This presents a risk to system security and resilience. Sensors were once solely applied for operational process use, but now act as inputs supporting a diverse set of organisational requirements. If these are not fully understood, incomplete risk assessment, and inappropriate implementation of security controls could occur. In search of a solution, operators may turn to standards and guidelines. This paper reviews popular standards and guidelines, prior to the presentation of a case study and conceptual tool, highlighting the importance of data flows, critical data processing points, and system-to-user relationships. The proposed approach forms a basis for risk assessment and security control implementation, aiding the evolution of ICS security and resilience.

Keywords

Industrial Control Systems; SCADA; Data Flow; Security; Resilience; Risk Assessment; Socio-Technical Systems

1. INTRODUCTION

Industrial Control Systems (ICS) are used across a variety of sectors, for the operation of industrial processes. These include electricity generation and distribution, water treatment and distribution, manufacturing, etc. – some of which are considered to be critical national infrastructures [10] due to the impact of their operations on societies' well-being.

Over recent years the industrial sector has seen a significant rise in the number of disclosed ICS vulnerabilities [23]. While this increase in technically focused research has its benefits, challenges still remain not only in how best to convey the importance of security to those in industry, but how best to understand operational objectives across multiple system levels/business areas, and ensuring any form of security implementation does not degrade usability or create a cascading effect, that adversely impacts local or business wide operational objectives.

In process industries such as oil, gas, and chemicals, the ability to identify shifts in patterns that could eventually cause undesirable output is vital. Of particular concern are critical data processing points, which if changed have the potential to impact processes operations, remaining undetected beyond the point of safe recovery. In [36], Weiss provides an example of how a seemingly insignificant change of sensor signal filtering parameters resulted in significant damage of equipment at a nuclear power plant.

Control systems used to be pneumatic in nature, prior to the transition towards electronic alternatives, and ultimately computer-integrated manufacturing (CIM) concepts of the 1970s, where data and information became the most essential ingredients in automation, with the key to handling data and information established as a transparent information flow inside an automation system. A challenge then arose in finding an automation architecture capable of integrating all levels and functional units of an enterprise, starting from strategic planning down to the process floor. To cope with the anticipated complexity, a strict subdivision of the data processing into a hierarchical model was devised that became known as the automation pyramid [30].

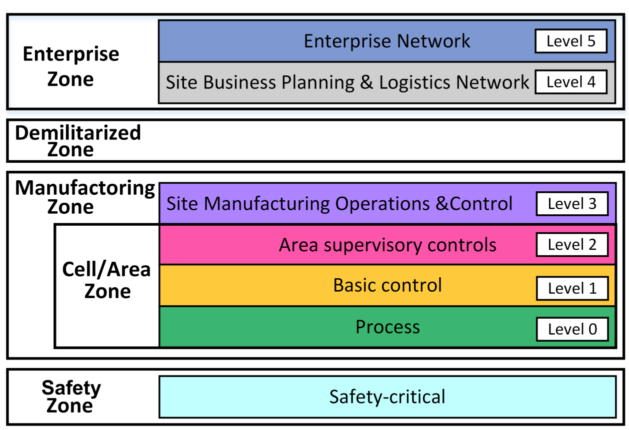

Figure 1: The Purdue Model [16]

CPS-SPC'16, October 28 2016, Vienna, Austria

ISBN 978-1-4503-4568-2/16/10. . . $15.00

DOI: http://dx.doi.org/10.1145/2994487.2994498

Fig. 1 depicts the automation pyramid, also referred to as the Purdue model. Discussed in [16], the Purdue model is seen as a simple way of compartmentalising ICS functionality into hierarchical layers. In accompaniment to Fig. 1, [16] provides additional summarisation of each system level, including example devices and their function. Allocation of devices to automation levels also highlights varying time constraints associated with data collection and response, contextualising the importance of device functions. Simply put, when discussing devices residing in the lower levels of an ICS, such as sensors, actuators, Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), etc. communications must take place on a scale of seconds, in some cases milliseconds. However, devices residing in mid to higher levels, such as data historians, human machine interfaces, Information Technology (IT) workstations, etc. may only be required to communicate on a scale of minutes to hours, in some cases days and weeks.

Whereas Operation Technology (OT) disciplines support physical value creation throughout an operational process, IT combines all necessary technologies for data and information processing, transmission, and storage. The boundary between these two distinct zones of ICS generally resides across levels three and four of the Purdue model. Since CIM conception, most industries have developed and managed OT and IT independently, as isolated domains. However, over recent years, OT has started to progressively adopt IT-like technologies [7]. A prerequisite to achieving these benefits is that strategic, organisational, and technological challenges are mastered. Implementing what some call IT/OT convergence (i.e. the end-to-end management of IT and OT), implies that IT and OT strategies are harmonized, common governance and process models are installed, security and data are managed centrally, and human resources are re-skilled to understand the distinct requirements of both disciplines.

While existing works have explored the challenges of IT/OT convergence, social and technical factors are often discussed in isolation, or in theoretical terms. Social factors relate to individuals skill sets, behaviours, goals, challenges, requirements, etc. Technical factors related to the adoption of IT technologies within the OT domain, increased complexity/diversity of devices, increased functionality and interactions across multiple system levels, etc. When combined, the requirement for increasing technical complexity and functionality can be understood, accounting for individuals' requirements in order to meet set objectives across each system level. However, detailed discussion of combined social and technical factors requires empirical data sets, and a comprehensive analysis, allowing for a clear interpretation of observed joint challenges. This paper presents the results of an empirical study, used to better understand technical data flows and processing points within an ICS, whilst also highlighting the complexity and crossover of human (social) factors.

Security standards and guidelines provide a resource by which practical steps can be taken to improve security and resilience; however, advice on understanding a system prior to risk assessment and control implementation is limited. Together with the challenges identified above, we therefore see the need for a tool that will aid the discovery of a systems attack surface. This includes identification of data flows and processing points, and highlighting of not only system-to-system, but system-to-user relationships. Obtaining clear visibility of data pathways is not a simple task. Where data from multiple sources may be processed and combined, prior to further transmission as new inputs to additional devices, complexity in the level of system-to-user interaction is increased, with a plethora of individual requirements, challenges, and goals.

The remainder of this paper is structured as follows. Section 2 introduces objectives, requirements, and challenges when managing data flows in ICS. Section 3 conducts a review of popular standards and guidelines used for risk assessment and selection of security controls. Section 4 introduces a case study and conceptual tool to better understand system-to-system and system-to-user relationships, prior to conclusions and future work in Section 5.

2. DATA FLOWS IN ICS

In many cases the controller and operator can observe the physical process only through sensor readings, and must have faith that the process data describes the true underlying situation. Processed in a variety of ways, sensor signals pass though a variety of functions such as amplification, scaling, conversion, filtering, aggregation and normalisation to name a few. Furthermore, data sources are combined through computation formulas prior to additional controller and application consumption. In essence, data processing is conducted to provide usable/actionable information, based on the requirements defined by data consuming circuits/devices/applications at each stage in a data chain. Any error in data processing along a pathway harbours the potential to degrade and even lose visibility of the process state. Understanding data sources and pathways is essential to the comprehension of undesirable impact on process operations, caused by errors or intentional manipulation of data streams.

2.1 Data Reliability

OT engineers are responsible for data content. Data must be collected from appropriate sources within the operational process, conforming to any defined time constraints. As OT has evolved, these requirements on data collection have seen a significant shift. Thus, individual sensor inputs are no longer solely used for local operational process decision making on the plant floor. For example, in the UK, regulators such as the Department for Environment, Food & Rural Affairs (DEFRA) require data which identifies an organisation's conformity to predetermined operational restrictions, quality and quantity of final effluent, for example [15]. These underlying regulations drive operational requirements. However, this same data may also be used for performance analysis, and subsequently decision makers at board level, to determine the financial viability of operational sites/zones, and for identification of required investment to streamline processes. Furthermore, it may also be applied to the remote alarm monitoring/management of unmanned operational processes. In some cases, this remote monitoring and management may form part of an organisational safety reporting processes. Without a clear understanding of deviations to original requirements for data collection, the application of system changes, let alone risk assessment and security control implementation, presents a significant challenge.

When instrumentation engineers recalibrate or replace a sensor, they will likely know to liaise with a PLC configuration engineer, in order to account for the applied changes within the PLC logic, therefore maintaining stable physical process operations. This fulfils the initial requirement of sensors, that of providing accurate input to operational decision making. However, when re-configuration requirements arise in relation to neighbouring devices, RTUs and Data Historians for example, if these are left unchanged, regulatory, alarm monitoring, safety, and performance analytics data may become compromised. In the given example, awareness of sensor data consumption beyond the PLC could fall outside the scope of an instrumentation engineer's role. It is for this reason that identification of complex system-to-system (device to device interactions) and system-to-user relationships (end user and maintenance personnel interactions with systems) and requirements, within the manufacturing zone (Fig. 1), demonstrate the reality of OT challenges, formed around the continuing deployment and development of new and/or existing OT technology, in parallel to the growing number of data users across all levels of ICS.

2.2 Data Integrity

Most attacks directed at operational processes (excluding espionage) will seek to tamper with process data and information flows. This is often assumed to involve a process by which the attacker infiltrates a communications link, then using replay, packet injection, or direction manipulation of payloads, achieves an undesirable change. Application of network monitoring and intrusion detection techniques are seen as effective mitigation strategies. However, the level of visibility they offer misses malicious manipulations occurring within any given device, and infrequent legitimate system-to-user interactions.

In ICS, data originates in the physical space, therefore data reliability and integrity starts from the first point of measurement being processed. Occurring at Level 0 of the Purdue model, an analogue signal must first be calibrated and scaled, transforming it into a useful unit of measurement. This represents the first step where malicious actors may manipulate the data [1]. Once converted into a digital value, the data is presented to a controller (PLC, RTU, etc.) serving as an input to a control algorithm. Process control decisions can be made automatically based on predefined logic, or manually through user interaction with the controller via a human machine interface (HMI).

Based on the automation pyramid principle described in Section I, system comprehension and visibility can be further increased through the mapping of data flows and data processing points within individual devices. Once mapped, a larger attack surface is revealed allowing for further refinement of the risk assessment process and subsequent security control implementation.

2.3 What is Missing

The potential impact on process operations caused through errors arising in the form of incorrect data processing configurations can be as significant as errors induced through malicious manipulation. The latter requires implementation of security controls. However, as ensuring data reliability already presents a significant challenge, implementation of security controls must be careful considered. In the event of risk assessment and security control implementation proceeding based on inadequate knowledge of system-to-system and system-to-user relationships within the OT domain, and between OT/IT domains, additional risk is posed to objectives across both domains.

Without a clear understanding of deviations to original device requirements, the application of risk assessment and security control implementation harbours a distinct possibility of inadequate or inappropriate restriction being implemented, degrading usability and negatively impacting operational, business, and security objectives across the organisation. In search of a solution, operators may look to standards and guidelines for advice on risk assessment and security control implementation. However, applying security standards requires an understanding of the system. With that, the level of system understanding required, and methodology by which it can be obtained/presented, are of critical importance.

Obtaining a view of system-to-system and system-to-user relationships, would provide a platform for comprehensive risk assessment and subsequent tailored security control implementation. Tailoring of controls with a more granular view of data flows and processing points through the ICS would increase harmonisation of data reliability and security. Furthermore, visibility of system-to-user interaction within data flows would allow for streamlined integration of change management. This ensures that operational requirements defined by OT and IT personnel remain unaffected, and where possible, optimised. Without the described level of visibility, not only could system degradation occur, but security controls could adequately protect one critical data flow, yet remain completely blind to another.

3. OVERVIEW OF THE STANDARDS AND GUIDELINES

In order to protect information, businesses are required to implement rules and security controls around the protection of information, including the systems used to store and process it. This is commonly achieved through the implementation of information security policies, standards, guidelines, and procedures. For ICS these can be industry specific [27], or more generic and all inclusive [32]. Applied as a pre-requisite for regulatory compliance, or for their comprehensive guidance, security standards and guidelines offer a resource which has gained interest within the ICS space. Therefore, the following sub-sections review a group of widely used standards and guidelines [1]. Designed to aid the risk assessment and security control implementation process, the following standards and guidelines are discussed. From the British Standards Institute (BSI), ISO 27001 [4], ISO 27002 [5], ISO 31010 [3], and ISO 27019 [6]. From the National Institute of Standards and Technology (NIST), 800-53 [21], 800-30 [20], and 800-82 [32]. To conclude, from the Centre for the Protection of Critical National Infrastructure (CPNI), Managing the Business Risk [11], Risk Assessment [9], Critical Security Controls written in collaboration with the Council on CyberSecurity [14], and Select and Implement Security Improvements [12].

These standards and guidelines have been selected due to their direct targeting of ICS and critical infrastructure en-

[1] ISA99 (ISA-62443/IEC 62443) is recognised as a leading ICS standard. However, as it is currently in working draft, and is likely to be closely linked to ISO 27001 in the upcoming revision, we have chosen not to include it here.

vironments [8], global acceptance as a "common-language" for information security [19], and use across government divisions including the Department of Defense [29].

3.1 Overview of Risk Assessment Processes

Risk assessments output critical information used to define an organisation's security requirements. Taking a basic view of risk, [22] defines risk as "the possibility of a threat exploiting a vulnerability and thereby causing harm to an asset". Therefore, in assessing risk, one should seek to understand the existing system and environment in such a way as to identify risks through pre-described assessment methodologies. System scope and objectives can influence the format of assessment, and subsequent output, for use in the implementation of security controls, mitigating identified risks.

ISO 31010 [3] breaks the risk assessment process down into three key stages: risk identification, risk analysis, and risk evaluation. A broad table of techniques is presented, where each technique's applicability is mapped across the three stages. From this table, each technique is then explained in detail, including its use, required inputs, process, outputs, and strengths/limitations.

NIST 800-30 [20] breaks the risk assessment process down into five stages: Identify Threat Sources and Events, Identify Vulnerabilities and Predisposing Condition, Determine Likelihood of Occurrence, Determine Magnitude of Impact, and Determine Risk. In addition to this, three tiers are defined to refine the requirements across the system: Organisation, Mission/Business Processes, and Information Systems. Taking these as founding principles, each of the five stages is discussed in detail, with required inputs, assessment scales, taxonomies, templates, etc. all included for further practical application.

CPNI Risk Assessment [9] provides a brief discussion of the risk assessment process. The discussion is broken down to four logical sections: identify the threat, decide what needs to be protected and identify vulnerabilities, identify measures to reduce risk, and review your security measures and drills.

NIST 800-82 [32] focuses on special considerations for performing risk assessments within ICS environments. This covers factors such as safety, physical impact, non-digital control components, propagation of impact to connected systems, etc. Additional points such as defining impact as per FIPS 199 [26] (considering ICS risk in relation to its impact on Confidentiality, Integrity and Availability) is also discussed. [26] states that through the use of its impact assessment methodology, one can apply the output in prioritisation of risk assessments, with lower impact systems left unassessed.

ISO 27019 [6] provides a very brief definition of risk assessment, including its use in security measures/control selection. However, beyond this brief definition no further ICS specific guidance is provided.

Managing the Business Risk [11] breaks the risk assessment process down into three stages, defining the risk assessment approach and supporting scales, high level prioritisation of the enterprise, and individual systems/site risk assessment. In addition to the three core steps, four pre-assessment steps are defined as understanding the systems, threats, impacts, and vulnerabilities. Each of these four steps is covered in detail, why each is important, and how it can be considered. From these four points, the expected key outputs of a risk assessment process are described, prior to discussion around the three risk assessment stages, including example impact scales, risk tables, and matrix.

Despite their varying levels of granularity, the risk assessment frameworks described here follow a similar process to the one summarised in Fig. 2. The described adaptation required to apply assessment approached in an ICS context, even if provided at a high level of abstraction, offers a starting point allowing for further exploration and development.

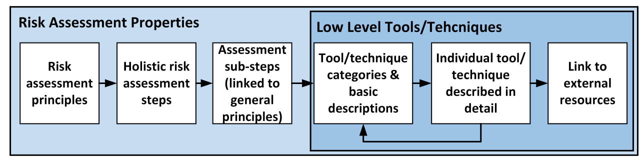

Figure 2: Risk assessment process overview

3.2 Overview of Security Controls Selection Processes

Security controls are the management, operational, and technical safeguards or countermeasures, employed within an organisational information system. These provide safeguards or countermeasures, against the realisation of security risks to assets identified through a risk assessment process, where assets are defined as any organisational resource (data, systems, humans, etc.) [37].

ISO 27001 [4] provides a set of overarching security controls categories, subcategories with associated objectives, and individual controls where each control is presented in the form of a clear concise description. Through the application of categorisation, selection of relevant controls is simplified. ISO 27002 [5] sits in parallel to the controls covered in [4], providing more granular detail on each control, including implementation guidance and other relevant information.

NIST 800-53 [21] presents guidance on security controls in a similar way to [4] and [5]. Presenting overarching security control categories, subcategories with associated objectives, and individual controls with relevant related controls highlighted for further exploration.

ISO 27019 [6] takes the security controls defined in an outdated revision of [5] ([2]) and discusses, where applicable, additional information specific to the energy utility sector.

NIST 800-82 [32] takes recommendations as described in [21] and provides additional ICS-specific Recommendations and Guidance, similar to, yet in more detail than [6]. An overlay is provided within appendix G, used to further understand how controls must be tailored to fit ICS environments. Furthermore, acknowledgement is made towards ICS specific challenges, and where recommended controls can not be applied, compensatory controls may be adopted in their place.

CPNI/Council on Cyber Security Top 20 Security Controls [14] is designed for a broad ranging audience, as such it does not contain the level of granularity offered by other works. However, twenty overarching categories of security controls are defined, sub-categories then present descriptions of specific security controls and their goals.

CPNI Select and Implement Security Improvements [12] is not designed to present a comprehensive set of security controls, but gives guidance on key factors to consider when selecting and implementing controls. Discussion around economies of scale, skill and experience, diversification, prioritisation, costing, change control, etc. are all covered within the context of ICS.

The security control selection and implementation standards and guidelines described here offer varying levels of granularity. Their process can be summarised as in Fig. 3. Tailoring of controls for use within an ICS context ranges from high level consideration of prioritisation, skills, etc. down to individual, control specific, augmentation advice. The presentation of advice at varying levels of abstraction can been as a positive, in that it plays to the strengths of a diverse audience, specifically where ICS operators are venturing into the world of security for the first time.

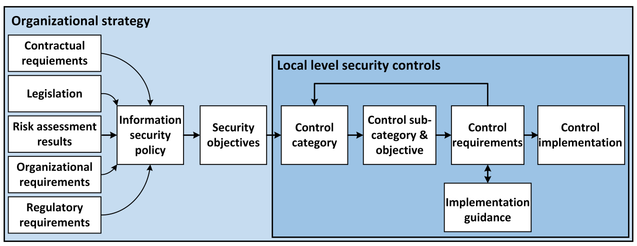

Figure 3: Security controls selection overview

3.3 What is Missing

One of the key challenges when performing a security risk assessment is estimating where all the risks lie. Incomplete understanding of risks yields narrowly formulated security objectives and scant security controls.

The provided overview of standards and guidelines demonstrates how well established approaches designed for IT systems have been adapted for an ICS audience. However, the focus remains on information security, protecting access, and ensuring secure delivery of packets, and not on securing process operations. With a primary security objective of protecting data integrity, as loss of data integrity directly results in loss of view, and therefore loss of control over the physical operational process. It is for this reason when seeking to perform a risk assessment, and to subsequently implement security controls, understanding the system on which such tasks are to be performed becomes critical.

Where guidance is provided around understanding the system, it may prove insufficient for comprehensive risk assessment and security control implementation within an ICS context. For example, [11] provides a set of questions that could be used to create an inventory of devices, technologies, asset owners, etc. considering upstream and downstream dependencies. However, where [3] defines prerequisites for individual assessment techniques, would the proposed inventory, created with little guidance other than a set of questions, fulfil such prerequisites. Furthermore, where security control implementation must consider system-wide objectives/requirements, in parallel to risk assessment outputs, a comprehensive understanding of the system is also required. This understanding is required at a technical system-to-system, and at a social system-to-user level.

Tools developed to assist the risk assessment process include [35], and provide the assessor a way in which their systems can be measured against a catalogue of standards. However, little advice is provided on how best to obtain the information required to ensure accurate results are produced. Additional training focusing on system familiarisation is offered as an optional on-site resource [33]. Alternatively, on-site offerings from ICS-CERT [34] can be requested in a further attempt to bridge this gap. However, these appear to be high-level, and do not encompass system-to-user relationships.

Viewpoints confined to a local level provide insufficient granular visibility, and clear comprehension of the given system, missing attack surfaces, and identification of not only IT vs. OT, but OT vs. OT challenges. The resulting effect is formulation of incomplete risk assessments. This has the potential to lead towards implementation of ineffective and even damaging security controls.

4. CASE STUDY

With the increasing complexity and challenges presented in modern day ICS, reliance on current standards and guidelines may not include adequate advice to ensure desired levels of system security and resilience. Although risk assessment methodologies and security controls are described in detail, advice on understanding the system may be insufficient.

To better understand and contextualise the relationships and interconnect between systems and users across an ICS, the following case study has been conducted in collaboration with a European utility company. Initially focusing on end-to-end system-to-system relationships at varying levels of abstraction, Fig. 4 has been created as a conceptual visualisation tool, aggregating information from several sources (network architecture reviews, configuration reviews, interviews, etc.). From this system-to-system baseline, system-to-user relationships are overlaid, thus presenting a holistic view or "understanding" of the system beyond approaches described by the reviewed standards and guidelines.

4.1 Data Flow Map

Fig. 4 presents the flow of data from a single sensor to remote access connectivity residing within the highest level of the ICS (Level 5). Each device (PLC, RTU, Historian, etc.), and sub-component (memory location, interface, function, etc.), is depicted by a square or circular node. Circular nodes represents user interaction/visibility of process data via an interface. Square nodes with dashed edges represent a function being applied to the data stream (i.e. a data processing point). To highlight the complexity of device configuration, system-to-system, and system-to-user interaction, the PLC (nodes within the black dashed line) has been presented at a lower level of abstraction, showing sub-components within a logical flow. This increased level of granularity allows for comprehension of critical functions and memory addressing, applied to the computational processing of one signal. Furthermore, separation of data used for monitoring functionality by the RTU and Historian (DB2), vs. process control functionality used within PLC control logic and by HMIs/Workstations (DB1), demonstrates a clear separation of duties and user access within the device.

Each node in Fig. 4 is colour coded to represent the system level in which it resides according to the Purdue model. However, as can be seen with some nodes (e.g."AI Card Slot 3") two colours are applied. This application of colour has been introduced where a device or sub-component, is accessed and/or is under the control/management of sys-

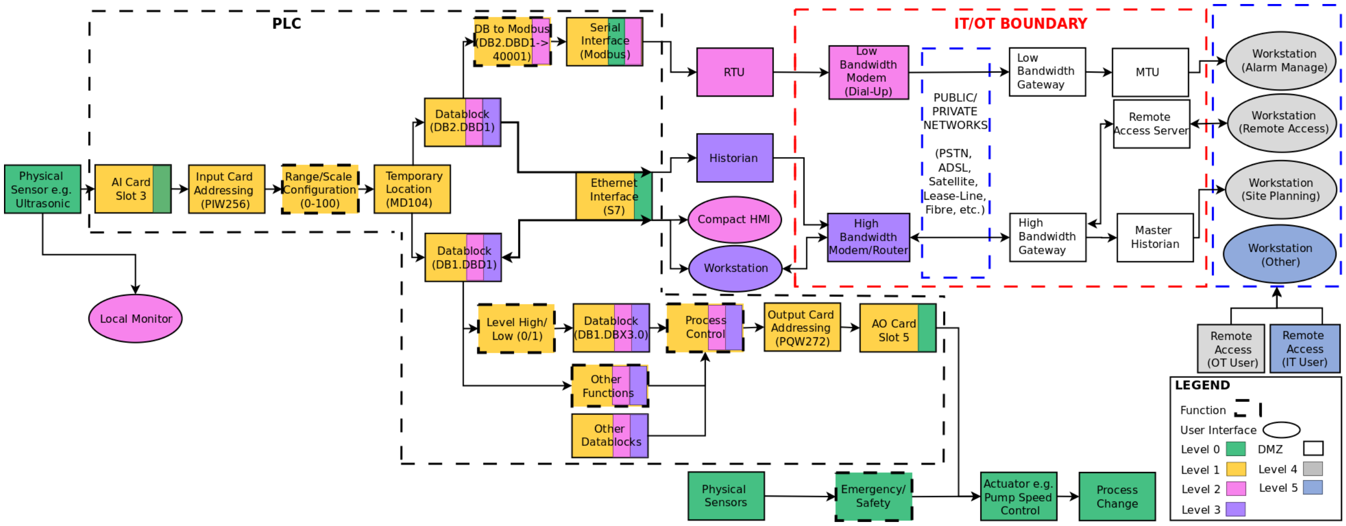

Figure 4: Data flow of a single sensor through the levels of ICS reference architecture

tem users from more than one level. In this example, the AI (analogue input) card represents a physical interface on the PLC (a PLC sub-component). Level 0 instrumentation engineers are responsible for sensors feeding this card, and Level 1 control engineers are responsible for the operational logic being executed on the PLC, therefore both require access. This shared access could be required for fault-finding and secondary verification of signal quality, among others. Through this example, and consideration towards security of the PLC, one could assume little additional risk is presented through shared ownership; however without a detailed level of system-to-user awareness, an appropriate assessment can not be conducted.

Additional detail on system-to-user relationships can be identified through the application of bidirectional links. For example, one such link can be seen between DB1.DBD1 and the HMI/Workstation. This communication path is predominantly used to observe the values stored in DB1.DBD1, however in the case of an emergency, operators are able to override this value. Situations of this nature can occur in the case of a failed or faulty sensor, with manual readings being taken directly at the source (i.e. a visual inspection of the operational process in question), before being entered into the HMI/Workstation interface.

Following guidance on appropriate assessment techniques described in [24], analysis of network diagrams and informal engagement with support/maintenance personnel was used to provide a high-level understanding of system devices. This allow us to build an overarching end-to-end flow of data over system devices and communication links. Applying the aforementioned colour coding, highlights devices and their position within the Purdue model. Interviews with personnel across each level were used in aligning access requirements to devices, thus identifying any shared ownership. As described above, colour coding was applied to highlight shared ownership/requirements. In all subsequent stages, analysis was directed towards one device, a PLC. The purpose of this narrowed scope was to identify sub-components of the PLC, allowing for more detailed granular analysis. Manufacturing zone (Fig. 1) network traffic captures and basic configuration reviews identified core communication interfaces and memory addressing. Additional refinement required a more detailed configuration review (PLC ladder logic), in parallel to interviews with manufacturing zone support/maintenance personnel.

Although the process description here presents a moderately linear approach, we found each step and technique allowed for greater comprehension of data captured across all steps. Therefore, while these described steps provide the foundation of our adopted approach, techniques were applied in a cyclic manner, running through several iterations of analysis prior to the resulting data flow map in Fig. 4.

Exploration of more complex system-to-user relationships first requires an understanding of role groups across each level of the ICS. The following section explores this, relating back to Fig. 4 and the overall discussion provided here.

4.2 System Users

A significant number and variety of roles were identified during the case study. These roles performed a multitude of functions across the organisation, from operational process management, to budgeting, mechanical engineering, and performance evaluation. We first sought help in existing literature [31], and this identified six key roles within ICS environments. These were Junior Operator, Senior Operator, Supervisor, Technician, Engineer and Manager. Although applicable to the case study, from interactions conducted with the participating organisation, we determined additional granularity would prove highly beneficial.

Firstly, baseline separation of core role functions and system levels as discussed in our previous work [18], provided a foundation for further discussion. As such, the role groups highlighted through the case study have been separated into two categories, “Operators” and “Support/Maintenance”. The operators group could include physical access to operational sites and control rooms, however system access excludes the ability to modify device/system configurations. The Support/Maintenance group could also include physical access to operational sites, control rooms, and data centres; however this role category includes the ability to modify device/system configurations. Table 1 presents a summary of our case study findings, identifying key role groups and the

ICS levels in which they operate. The view of roles groups provided through this case study adds significantly more granularity, particularly when tied to system levels. Based on Table 1, we can begin to analyse nodes within Fig. 4, overlaying role information, and understanding challenges induced through previously unconsidered system-to-user relationships.

Operator Roles	ICS Level
Process Control Operators	2,3,4,5
Local Process Managers	2,3,4,5
Regional Process Managers	3,4,5
Regulatory Monitors/Testers	2,3,4,5
Performance Analysts	4,5
3rd Party Contractors	0,1,2,3,DMZ,4,5
Alarm Management Centre Operator	4,5
Health and Safety Officers	0,1,2,3,DMZ,4,5
Home Workers	3,4,5
Support/Maintenance Roles	ICS Level
Electrical Engineers	0,1,2,5
Mechanical Engineers	0,5
Control System Engineers	0,1,2,3,5
Instrumentation Engineers	0,1,2,5
Telemetry Engineers	0,1,2,3,DMZ,4,5
Communications Engineers	3,DMZ,4,5
Information Technology Engineers	DMZ,4,5
3rd Party Contractors	0,1,2,3,DMZ,4,5
Home Workers	3,DMZ,4,5

Table 1: ICS roles and associated permissions at ICS levels

It is important to note that roles and permission as presented in Table 1 are not static. The diversity in role groups across large vs. small ICS, sub-roles, and deviations in responsibilities over time, all add to role dynamics. For example, the involvement of work experience/placements, apprenticeship schemes, reorganisations, etc. can all influence the system-to-user dynamic, even if for a short period. Also, levels of seniority exist within some of the defined groups. For example, in some engineering roles, junior engineers (often referred to as "Technicians") perform limited tasks when compared to fully qualified engineers, and senior engineers may perform additional tasks, or act as a knowledge-base/resource for engineers and junior engineers alike.

To further highlight the importance of role identification and system level mapping, an example of portable device use was discussed though the case study. Instrumentation engineers performing tasks within Level 0, connected their laptops not only to the varying levels of OT networks, but to the corporate IT network. Historically a dual laptop approach had been adopted (usage of dedicated industrial and general purpose laptops). However, consolidation was deemed appropriate for cost saving and ease of ongoing device management. The risk associated with devices being moved between OT and IT networks would at least on first impressions appear to be significant, with security controls restricting the flow of data between IT and OT effectively bypassed. However, where the level of risk may or may not be increased through this approach to portable device use, as with the aforementioned analogue input card example, without a clear understanding of system-to-user relationships, appropriate assessment can not take place.

4.3 Discussion

Taking the previously discussed requirements of a single sensor input (regulators, performance analysts, remote alarm management, etc.), Fig. 4 and the associated role groups in Table 1, provide a platform on which further analysis of data flows and critical data processing points can be identified and assessed. Expanding on previous examples, we discussed the issue of multiple roles per node with a DMZ historian server engineer. Historians are responsible for collecting data from remote field sites, performing complex computational functions, and providing users with data used in a variety of analytical frameworks (performance analysis, regulatory requirements, etc.).

In Fig. 4 a temporary marker memory address in the PLC logic (MD104) splits into two discrete datablocks, one for on-site control logic and workstation interaction, the other for off-site monitoring and alarm management, with several systems and users involved in directly supporting/utilising the data at a local level (Levels 1, 2, and 3). The types of system faults discussed, related to Level 1 control engineers (responsible for process logic) modifying functions or addressing prior to this data split. As the scope of their interaction with the PLC is focused on process operations, there was little consideration/understanding for other system and user requirements. As a result, while all control logic/addressing residing within process operations was modified to reflect changes further down the chain, other logic/addressing was not, leading to the corruption of calculations and values within the historian server.

The way in which errors in operational data discussed here are typically discovered further highlights the importance of role and device mapping. End users of this data were highlighting deviation in values post specified dates and times, a somewhat reactive approach. From the initial suspicions around spurious data, essentially data quality concerns, historian support engineers would drill down into complex mathematical calculation to find a root cause. Where calculation are derived from up to 30+ operational tags (signal inputs), this process could prove time consuming. Furthermore, where data is processed at multiple points in the system, as seen in Fig. 4, the requirement for a high level of access privileges becomes apparent, and where visibility of data ends at the multicoloured node (PLC addressing), interaction with Level 1 control engineers would be required to better understand any changes further downstream.

Additionally, with regards to the use of a marker memory location (MD) prior to transferral into datablocks (DB), this could be considered a poor PLC coding choice. The size of marker memory may be limited given the age of the device, offering limited value retention capabilities when the device is powered down, and increasing PLC logic complexity. A cleaner option would be to move this value directly into the primary process control and local monitoring datablock (DB1), then if required by the RTU and Historian, pass this value directly from DB1 into DB2. Derived values generated by the PLC logic (e.g. where two sensor values are entered into a calculation arriving at a new value) are already being passed from DB1 into DB2, therefore including sensor values in this function would be a more logical and cleaner approach, accompanied by the additional benefits offered through datablock usage.

The conducted case study has been used to highlight technical complexities of interconnecting devices found within ICS, and in the case of a PLC, complex configuration/logic, including the separation of data based on operational objectives. From this, the overlay of role groups has shown the quantity and diversity of individuals operating and maintaining such systems. Overall the case study has demonstrated the challenges of addressing security, and that security may not be addressed through purely technical means (firewalls, IPS, etc.). Whether they be assessment metrics or security controls, challenges must be addressed from a socio-technical (humans and systems) viewpoint, incorporating the core operational objectives of each level and role within assessment, planning, and mitigation strategies.

The level of granularity provided through the application of Fig. 4 to security control implementation, based on appropriate comprehensive risk assessment outputs, allows for harmonisation of data reliability and security. This is achieved through the tailoring of security controls considering system-to-system and system-to-user interactions, and requirements. For example, at a low level, the deployment of firewall rules controlling system and user interaction with a specified PLC memory location can be achieved without fear of system degradation between OT systems, addressing OT vs OT concerns, and between OT and IT systems, addressing OT vs IT concerns.

5. CONCLUSION AND FUTURE WORK

Existing approaches to risk assessment and security control selection as defined by the reviewed standards and guidelines provide a good starting point. However, initial phases of such assessments and ongoing support could be enhanced through a better understanding of end-to-end system-to-system and system-to-user interaction. From a risk perspective we have highlighted that simply obtaining an inventory of devices and network architectures is insufficient to comprehensively map risk in ICS environments. Understanding the relationships between roles and devices, and where possible, roles and device sub-component parameters, is required to develop risk mitigation strategies.

Although the evolution of next-generation ICS security control appliances seeks to provide granular rule-sets over network traffic flows [13], guidance on obtaining a clear understanding of data flows and associated stakeholders is limited. Used in collaboration with our tool, a feedback loop for granular formulation of control policies and traffic restrictions enforced by security products will be made possible.

Where previously described assessment tools [35] lack guidance on obtaining system-to-system and system-to-user knowledge, we believe our tool/approach could be adopted as a pre-requisite. Applied in this way takes assessors beyond current on-site ICS-CERT offerings, which assist in the identification of high-level (end point-to-end point) data flows, and exclude system stakeholders [34]. This increased understanding/familiarisation of system-to-system and system-to-user relationships will allow for more detailed, accurate assessment results to be generated. To further validate this assertion, we will seek to engage with risk assessors and security practitioners at real-world facilities, while making use of Lancaster's [28, 17] and Singapore's (Secure Water Treatment (SWaT)) [25] test-bed environments. This will involve the evaluation of risk assessment and control implementation, applying existing methodologies for "understanding the system", prior to the use of our proposed tool.

5.1 Future Work

As we have not yet provided a method by which others can effectively obtain granular data flows within their own environments, this will be our core focus in future work. This approach will be accompanied by a framework of parameters one must adhere to in the creation of data flow, processing, and user interaction maps. In addition to this, integration of tools and techniques for data capture will be explored, in order to assist the process.

The development of a formal methodology will aim to ensure practical scalability of our tool. Focused management of methodological overhead plays a significant role in achieving this goal. This can be assisted through the use of passive network analysis tools [13] [38], and continuing industry engagement. Detailing techniques for signal prioritisation will also be used, narrowing scope where insufficient resources are available for comprehensive analysis. Through ongoing discussion with industry, we believe RTU criticality scale could be used as a metric. Our engagement with industry has shown that large scale manufacturing zones can have as little as a few 10s of signals of highest criticality, providing a starting point for granular data flow, processing, and user interaction mapping.

Going further, we will explore scoping of parameters that focus on time constants of system-to-system interactions and associated data processing point criticality (time to negative impact), essentially aiding the formulation of device configuration requirements. This increased scope in "understanding the system" will provide yet more granularity, giving risk assessment and security control implementation highly detailed visibility of device requirements/objectives.

Increased visibility into data flows, alongside comprehension of data processing points, and data consumption relationships, will be essential to forensic investigations. As a starting point we will look to explore the proposed tools use in the determination of infected devices (where unauthorised data change is occurring), estimation of attack origins (through the analysis of interdependencies), and identification of compromised user credentials.

6. REFERENCES

[1] A. Bolshev, J. Larsen, M. Krotofil, and R. Whitmann. A rising tide: Design exploits in industrial control systems. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Aug. 2016.

[2] British Standards Institute. Information technology - Security techniques - Code of Practice for Information Security Management. 2005.

[3] British Standards Institute. BS ISO/IEC 31010 - Risk management - Risk Assessment Techniques. 2010.

[4] British Standards Institute. BS ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems - Requirements. 2013.

[5] British Standards Institute. BS ISO/IEC 27002 - Information Technology - Security Techniques - Code of Practice for Information Security Controls. 2013.

[6] British Standards Institute. BS ISO/IEC 27019:2013 - Security Techniques - Information Security Management Guidelines Based On ISO/IEC 27002 for Process Control Systems Specific to Utility Industry. 2013.

[7] P. Carson. The IT vs. OT debate | Intelligent Utility. *Intelligent Utility Magazine*, pages 32–34, 2010.

[8] Centre for the Protection of National Infrastructure. Cyber Security. http://www.cpni.gov.uk/advice/cyber/. Retrieved: December, 2015.

[9] Centre for the Protection of National Infrastructure. Risk Assessment. http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan/Risk-assessment/. Retrieved: December, 2015.

[10] Centre for the Protection of National Infrastructure. The National Infrastructure. http://www.cpni.gov.uk/about/cni/, 2014. Retrieved: January, 2016.

[11] Centre for the Protection of National Infrastructure. Security for Industrial Control Systems: Manage the Business Risk (a good practice guide). 2015.

[12] Centre for the Protection of National Infrastructure. Select and Implement Security Improvements. 2015.

[13] Check Point Software Technologies. Critical Infrastructure & ICS/SCADA. https://www.checkpoint.com/products-solutions/critical-infrastructure/, 2016. Retrieved: July, 2016.

[14] Council on Cyber Security. The Critical Security Controls for Effective Cyber Defense. 2014.

[15] DEFRA. Waste Water Treatment in the United Kingdom. http://tinyurl.com/nhkhhyb, 2012. Retrieved: June, 2015.

[16] P. Didier, F. Macias, J. Harstad, R. Antholine, A. Johnston, S, S. Piyecsky, M. Schillace, G. Wilcox, D. Zaniewski, and S. Zuponcic. Converged Plantwide Ethernet (CPwE) Design and Implementation Guide. *CISCO Systems and Rockwell Automation*, 2011.

[17] B. Green, D. Hutchison, S. A. F. Frey, and A. Rashid. Testbed Diversity as a Fundamental Principle for Effective ICS Security Research. In *International Workshop on Security and Resilience of Cyber-Physical Infrastructures*, pages 1–8, 2016.

[18] B. Green, D. Prince, U. Roedig, J. Busby, and D. Hutchison. Socio-Technical Security Analysis of Industrial Control Systems (ICS). In *2nd International Symposium for ICS & SCADA Cyber Security Research(ICS-CSR)*, 2014.

[19] E. Humphreys. Information Security Management Standards: Compliance, Governance and Risk Management. *Information Security Technical Report*, 13(4):247–255, 2008.

[20] Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. *NIST Publication*, 2012.

[21] Joint Task Force Transformation Initiative. Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication*, 2013.

[22] A. Jones and D. Ashenden. *Risk Managment for Computer Security - Protecting Your Network and Information Assets*. Elsevier, 2005.

[23] Kaspersky Lab. ICS Vulnerabilities Statistics 2015. http://tinyurl.com/jh4658o, 2015. Retrieved: June, 2015.

[24] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, and A. Rashid. Assurance Techniques for Industrial Control Systems (ICS). In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, pages 101–112. ACM, 2015.

[25] A. P. Mathur and N. O. Tippenhauer. Swat: a water treatment testbed for research and training on ics security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36, April 2016.

[26] National Institute of Standards and Technology. FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. 2004.

[27] Norwegian Oil and Gas Association. 110 - Recommended Guidelines for Implementation of Information Security in Process Control, Safety and Support ICT Systems During the Engineering, Procurement and Commissioning Phases. Technical report, 2008.

[28] B. Paske, B. Green, D. Prince, and D. Hutchison. Design and Construction of an Industrial Control System Testbed. In *PGNET*, pages 151–156, 2014.

[29] R. Ross. Managing enterprise security risk with NIST standards. *Computer*, 40(8):88–91, 2007.

[30] T. Sauter, S. Soucek, W. Kastner, and D. Dietrich. The Evolution of Factory and Building Automation. *IEEE Industrial Electronics Magazine*, 5(3):35–48, Sept 2011.

[31] R. Singla and A. Khosla. Intelligent Security System for HMI in SCADA Applications. *International Journal of Modeling and Optimization*, 2(4):444–448, 2012.

[32] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn. Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication*, 2015.

[33] U.S. Department of Homeland Security. Assessment Program Overview. https://ics-cert.us-cert.gov/Assessments, 2016. Retrieved: September, 2016.

[34] U.S. Department of Homeland Security. Control Systems Architecture Analysis Services. http://tinyurl.com/gnr4g5g, 2016. Retrieved: September, 2016.

[35] U.S. Department of Homeland Security. Cyber Resilience Review & Cyber Security Evaluation Tool. http://tinyurl.com/jqes9te, 2016. Retrieved: September, 2016.

[36] J. M. Weiss. Presentation on how to hack a chemical plant and its implication to actual issues at a nuclear plant. http://tinyurl.com/jr985ru, 2015. Retrieved: January, 2016.

[37] M. Whitman and H. Mattord. *Principles of information security*. Cengage Learning, Boston, 4 edition, 2011.

[38] Wireshark.org. About Wireshark. https://www.wireshark.org/, 2016. Retrieved: July, 2016.