Global Flow Measurement Workshop
22 - 24 October 2024

Technical Paper

Cybersecurity Considerations for Flow Measurement Infrastructure in the Digital Age

Hosam Ismail, Emerson Automation Solutions
Gary Collister, Emerson Automation Solutions

1 INTRODUCTION

In the oil and gas industry, custody transfer measurement systems are crucial for accurate financial and legal transactions. Discrepancies or tampering can lead to significant financial losses, legal disputes, and reputational damage.

Unlike other aspects of flow measurement operations governed by stringent regulatory frameworks (consider flow calculations as an example), cybersecurity for metering systems has lacked comprehensive, enforceable standards. This regulatory gap meant that some companies developed and implemented their own security protocols, often based on perceived risks and available resources rather than a standardized approach. In contrast, other companies didn’t consider this requirement, which resulted in variable security postures and challenges in maintaining and updating the systems.

A far more cohesive approach is required to secure oil and gas measurement systems, this being recognized in the context of the broader oil and gas industry by the World Economic Forum, announcing in 2022 that 18 oil and gas companies had pledged to come together in a collective effort to improve cybersecurity within the domain [1]. There are now a plethora of best practices, guidelines, and standards that can be drawn upon to determine a baseline and recommended set of protective measures for flow measurement systems.

This paper will discuss how introducing a cybersecurity management system can help mitigate risks and ensure a more consistent and secure approach to protecting custody transfer measurement systems. The paper will further propose what could be considered the baseline cybersecurity requirements for such systems, given their common risks.

2 FLOW MEASUREMENT SYSTEMS CYBERSECURITY CHALLENGES

2.1 Historical Architecture

For many years, metering supervisory systems in the oil and gas industry were designed to be largely isolated from the rest of the network infrastructure. This separation was intended to ensure that the critical metering operations were insulated from potential disruptions and unauthorized access from external sources. The Industrial Control System (ICS) on the plant Local Area Network (LAN) was responsible for overall plant operations but had limited interaction with the metering LAN, usually a simple Modbus serial or Modbus Transmission Control Protocol / Internet Protocol (Modbus TCP/IP) interface. Fig. 1, depicts a simple segregation between the metering LAN, the plant LAN, and beyond to the broader Enterprise LANs and, of course, the Internet. This perceived isolation meant that cybersecurity was often given little attention or priority.

However, this isolation, while perceived as having a positive impact on cybersecurity, resulted in some significant drawbacks:

- Supervisory systems were frequently overlooked as they were not connected to the broader network infrastructure, which meant they were often exempt from scrutiny during design and installation and from ongoing security audits.

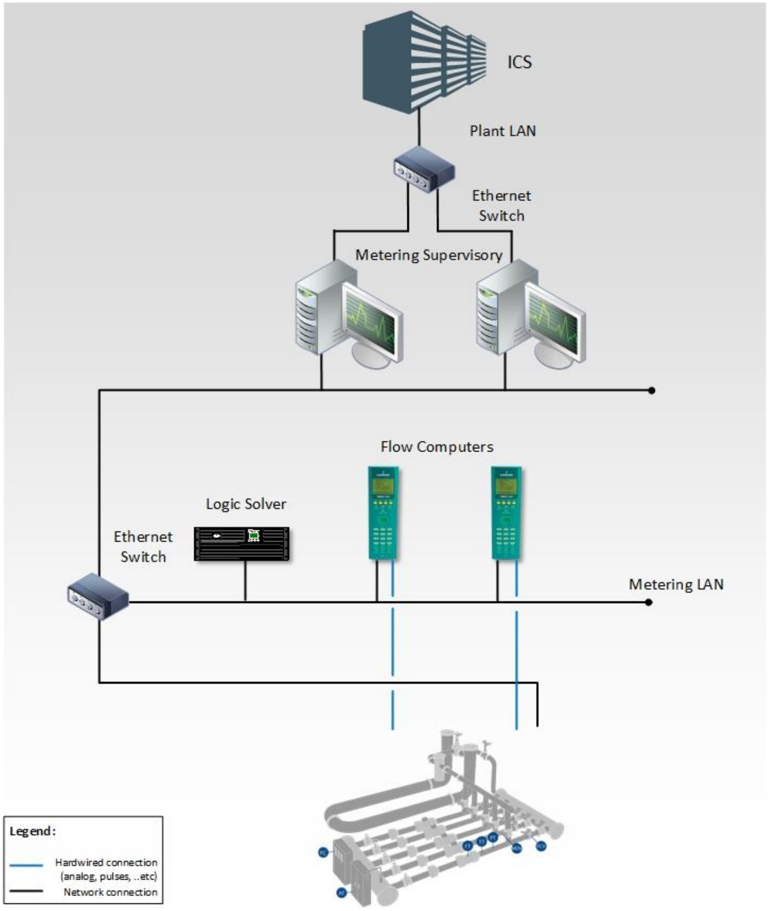

Fig. 1 - Historical Flow Measurement System Architecture

- Servers hosting supervisory systems could be located on desks in Local Equipment Rooms or Control Rooms, providing poor physical security.
- Due to the difficulty in transferring data, reports, and backups from these systems, it was common practice to use Universal Serial Bus (USB) drives for this purpose.
- With no access to broader Information Technology (IT) user access control, such as Active Directory, most systems relied on local users and passwords, not always adhering to best practices and possibly leaving back doors in terms of the user accounts available – consider vendor default accounts and accounts for personnel that may have left the organization.

2.2 Modern Cybersecurity Vulnerabilities

With the advent of digitalization, remote connectivity, and cloud-based solutions, the isolation of metering systems has significantly diminished, potentially alleviating some of the issues but also exposing these systems to a range of new cybersecurity vulnerabilities, including:

2.2.1 Access Risks

The increased connectivity between the metering LAN and external networks results in a broader pool of personnel who could potentially access the metering systems and, intentionally or unintentionally, make unauthorized changes to the fiscal regimes. This could compromise the integrity of the fiscal data and result in inaccurate measurements and financial discrepancies. Furthermore, black hat hackers may exploit this vulnerability for more malicious purposes like Industrial Espionage and Financial Exploitation, Denial of Service (DoS) attacks [2], [3], [4] and Operational Disruptions. In 2022, the Federal Bureau of Investigation (FBI) reported that ransomware had been specifically designed to disrupt key industrial targets [5].

2.2.2 Protocol Vulnerabilities

- Unencrypted Communications: Many communication protocols used in metering systems, such as Modbus, lack encryption. This vulnerability allows attackers to intercept and read data packets, exposing sensitive information to eavesdropping attacks [6], [7].
- Lack of Authentication: Traditional protocols often do not include authentication mechanisms, making it easy for unauthorized devices to connect and issue commands to metering systems.
- Replay and Man-in-the-Middle Attacks: The absence of robust security features in protocols like Modbus makes them vulnerable to replay and man-in-the-middle attacks, where attackers can intercept, modify, or retransmit valid data packets to disrupt operations. ESET researchers in 2024 discovered an advanced adversary man-in-the-middle attack targeting telecommunications traffic [8].
- Broadcast Storm Vulnerability: Modbus TCP/IP can be susceptible to broadcast storms, where excessive broadcast traffic overwhelms the network, causing DoS conditions.
- Protocol-Specific Attacks: Modbus is vulnerable to malformed packet injections and improper handling of exceptional conditions, which can crash or exploit devices.
- Limited Access Control: Traditional Modbus implementations do not support fine-grained access control, which means that once any device is connected to the network, it can issue any command without restriction.

2.2.3 Legacy Systems

- Outdated Software and Hardware: Many metering systems still rely on outdated software and hardware, which lack modern security features. These legacy systems are particularly vulnerable to cyberattacks, as they often cannot be easily updated or patched. An incident in July 2024, reported by Dragos [9], highlights the requirement for network monitoring on measurement systems, something that previously may have been considered excessive on such systems. FrostyGoop is a malware that explicitly targets Modbus TCP/IP communications over port 502. It can read and write from/to Modbus holding registers, and, crucially, anti-virus did not pick up the malware as a threat. This incident underscores the need for protocol-aware monitoring tools to be in continuous operation on measurement systems, especially given the widespread use of Modbus within the domain.
- Integration with Modern Systems: The convergence of Information Technology (IT) and Operational Technology (OT) networks means that traditionally isolated metering systems are now connected to enterprise systems. This integration increases the attack surface and exposes metering systems to a broader range of cybersecurity threats.

2.2.4 Remote Access

- Susceptible to Exploit: While remote access brings many benefits in terms of operational efficiency and support, many software packages utilized for this purpose are prime targets for attack. In 2023, Claroty noted that over 70% of identified industrial control system vulnerabilities were exploitable remotely [10].

2.2.5 Complexity

- Design: Alongside the benefits of greater connectivity, there is an associated increase in the complexity of cybersecurity measures that need to be implemented. This complexity manifests itself in requirements for specialists with extensive knowledge of the cybersecurity environment and an organization that can manage the increased number of components and vendors associated with the solution.
- The lack of proper network segmentation has given rise to several potentially serious vulnerabilities in the ICS environment [4].
- Financial implications: Many components of a modern, comprehensive cybersecurity solution are initially expensive and come with ongoing costs [5], [10].

3 REGULATORY FRAMEWORK AND STANDARDS

There is a broad spectrum of continuously growing OT cybersecurity legislations, which are of variable degrees of relevance to custody transfer metering systems. For example, the cybersecurity directives issued by the Transportation Safety Administration (TSA) in 2021 and 2022 imposed several obligations on many oil and gas pipeline operating companies in the United States [11], [12]. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) [13] mandates that specific critical infrastructure sectors, including oil and gas, must report significant cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) to enhance the federal government's ability to understand, mitigate, and respond to cyber threats.

To protect Critical National Infrastructure (CNI), the UK’s Network and Information Systems (NIS) released Regulations 2018 [14]. These regulations were originally based on the EU’s NIS Directives, but some changes and adaptations have been made to fit the UK’s specific needs, especially after Brexit. In 2022, the UK government set the National Cyber Strategy [15], which is considered the guide to the nation's approach to cybersecurity.

The European Union recently imposed the Network and Information Systems Directive 2 (NIS2) to improve the cybersecurity resilience of critical infrastructure across member states. The NIS2 is a revised version of the original NIS Directive (Directive (EU) 2016/1148), which was adopted to enhance the level of cybersecurity and resilience of industrial networks and information systems across the EU. The NIS2 Directive is set to be transposed into national law by October 17, 2024. The new legislation mandates that essential entities implement ten minimum cybersecurity risk-management measures based on an all-hazard approach to address cyber threats, as indicated in Article 21 [16]:

- Risk Analysis and Security Policies.
- Incident Handling and Reporting Requirements.
- Business Continuity and Crisis Management.
- Supply Chain Security.
- System Security measures around Acquisition, Development, and Maintenance.
- Assessments and Audits of the Security Measures.
- Cybersecurity training and practices for basic cyber hygiene.
- Use of Cryptography and Encryption where appropriate.
- Asset Cyber Program Management and Access Control.
- Using multi-factor authentication and continuous authentication solutions when appropriate.

On the other hand, standards are voluntary codes with no obligations to comply with unless when compliance is required by contractual obligations or referred to in national legislation. A few international standards might be referenced when assessing the resilience of system design and management to cyber threats. The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have jointly developed and published the ISA/IEC 62443 series of standards to address the need to improve the cybersecurity of Industrial Automation Control Systems (IACS). The standard is structured into four groups, each with its specific focus. These groups are the general group, policies and procedures group, system group, and components group.

In 2013, President Obama signed Executive Order 13636, Improving Critical Infrastructure Cybersecurity, which aimed to strengthen cybersecurity efforts within the United States. The Executive Order directed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework to control and reduce cyber risks to critical infrastructure. The NIST CSF (Cybersecurity Framework) is widely used across various sectors to enhance cybersecurity resilience. It provides a framework of top-level cybersecurity goals that organizations can utilize to get a better understanding, assess, prioritize, and effectively communicate their cybersecurity efforts [17]. In February 2024, the NIST released the NIST CSF2, which is intended to help not only those organizations in critical infrastructure but all types of organizations to manage and reduce cyber risks. In the latest revision, the NIST has updated the CSF's core guidance and created a suite of tools to help organizations implement and manage cybersecurity measures. The Framework Core includes five functions—Identify, Protect, Detect, Respond, and Recover—providing a high-level, strategic view of an organization's cybersecurity risk management.

The API 1164 standards, Pipeline Control Systems Cybersecurity, is targeted for pipeline operators. The standard outlines the requirements and framework needed to develop and manage the pipelines' Industrial Automation and Control (IAC) cybersecurity as part of the TSA's Corporate Security Program. References are made within this standard to both the TSA regulatory requirements and the NIST CSF. The API 1164 defines three profiles of cybersecurity activities and outcomes based on the business objectives and potential impact.

Both ISA/IEC 62443 and NIST CSF offer valuable guidance for cybersecurity best practices but serve different primary audiences and purposes. ISA/IEC 62443 is particular to industrial control systems, providing detailed and prescriptive requirements, whereas NIST CSF offers a more flexible framework suitable for a wide range of sectors and organizations.

4 IACS CYBERSECURITY MANAGEMENT

4.1 Cybersecurity Management System

Developing and implementing an efficient IACS cybersecurity strategy is a continuous process that starts during the early engineering design stage and continues throughout the system's lifecycle, with the goal being to determine and mitigate cyber risks. The ISA/IEC 62443-2-1 [18] defines the elements of a Cybersecurity Management System (CSMS) that organizations can adopt to protect their OT assets from cyber risks, as indicated in Fig. 2. These elements are classified, as per the same standard, into three main categories:

4.1.1 Risk Analysis

This category describes the requirements for developing the business rationale that justifies the expenditures and ensures management's commitment. It introduces the basis for risk identification, classification, and assessment process describing the cyber risks and assessing the probability and severity of these risks. Based on the outcome of this analysis, a customized cybersecurity management program is developed to address the specific organization's risks. The ISA/IEC 62443-3-2 [19], provides guidance for the cybersecurity risk assessment process.

For flow measurement systems, the vulnerabilities and threats may vary depending on the specific system, but consequences are usually common. For instance, unauthorized changes in fiscal calculations will lead to reputational damage and financial implications proportional to the system's throughput and the bias introduced.

4.1.2 Addressing Risk with the CSMS

This category presents the core aspects of the CSMS and comprises the system's requirements, scope, and details. The security policy, organization, and awareness element group discusses the development of cybersecurity policies and procedures, staff training, and business continuity planning.

The selected security countermeasures element group introduces the main types of Security Controls, such as Personnel Security, Physical Security, Network Segmentation, and Access Control.

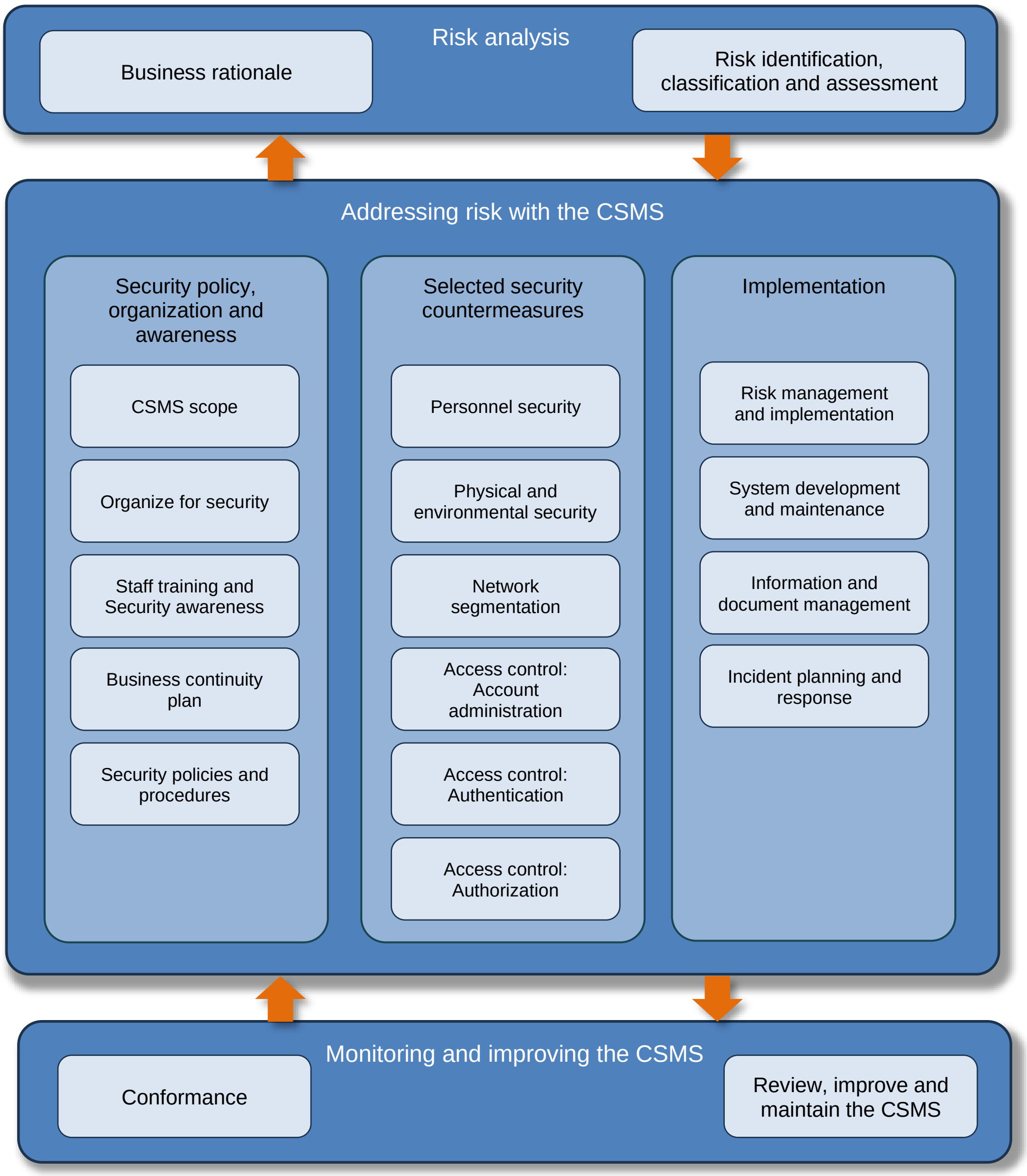
Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and Security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: Account administration
Access control: Authentication
Access control: Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS

Fig. 2 - ISA/IEC 62443 Graphical view of elements of a cybersecurity management system
Source: Data from ISA/IEC-62443-2-1 (99.02.01)-2009

The CSMS implementation element group provides guidance on selecting, developing, and implementing countermeasures to operate and maintain an effective cybersecurity program. These technical and administrative countermeasures ensure that the organization's desired risk tolerance level is continuously maintained. This includes maintenance practices and management of changes to existing systems, as well as the development of new systems.

A key component to addressing risks with a CSMS is incident response planning. Organizations should establish a cross-functional team comprising IT, OT, operations, and management personnel. This team should identify critical assets within the flow measurement system, including key devices such as flow meters, flow computers, and supervisory components. Incident categories specific to the domain, such as loss of view, loss of control, and lost and unaccounted-for measurements, should be defined. Clear roles and responsibilities for each team member during an incident must be established.

The incident response plan should encompass elements such as:

- Incident detection and reporting procedures.
- Containment and mitigation strategies.
- Recovery and system restoration procedures.

Regular testing and refinement of the plan are essential. This includes:

- Conducting and documenting tabletop exercises simulating various incident scenarios.
- Performing periodic drills involving both IT and OT teams.
- Updating the plan based on insights gained from exercises and actual incidents.

The incident response plan should be integrated with the measurement system's existing change management, maintenance plans, and backup procedures. Procedures for securely storing and accessing system backup, documentation, and network diagrams needed during an incident should be developed.

4.1.3 Monitoring and Improving the CSMS

The element group provides guidance on the requirement for conformance audits and periodic assessments to ensure that the developed CSMS is followed. The CSMS should be periodically evaluated and improved to ensure that it meets the evolving cyber threats and regulatory requirements. The following activities can assist in the risk re-assessment:

- Review the cybersecurity incidents since the last assessment.
- Review the cybersecurity-related system modifications since the last assessment.
- Review current vulnerabilities based on the product’s lifecycle and manufacturer’s notifications.
- Review changes in the relevant regulations and threats.

4.2 NIST Layered Security (Defense-In-Depth)

Several emerging technological trends and the associated concerns are set to impact ICS cybersecurity significantly. These include the Industrial Internet of Things (IIoT), Cloud Computing, and Big Data analytics tools, which significantly increase the integration between IT and OT as organizations adopt these new advances. Organizations can strengthen their overall cybersecurity by deploying systematically layered security controls, including administrative and technical measures. NIST describes a Defense-in-Depth (DiD) approach [20] depicted in Fig. 3; it aims to provide redundancy in case one layer fails, ensuring the system's overall security. Defence-in-depth layers can be classified into five security layers, as detailed in the following sections.

4.2.1 Layer 1 – Security Management

The security management layer comprises the core administrative activities required for cybersecurity program development and risk management. These activities start with building the business case, defining the strategy, developing the policies and procedures, creating an incident response plan, and developing cybersecurity awareness across the organization.

For flow measurement systems, controlled maintenance procedures are usually in place to detail the activities performed on the system. These should be extended to cover policies and procedures required for access control, including authentication and authorization mechanisms and role-based access principles.

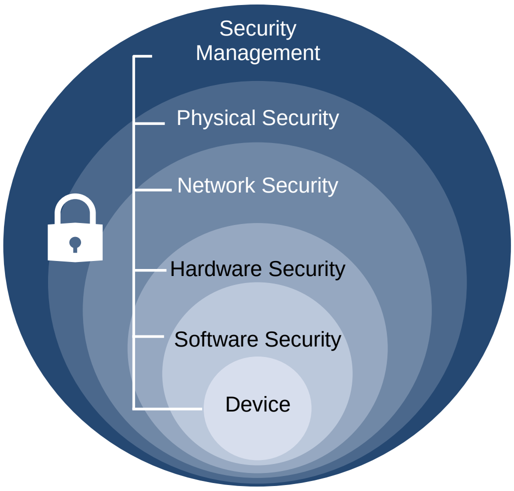

Fig. 3 - Defense-in-Depth Security Layers

An incident response plan should be developed and include procedures tailored to the flow measurement system, such as:

- Protocols for managing incidents affecting flow computers and flow meters with digital communication interfaces (e.g. unauthorized changes).
- Backup measurement nodes, measurement continuity, and mis-measurement handling.
- Criteria for isolating flow measurement system components during an incident, balancing security with regulatory and operational requirements. For example, flow computers with pulse, analog, or point-to-point serial interfaces could be disconnected from the network during an incident and still provide fiscal reporting and control functions.

Training and cybersecurity awareness programs for metering technicians and operation personnel are essential for a comprehensive DiD strategy.

4.2.2 Layer 2 – Physical Security

This layer comprises measures to secure physical access to critical systems and infrastructure using doors, locks, security personnel, and other measures. All computing and networking equipment should be locked in secured areas when access is not required. Access monitoring and surveillance systems should be deployed to record any unauthorized access. Physical security systems may include different types of access control and surveillance methods, such as security cameras, alarm systems, ID card scanners, and biometric security systems.

4.2.3 Layer 3 – Network Security

This includes adopting network segmentation and isolation, centralized logging, and network monitoring principles.

- **Network Segmentation:** In this approach, the ICS devices are grouped into zones with different security levels. Data flows in and out of the security zones through a particular type of security zone called conduits. Network devices with traffic enforcement capabilities, such as managed switches, routers, firewalls, and unidirectional gateways or data diodes, can be utilized to achieve network segmentation and isolation [20]. The flow measurement system may be integrated into the existing ICS network and cybersecurity infrastructure or designed as a standalone system. Deployment of the necessary network security devices can be decided based on the network architecture.

- **Events Logging:** Modern network devices log events relevant to security for monitoring and incident response analysis. When troubleshooting a problem, it’s usually required to correlate events from multiple log sources. A centralized log management system supports records retention and facilitates log analysis. However, whether a centralized log management system is required depends mainly on the risk assessment and network size. Considering a standalone flow measurement system with two supervisory systems, installing a centralized logging system may not be justified.

- **Network Monitoring:** Network monitoring includes tracking the network activities to detect and potentially respond to issues. This process is supported by several tools, including Behavior Anomaly Detection (BAD) systems to detect abnormal behavior, Intrusion Detection Systems (IDS) to monitor the network for malicious activities, and Intrusion Prevention Systems (IPS) to detect malicious behaviors and take actions to prevent it based on pre-identified rules. Considering the cost of installing and managing some of these tools in a flow measurement system, their deployment should be based on the risk assessment.

4.2.4 Layer 4 – Hardware Security

Hardware security capabilities improve endpoints to meet specific functional and security needs. These needs include device identity, endpoint hardening, integrity protection, and access control to establish the device's trust. For example, unused ethernet or USB ports in the metering supervisory computers and ethernet switches should be blocked.

4.2.5 Layer 5 – Software Security

The utilization of software security measures aims to bolster endpoint security. These measures include:

- **Application Whitelisting:** Application whitelisting allows only authorized applications to run on the host and restricts the usage of any resources to those approved. Application whitelisting agents can be deployed to the flow measurement nodes as either managed or standalone, based on the system architecture.

- **Patching:** Software should be updated and patched regularly to fix vulnerabilities. However, deploying patches to OT environments requires additional testing and validation to ensure that the patches do not impact the ICS functionality. Organizations should examine the applicable security patches and make an informed decision about addressing the identified vulnerabilities. Please refer to Fig. 4, for the patch management decision tree presented in the Control Systems Security Program, DHS [20].

  Patches should be tested on a test bench whenever possible before being deployed into the online system. Based on the flow measurement system size and the system architecture, patches can be updated locally or pushed through a dedicated Patch Management Server.

- **Configuration Management:** These measures involve both configuration security and application hardening. It comprises implementing access controls to limit access or enabling encryption to safeguard data both at rest and in transit. For example, OPC UA should be deployed for client-server communication, where possible, as a replacement for the OPC DA because of its built-in security features.

  Application hardening measures could include blocking specific network ports, application features, or unnecessary services from running on the system.

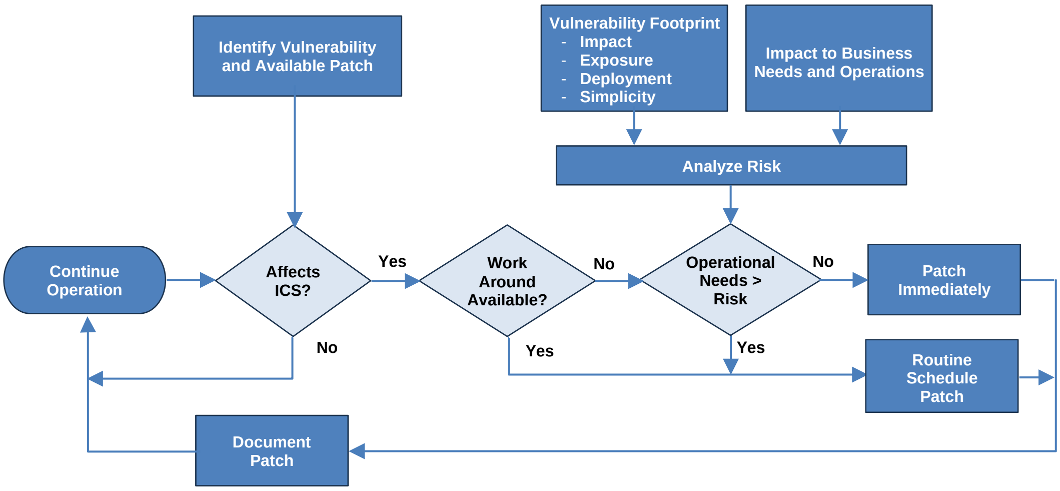

Fig. 4 - Patch management decision tree - Control Systems Security Program, DHS

5 CYBERSECURITY REQUIREMENTS FOR FLOW MEASUREMENT SYSTEMS

Given the nature of flow measurement applications, where data integrity and confidentiality are critical, enforcing the necessary cybersecurity controls is imperative without compromising the system's availability. A risk assessment should determine the measures needed to reduce the cybersecurity risks to an acceptable level for the organization. Regulatory bodies should weigh the cost implications of mandating higher security measures, particularly when such measures may not be justified. For example, compliance with NIST or ISA/IEC 62443 Security Level 1 on a flow measurement system with limited throughput might not be warranted, considering the significant capital and operational costs involved and the increased system footprint, which is especially concerning in offshore installations.

With most of the relevant measurement standards and local regulations lacking specific cybersecurity guidance and mandates, reaching a consensus on what would be considered baseline requirements for flow measurement systems that organizations can consider when designing and deploying measurement systems is necessary. Baseline controls defined in this paper are intended to protect the measurement system against basic threats as defined in the API 1164 [21] and comprise a deliberate attack that is simple, low-resourced, and doesn't leverage any specific skills in addition to unintentional or continental security violations.

5.1 Security Management and Risk Controls

The security risk assessment process, as outlined in ISA/IEC 62443-3-2 [19], begins with conducting an initial risk assessment. ISA/IEC 62443-3-2 suggests partitioning the system under consideration (SUC) into zones and conduits. A security zone refers to an operational asset group or a collection of groups with common security requirements enclosed within a logical boundary based on risk or function. For instance, in a typical custody transfer metering system—located primarily at Levels 0, 1, and 2 of the Purdue model, where Level 0 includes smart field instruments, Level 1 comprises the flow computers and PLCs, and Level 2 hosts the metering HMI—a similar partitioning approach is applicable.

ISA/IEC 62443-3-3 [22] defines seven Foundational Requirements (FRs), refer to Fig. 5, each associated with specific System Requirements (SRs) and Requirement Enhancements (REs). These requirements are designed to help achieve the Target Security Level (SL-T) necessary to meet the identified security needs. The outcome of the risk analysis includes a Zone and Conduit model alongside associated Risk Assessments and Target Security Levels (SL-T). The relevant FRs and proposed baseline SRs are summarized in APPENDIX A.

A custody transfer metering system may be located in a distinct zone with conduits linking it to the broader process system or split across multiple zones.

Furthermore, as indicated in the previous sections, detailed procedures should be developed to manage the identified cybersecurity risks; such procedures typically include the incident response plan, operating procedures, staff training, and regular assessments.

Foundational Requirements (FRs):	
FR1	Identification and Authentication Control (IAC)
FR2	Use Control (UC)
FR3	System Integrity (SI)
FR4	Data Confidentiality (DC)
FR5	Restricted Data Flow (RDF)
FR6	Timely Response to Events (TRE)
FR7	Resource Availability (RA)

Fig. 5 - ISA/IEC 62443 Foundational Requirements

5.2 Physical Security

Physical controls include securing the location of the flow measurement systems' equipment and controlling the physical access to them in the field and control room. For example, desktop-mounted metering supervisory computers should be avoided and replaced with rack-mounted servers installed in cabinets secured with physical locks and physical tamper detection, or virtual machines where feasible. This supports implementing account management (SR 1.3), authenticator management (SR 1.5), and system use notification (SR 1.12). Furthermore, physical security acts as the first layer to ensure the integrity of communication (SR 3.1).

5.3 Network Security

To establish network security and satisfy the baseline requirements, the legacy metering system architecture indicated in Fig. 1 can be revised. The components in the revised architecture, indicated in Fig. 6, work in synergy to fulfill the security requirements and defense-in-depth strategy.

5.3.1 Firewalls

Firewalls enforce network segmentation (SR 5.1) and zone boundary protection (SR 5.2), ensuring that communications between different zones are tightly controlled and monitored. This also includes restricting general-purpose person-to-person communications (SR 5.3).

For flow measurement systems, there are some key considerations when determining the segments, which should be selected based on the level of criticality and the exposure to potential threats. An argument could be made for three segments within a flow measurement system: one for the field devices, one for the flow computers and PLCs, and one for the metering supervisory computers; indeed, outside of flow measurement, this is considered by some to be best practice [23], [24].

Adding firewalls or other protective equipment between the flow computers and field devices (such as velocity from ultrasonic flow meter via Modbus TCP/IP) could impact the latency and calculation cycle time of the flow computers and, hence, may not be prudent in a baseline system. Flow computers can, in some cases, be set up to provide independent control and reporting of fiscal and other critical measurement systems without the need for the supervisory computer to be connected. This would suggest that allocating two network segments to a typical flow measurement system may be warranted. This design becomes crucial during a DoS attack to satisfy denial of service protection (SR 7.1).

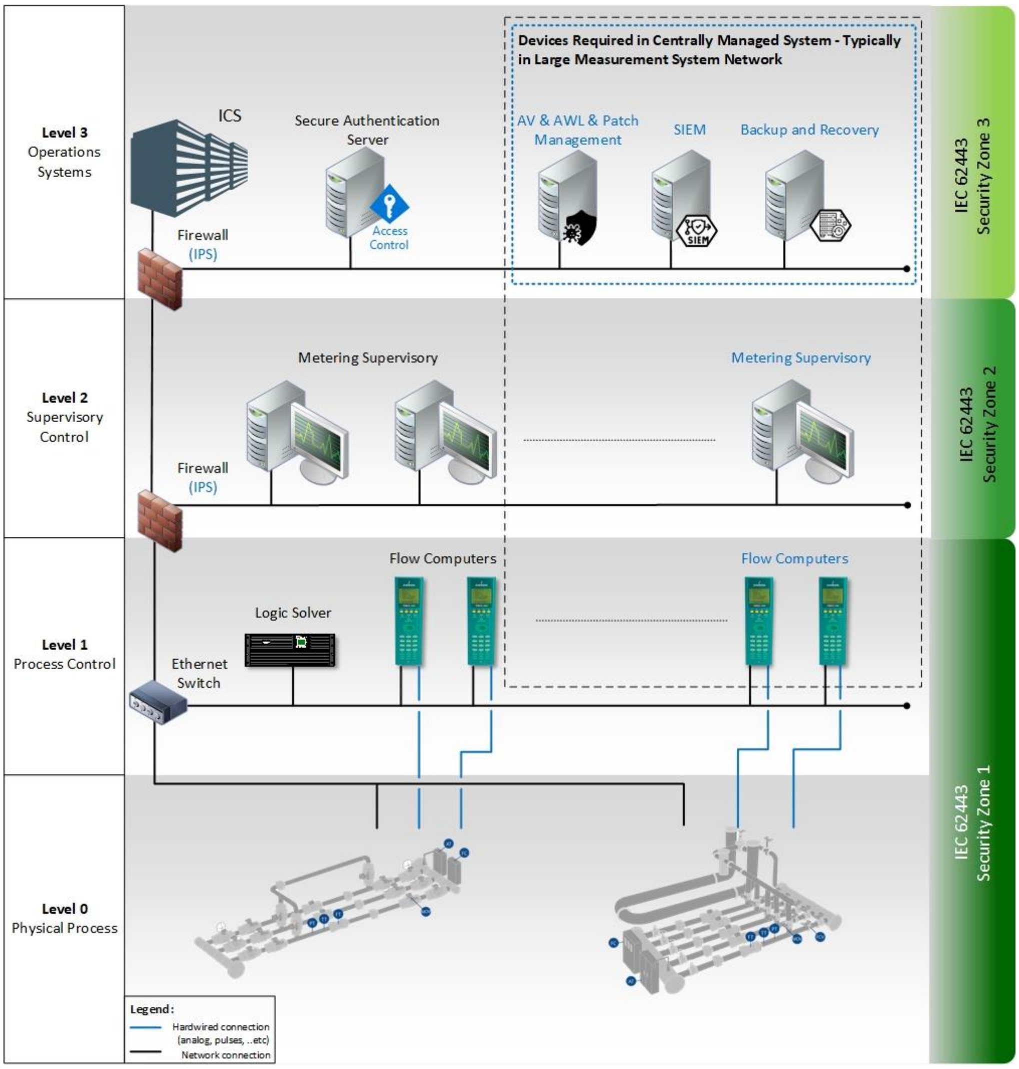

Fig. 6 - Sample Implementation of Cybersecurity Countermeasures in Modern Metering System Architecture*

** Items in blue are for complex systems and are subject to risk assessment*

5.3.2 Intrusion Prevention System (IPS)

IPS systems detect and prevent unauthorized access and attacks within the network, supporting requirements for malicious code protection (SR 3.2) and continuous monitoring (SR 6.2). Note that many Next Generation Firewalls (NGFW) include IPS as a service; however, they can be complex to configure initially and to manage on an ongoing basis. False positives can result in the system communications being shut down, a critical risk we wish to avoid; therefore, IPS is not part of the baseline recommendation for simple flow measurement systems.

5.3.3 Centralized Authentication Server

These servers manage authentication across the network, handling human user identification and authentication (SR 1.1), account management (SR 1.3), identifier management (SR 1.4), and authenticator management (SR 1.5). It would also address wireless access management (SR 1.6) and enforce strong password-based authentication (SR 1.7) in addition to imposing authenticator feedback (SR 1.10) and unsuccessful login attempts (SR 1.11) policies.

Legacy approaches to flow measurement systems typically have local usernames and passwords managed by the supervisory system and/or the devices themselves. As discussed earlier, this can result in weak passwords and unnecessary user accounts, potentially including administrator accounts left during the initial configuration. Therefore, centralized authentication is a baseline requirement.

Multi-factor authentication can be impractical in some flow measurement systems, given the restrictions of carrying mobile devices on many sites – preventing push notifications or the difficulty with fingerprint sensors in dirty environments, for example, in local equipment rooms. Based on the risk assessment, multi-factor authentication may be a prudent inclusion, especially where access is from an office-style environment, and is recommended where practical.

5.3.4 Security Event Audit Management

Dedicated and sophisticated Security Information Event Management (SIEM) systems centralize the collection, analysis, and storage of audit logs (SR 6.1), support auditable events (SR 2.8), and ensure audit storage capacity (SR 2.9). This component helps ensure timely responses to events, thereby maintaining overall system security.

The downside of a dedicated SIEM system is the cost, which can run into hundreds of thousands of dollars; hence, deploying such systems will be subject to risk analysis. On a typical metering system, it is sufficient to enable Windows Event Logs (or equivalent), and this forms the baseline recommendation.

5.3.5 Network Access Control (NAC)

NAC manages and controls access to the network, enforcing access control policies based on device identity and security posture. This supports authorization enforcement (SR 2.1) and mobile/portable device control (SR 2.3). The key features of NAC are:

- Authentication: Verifying the identity of devices and users before allowing access to the network.
- Authorization: Ensuring that only authorized devices and users can access specific network resources.
- Posture Assessment: Checking the security status of devices (e.g., antivirus, patches) before they can connect.
- Remediation: Redirecting non-compliant devices to remediation networks or services to bring them into compliance.
- Monitoring: Continuous monitoring of devices and users on the network for suspicious or unauthorized activities.

Once again, these solutions (hardware or software) can be expensive and complex to configure and manage. NAC can be a worthwhile option on large, critical, or high-risk flow measurement systems, but this would not form part of the baseline requirements for typical systems.

5.4 Hardware Security

Endpoint hardening and blocking unused ethernet or USB ports should be implemented in the metering supervisory computer and ethernet switches; this helps in implementing the least functionality principle (SR 7.7).

The hardware used in the measurement system network should be sourced from trusted vendors to mitigate the risk of supply chain attacks, where malicious actors compromise the system by tampering with hardware or software during manufacturing, distribution, or delivery through a third-party supplier.

5.5 Software Security

5.5.1 System and Application Whitelisting

These solutions help to meet the requirements of malicious code protection (SR 3.2), ensuring systems are protected from malware and other malicious code.

Where the flow measurement system supports whitelisting as part of the standard feature set, this should enabled; however, for baseline purposes, a dedicated whitelisting package is not a requirement.

5.5.2 Protocol Selection and Data Encryption

As discussed earlier, Modbus is not a secure communication protocol, and it is increasingly being targeted as a vulnerable attack vector. Many field devices still rely on Modbus as the primary means of transferring process information; where possible, Modbus should be replaced with more modern and secure protocols such as Open Platform Communications Unified Architecture (OPC UA), Advanced Message Queuing Protocol (AMQP), and Message Queuing Telemetry Transport (MQTT). Modern protocols support encryption using SSL/TLS, authorization using tokens or certificates, authentication using access control lists/policies, and role-based access, making them a far more secure choice for interfaces in metering systems.

Data encryption ensures information confidentiality (SR 4.1) during transmission, particularly when data is sent across less trusted networks or between zones. The downside of encryption is the requirement for all devices in the chain to be able to handle the protocols themselves and the certificates associated with encryption.

As a baseline recommendation, Modbus should be avoided as the initial step; self-signed certificates can be an optional addition, where practical as a second step, and finally, for systems where the risk assessment justifies the complexity and costs, third-party signed certificates can be used.

5.5.3 Anti-Malware/Endpoint Protection and System Patching

Anti-malware is deployed on critical systems at Level 1 to provide malicious code protection (SR 3.2) and verify security functionality (SR 3.3) across all systems. This component helps maintain system integrity by preventing and detecting malware.

Anti-malware is an essential baseline requirement, and for most flow measurement systems, simple endpoint protection with a recognized package is sufficient. Centralized, managed options can always be considered where the justification exists.

The initial risk assessment should include an investigation and recommendation on how often this software should be updated. It should also consider patching frequency and testing requirements for general software updates to the devices and supervisory computers.

5.5.4 Backup and Recovery Systems

These systems ensure control system backup (SR 7.3), recovery and reconstitution (SR 7.4), and support for emergency power (SR 7.5). This involves both data and configuration backups, as well as disaster recovery plans.

Dedicated backup and recovery systems can be expensive, and for most flow measurement systems, which comprise few servers, a simple manual process is sufficient for baseline purposes. These backups can be stored in digital format on company assets and be subject to standard company recovery policies.

Care should be taken to include all configuration data and reports within the scope of the backups to simplify the recovery process. This should also include network configuration and device settings to protect against unintentional misconfigurations by users, satisfying a basic level of (SR 7.6).

5.5.5 Input Validation

All user interfaces in the system, including the flow computer (via web browser, front panel, or other dedicated user interfaces) and the supervisory computers, must implement robust input validation to prevent injection attacks and other input-based vulnerabilities (SR 3.5).

Given that flow supervisory systems often rely on structured databases with Structured Query Language (SQL) querying, they can be particularly vulnerable to SQL injection attacks. Proper input validation and sanitization (for example, removal of SQL keywords) must be enforced to mitigate these risks and ensure data integrity.

5.6 Secure Remote Access

In modern flow measurement environments, remote access capabilities have become increasingly necessary for efficient operations, maintenance, and support. However, these remote connections can introduce significant security risks if not properly managed.

Remote access can be granted for performance monitoring and troubleshooting through an outbound Virtual Private Network (VPN) connection using a secure cloud-based infrastructure that supports the security key components, including physical security, multi-factor authentication (MFA), user identification and authentication (SR 1.1), device identification and authentication (SR 1.2), role-based access control (SR 2.1), and audit logs (SR 6.1).

Organizations should implement MFA and establish a robust process for approving and managing remote access privileges, ensuring adherence to the principle of least privilege. This aligns with (SR 1.13), ensuring that all remote access attempts from untrusted networks are subject to stringent authentication and authorization checks.

Using VPNs with strong encryption is recommended, alongside the consideration of dedicated remote access gateways or jump servers to provide an additional layer of security and control. These solutions should be configured to meet the requirements of (SR 5.2) for zone boundary protection, effectively isolating the flow measurement environment from potential external threats.

Session management and monitoring are critical components of secure remote access. Implementing session timeouts and automatic disconnection of idle sessions, as per (SR 2.6), helps mitigate the risk of unauthorized access through abandoned sessions. Furthermore, comprehensive monitoring and logging of all remote access sessions, including user activities, provide valuable data for security analysis and incident response. Real-time alerting for suspicious remote access activities enhances the organization's ability to promptly detect and respond to potential security threats.

The security of the remote access infrastructure itself cannot be overlooked, and remote access routes should be carefully segmented to ensure they do not impact the core measurement data flows. Regular patching and secure configuration of all systems and components involved in remote access, such as VPN concentrators and firewalls, are essential. Organizations should implement a process for regular security assessments of the remote access infrastructure to identify and address potential vulnerabilities proactively.

Given the security concerns surrounding remote access, the risk assessment should include careful quantitative as well as qualitative reasoning around whether remote access is necessary, for example:

- How difficult would it be to mobilize technical support to the site versus the implications of the system being down for a period of time?
- Is there a significant logistic burden to deploy a technician physically to the site? Is there any safety or security constraints?
- How often is remote support anticipated?
- Could the necessity of remote support be reduced through increased training for the operators? For example, could highly trained operators meet at least some of the most likely support needs in conjunction with telephone support?
- If remote access is necessary, what degree of control will be granted – read/write versus read-only? Will local operator supervision be required for every remote access session?

In modern flow measurement systems, operators are more likely to consider and be receptive to remote operations, given the potential benefits in terms of safety and costs associated with not having personnel on site. Hence, one possible compromise would be to have the flow measurement system capable of remote operation within the operator’s network, i.e., not via the Internet. This would allow the operator to implement remote operations from a centralized location or locations where support staff could leverage that link without necessarily having to travel to the site.

5.7 Centralized Versus Decentralized Approach

When considering cybersecurity solutions, the choice between centralized and decentralized systems can significantly impact the cybersecurity strategy. Centralized cybersecurity solutions, where the implemented security tools are managed from a single dedicated platform, allow for a unified approach to security management, making enforcing policies across multiple systems easier and simultaneously reducing the cost and redundancies associated with resources and tools. For example, a new measurement system could be integrated into the existing plant's cybersecurity infrastructure. Otherwise, the cost of dedicated cybersecurity tools can significantly increase the cost of the measurement system.

The drawback of such an approach can be the scalability issues of the cybersecurity infrastructure, which may become a bottleneck as the organization grows. Also, the integration challenges of a new system to an existing infrastructure will require a thorough assessment by the Original Equipment Manufacturer (OEM) to ensure the compatibility of the existing cybersecurity solutions with their systems.

On the other hand, decentralized cybersecurity tools may be customized to address specific security needs and offer better resilience if one system in the plant network is compromised. However, managing multiple isolated systems can be more complex and resource-intensive, in addition to the challenges of ensuring consistency of the security policies across all the systems.

6 CONCLUSION

In the evolving digital landscape of the oil and gas industry, the cybersecurity of flow measurement systems has emerged as a critical concern. As these systems increasingly integrate with broader network infrastructures, the traditional isolation that once provided a semblance of security is no longer sufficient. The shift toward more interconnected and digitalized environments exposes these systems to a multitude of cybersecurity vulnerabilities, ranging from unauthorized access and protocol vulnerabilities to advanced persistent threats.

This paper has highlighted the pressing need for a cohesive, standardized approach to securing flow measurement systems. Organizations can better protect their critical measurement infrastructure by implementing industry standards such as ISA/IEC 62443 and NIST CFS and by adopting robust cybersecurity management systems. Adopting a defense-in-depth strategy, which includes layered security controls, network segmentation, and comprehensive incident response planning, is essential to mitigate risks and enhance resilience.

Regulatory frameworks and standards, while varied, offer a foundational baseline that can be adapted to the specific needs of flow measurement systems. As the regulatory environment evolves, ongoing collaboration between industry stakeholders, standards bodies, and regulatory agencies will be paramount. This collaborative effort will ensure that cybersecurity measures remain robust, scalable, and adaptable to emerging threats.

In conclusion, securing flow measurement infrastructure in the digital age is not just a technical necessity but a strategic imperative. It requires a proactive approach, integrating best practices and continuous improvement to safeguard financial, legal, and operational stability. By prioritizing cybersecurity, the oil and gas industry can protect its assets, maintain trust, and ensure the integrity of critical measurement processes.

7 REFERENCES

[1] World Economic Forum Annual Meeting, Davos, Switzerland, 2022.

[2] A. Ribeiro, Colonial Pipeline incident helped reinforce cybersecurity across critical infrastructures, but still, a long way to go, Industrial Cyber, 2022.

[3] A. Ribeiro, Resecurity warns of rising ransomware threats in energy sector, particularly targeting nuclear, oil and gas industries, Industrial Cyber, 2023.

[4] A. Riberiro, Claroty’s Team82 finds path-traversal vulnerability in ABB TotalFlow flow computers and controllers, Industrial Cyber, 2022.

[5] A. Ribeiro, GAO reports offshore oil and gas infrastructure faces cybersecurity risks from threat actors, vulnerabilities, potential impacts, Industrial Cyber, 2022.

[6] J. A. S. A. Santiago Figueroa-Lorenzo, A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach, Multidisciplinary Digital Publishing Institute, October 2019.

[7] S. V. G. O. Tiago Martins, Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported, Multidisciplinary Digital Publishing Institute, 2022.

[8] A. Ribeiro, New Kaspersky ICS CERT report reviews Q1 APT, financial attacks on industrial enterprises, Industrial Cyber, 2024.

[9] C. A. K. O. Mark (Magpie) Graham, Impact of FrostyGoop ICS Malware on Connected OT Systems, Dragos Intelligence Brief, July 2024.

[10] A. Ribeiro, Claroty finds that over 70% of flaws remotely exploitable through network attack vectors, Industrial Cyber, 2021.

[11] Pipeline Security Guidelines, Transportation Security Administration, March 2018 (with Change 1 (April 2021)).

[12] Memorandum: Pipeline Cybersecurity Mitigation Actions, Contingency Planning and Testing, U.S Department of Homeland Security, July, 2023.

[13] Cyber Incident Reporting For Critical Infrastructure, United States Congress, Act of 2022.

[14] The Network and Information Systems Regulations, HM Government, 2018.

[15] National Cyber Strategy 2022- Pioneering a cyber future with the whole of the UK, HM Government, 2022.

[16] Directive (EU) 2022/2555 of The European Parliament and of The Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 (NIS 2 Directive), Official Journal of the European Union, 2022.

[17] The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, February, 2024.

[18] ISA/IEC-62443-2-1, Security for industrial automation and control systems, Part 2-1: Establishing an industrial automation and control systems security program, 2009.

[19] ISA/IEC-62443-3-2, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design, 2020.

[20] Guide to Operational Technology (OT) Security, NIST Special Publication NIST SP 800-82r3, National Institute of Standards and Technology, September 2023.

[21] Pipeline Control Systems Cybersecurity - API STANDARD 1164 - THIRD EDITION, AUGUST 2021.

[22] ISA/IEC-62443-3-3, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels, 2013.

[23] K. Kish, Tales From the Road: If Your SCADA Network Isn’t Segmented, It’s Not Secure, Direct Defense, 2021.

[24] SCADA Security Design – How to Secure OT / ICS Network Environments, S5 Technology Group, 2022.

APPENDIX A
BASELINE SYSTEM REQUIREMENTS

FR 1 – Identification and Authentication Control (IAC)

Identification and Authentication Controls ensure that only authorized users can access the system. The following SRs are recommended:

- SR 1.1: Human User Identification and Authentication – Ensures that every human user accessing the system is uniquely identified and authenticated.
- SR 1.3: Account Management – Manages user accounts to control access based on the user's role.
- SR 1.4: Identifier Management – Manages user identifiers (e.g., usernames) to prevent unauthorized access.
- SR 1.5: Authenticator Management – Manages authenticators (e.g., passwords) to ensure they are secure and regularly updated.
- SR 1.6: Wireless Access Management – Controls access to the system via wireless networks to prevent unauthorized connections.
- SR 1.7: Strength of Password-Based Authentication – Ensures passwords meet strength requirements to resist brute-force attacks.
- SR 1.10: Authenticator Feedback – Limits feedback to users during authentication to avoid revealing unnecessary information.
- SR 1.11: Unsuccessful Login Attempts – Implements controls to limit the number of failed login attempts to mitigate brute-force attacks.
- SR 1.12: System Use Notification – Notifies users of system use conditions to reinforce security awareness.

FR 2 – Use Control (UC)

Use Control ensures that once users are authenticated, their actions are authorized and monitored. The following SRs are recommended:

- SR 2.1: Authorization Enforcement – Enforces permissions to ensure users can only perform actions they are authorized to.
- SR 2.2: Wireless Use Control – Controls the use of wireless devices to ensure secure communication.
- SR 2.3: Use Control for Portable and Mobile Devices – Manages the use of portable devices to prevent unauthorized access or data leakage.
- SR 2.5: Session Lock – Locks sessions after inactivity to prevent unauthorized access when users are away.
- SR 2.8: Auditable Events – Defines which events should be audited to detect and respond to unauthorized activities.
- SR 2.9: Audit Storage Capacity – Ensures sufficient capacity for audit logs to facilitate effective monitoring and analysis.

FR 3 – System Integrity (SI)

System Integrity controls are designed to protect the system from unauthorized changes and ensure it functions as intended. The following SRs are recommended:

- SR 3.1: Communication Integrity – Protects the integrity of data in transit to prevent tampering.
- SR 3.2: Malicious Code Protection – Ensures systems are protected from malware and other malicious code.

- SR 3.3: Security Functionality Verification – Verifies that security functions are operating correctly.
- SR 3.5: Input Validation – Ensures that all inputs to the system are valid and safe, preventing injection attacks and other input-based vulnerabilities.

FR 4 – Data Confidentiality (DC)

Data Confidentiality ensures that sensitive information is protected from unauthorized access and disclosure. For flow measurement systems, while not all SRs may be applicable, SR 4. 1 is critical:

- SR 4.1: Information Confidentiality – Ensures that data is encrypted or otherwise protected to maintain its confidentiality during storage and transmission.

FR 5 – Restricted Data Flow (RDF)

Restricted Data Flow controls data movement between zones and within the system to ensure that it follows defined security policies. The following SRs are recommended:

- SR 5.1: Network Segmentation – Implements network segmentation to limit the spread of threats across the network and isolate sensitive parts of the system.
- SR 5.2: Zone Boundary Protection – Protects the boundaries between security zones to prevent unauthorized access or data leakage.
- SR 5.3: General Purpose Person-to-Person Communication Restrictions – Limits direct communication between users to reduce the risk of data leakage or unauthorized communication.

FR 6 – Timely Response to Events (TRE)

Timely Response to Events ensures that the system can respond promptly and effectively to security incidents. The following SR is recommended:

- SR 6.1: Audit Log Accessibility – Ensures that audit logs are accessible for review and analysis, facilitating quick detection and response to security events.

FR 7 – Resource Availability (RA)

Resource Availability ensures that the system continues to operate despite adverse conditions, such as attacks or failures. The following SRs are recommended:

- SR 7.1: Denial of Service Protection – Implements measures to protect the system from Denial of Service (DoS) attacks, ensuring continuous operation.
- SR 7.3: Control System Backup – Ensures that the system has up-to-date backups to recover from failures or attacks.
- SR 7.4: Control System Recovery and Reconstitution – Defines processes for recovering and reconstituting the system after an incident.
- SR 7.5: Emergency Power – Ensures the availability of power during emergencies to maintain system operations.
- SR 7.6: Network and Security Configuration Settings – Manages network and security settings to ensure they are secure and consistent with security policies.
- SR 7.7: Least Functionality – Limits the functionality of the system to only what is necessary, reducing potential attack surfaces.