Securing The Forgotten Link: Selecting and Evaluating Compensating Security Measures for Legacy Device Integration Paths

Sabrina Kaniewski[1 [009−0004−3966−9681]], Nils Lohmiller[1 [0009−0008−1301−4002]], Michael Menth[2 [0000−0002−3216−1015]], and Tobias Heer[1 [0000−0003−3119−252X]]

[1] Institute for Secure Networked Systems, Esslingen University, Germany
{sabrina.kaniewski,nils.lohmiller,tobias.heer}@hs-esslingen.de
[2] Chair of Communication Networks, University of Tübingen, Germany
menth@uni-tuebingen.de

Abstract. A common solution to integrating older devices without state-of-the-art security features, i.e., *legacy devices*, in industrial networks is the use of security gateways. The gateway sits between the legacy device and the network and can enforce security features such as authentication and encryption. However, the gateway secures only the communication on the network side but does not mitigate the absence of security features in the legacy device. Consequently, the link connecting the legacy device to the gateway, which we refer to as *legacy link*, remains vulnerable and unaddressed. In this work, we provide a systematic analysis of compensating security measures to address this vulnerable legacy link. We examine physical, technical, and operational measures, assessing their ability to prevent or detect physical tampering and unauthorized access to communication. For a structured comparison of their effectiveness, we introduce an evaluation framework that considers detection properties, applicability specifics, costs, attack mitigation, and adherence to security controls from international standards (i.e., ISO/IEC 27002 and IEC 62443). Using this framework, we discuss two use cases to demonstrate how practitioners can derive complementary measures to form minimal yet effective security concepts tailored to specific environmental and regulatory constraints. This work supports practitioners in enhancing the secure integration of legacy devices in diverse industrial domains.

Keywords: Cyber-physical systems security · CPS · SCADA · Brownfield networks · Network security · Security controls.

1 Introduction

Industrial networks, e.g., Cyber-Physical Systems (CPS) and Supervisory Control and Data Acquisition (SCADA) systems, are increasingly targeted by attacks. These networks often contain older devices that do not implement state-of-the-art security features or do so only insufficiently, so-called *legacy devices*. Due to high acquisition costs and long amortization periods, replacing legacy devices is often

Accepted for publication in Proceedings of *21st International Conference on Availability, Reliability and Security (ARES)*, Linköping, Sweden, August 24-27, 2025.

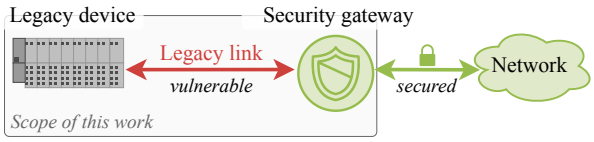

Fig. 1. Scope of this work: the *legacy link* connecting the legacy device and the security gateway remains vulnerable.

impractical. Retrofitting is often infeasible due to complex re-certifications. This mismatch creates a contradiction between the increasing security requirements in critical networks (e.g., by the NIS2 Directive and the Cyber Resilience Act) and the outdated but irreplaceable legacy devices. It remains an open question how to integrate legacy devices securely within today's networks.

A common solution to integrating legacy devices is to place them behind a security gateway, which implements critical security features, e.g., authentication and encryption [4,9,11]. However, while the gateway secures communication toward the network, it does not solve the absence of security features on the legacy device side. Rather, unsecured communication is limited but persists on the *legacy link*, i.e., the link connecting the legacy device to the gateway, see Fig. 1. As the legacy link remains vulnerable, it still poses an attack vector. An attacker can exploit access to the legacy link and, e.g., embed a malicious device to perform message fabrication, possibly disrupting operations or compromising the security of the entire network. However, this legacy link is often treated as out of scope. To securely integrate and operate legacy devices, we require additional compensating measures to secure the vulnerable legacy link.

Different physical, technical, and operational measures can be applied to secure the legacy link, e.g., access control lists to filter traffic at the gateway, or enclosures to prevent physical access. However, given the diversity of device types and deployment environments (e.g., manufacturing, energy, or railway), determining which measures are most effective remains a challenge. Thus, a framework is required to support the comparison and selection of suitable measures.

In this work, we present and categorize diverse compensating measures to secure the legacy link. To enable a structured comparison, we introduce a set of evaluation criteria, including detection properties, applicability specifics, costs, attack mitigation, and adherence to standard controls. We outline a framework that allows for the selection of evaluated measures. This framework supports practitioners in selecting an appropriate combination of measures that sufficiently secures the legacy link while considering specific constraints and requirements of the deployment context. The main **contributions** of this work are as follows:

- We systemize diverse physical, technical, and operational compensating security measures to enhance the secure integration of networked legacy devices.
- We derive and apply evaluation criteria aligned with representative attack types and international security controls (ISO/IEC 27002 and IEC 62443) for a structured evaluation of measures.

– We present a framework that provides a systematic tool for comparing different compensating security measures and identifying a suitable combination to secure the legacy link in a given use case.

The remainder of this work is structured as follows. In Section 2, we detail the scope of the legacy link. Section 3 presents compensating security measures. Section 4 outlines the evaluation framework, including the evaluation criteria and attack model. In Section 5, we demonstrate the application of the framework using two representative use cases, and, in Section 6, we discuss how to extend the framework. Section 7 discusses related work. We conclude this work in Section 8.

2 Scope: Legacy Link

IP- and Ethernet-based networked industrial legacy devices frequently communicate using protocols such as MODBUS/TCP in process control systems, DNP3 in electric or water utilities, or EtherNet/IP and PROFINET in factory and process industries. In their base variants, these protocols offer no built-in support for integrity, authentication, or confidentiality. Although security extensions for these protocols have been proposed (e.g., Modbus/TCP Security or DNP3 Security), their adoption is optional and often infeasible for deployed systems. In practice, implementing such extensions would require device replacement, entailing downtime and costly re-certification efforts. If a device requires further security, a security gateway is often added rather than replacing the still functional device.

A gateway serves as a connection point to the network. It can authenticate to upstream networks, enforce encryption, and provide additional functions such as logging or firewalling. Crucially, these security features terminate at the network interface of the gateway. Communication on the legacy link, i.e., the physical and logical connection between the device and gateway, remains unauthenticated and unencrypted. We consider the following objectives for securing the legacy link:

– **Availability**: the legacy device's services must remain continuously available;
– **Integrity**: unauthorized communication by a device other than the legitimate legacy device must be mitigated; and
– **Confidentiality**: communication over the legacy link must be protected from unauthorized observation and disclosure.

As legacy devices typically expose no cryptographic identity and offer only the limited functionality they were designed with, any verification of who is connected to the gateway must rely on characteristics available on or near the legacy link (e.g., link state transitions, device fingerprints, traffic patterns, or physical connectors). These constraints motivate the need for compensating measures that secure the legacy link without modifying the legacy device. We further set three practical requirements to be met by compensating measures to ensure applicability across diverse legacy device types and domains: *protocol-agnosticism*, i.e., measures should not depend on specific application-layer protocols; *standard-compliance*, i.e., measures should align with established industrial security controls to support use in regulated environments such as a utility facility; and *cost-effectiveness*, i.e., measures should operate with acceptable maintenance effort.

3 Security Measures

This work aims to provide a framework for selecting suitable compensating security measures evaluated according to defined criteria that address the security objectives of the legacy link within a given deployment context. Depending on the specific technical or economic prerequisites of the deployment context, different measures may be appropriate for achieving the desired security objectives. For example, a security seal can indicate whether a device enclosure has been opened, while a link-down detection mechanism can reveal whether a cable has been unplugged. Although both measures serve a similar purpose, i.e., detecting physical tampering, their effectiveness and applicability may vary across deployment contexts, making a direct comparison difficult without suitable evaluation criteria. As a first step towards this framework, we contribute a (non-exhaustive) set of physical, technical, and operational compensating security measures, providing a structured foundation for their systematic evaluation and comparison.

3.1 Physical Measures

Physical measures are to be understood in addition to general physical controls, e.g., security perimeters or entry controls. Their role is to prevent or detect physical tampering with the legacy link, e.g., unauthorized cable unplugging.

P1 Cable Lock. Cable locks are designed to prevent the unauthorized removal of a network cable by physically securing it within, e.g., the Ethernet port. While cable locks hinder casual removal, physical tampering is not entirely prevented, as an attacker may still cut the cable.

P2 Enclosure. Enclosures physically encase the legacy device, its network connection, and the gateway. By restricting physical access, enclosures aim to prevent tampering with the legacy link. However, enclosures also introduce drawbacks. They hinder maintenance checks, reduce flexibility in accessing the device, and may be impractical in space-constrained or dynamically changing environments, e.g., when the device is often relocated.

P3 Security Seal. Security seals, e.g., label or pull-tight seals, provide a means to detect physical tampering. For example, label seals can be placed at the opening of an enclosure or the cable head. Gaining access to the network then requires breaking the seal, leaving a broken seal as visible evidence of tampering. Personnel performing routine checks can detect such broken seals, reporting unauthorized access. While simple and low-cost, seals are unsuited for contexts where devices are frequently unplugged or for rugged environments, as they can be accidentally broken or degrade over time.

P4 Sensor Monitoring. Sensor-based monitoring aims to detect physical tampering using, e.g., contact sensors, such as magnetic reed switches, that detect state changes. A sensor can be installed inside an enclosure, where an opening triggers a change in the monitored state, or at cable ends, sensing when a cable is unplugged. The gateway can continuously monitor these sensor signals, enabling automated detection of tampering events and the generation of alerts that are forwarded to a centralized monitoring system.

3.2 Technical Measures

Technical measures describe network and system-level mechanisms that can be implemented at the security gateway to prevent or detect unauthorized logical access. These measures may operate at different layers of the protocol stack, ranging from link-layer MAC filtering to application-level device fingerprinting.

T1 Access Control List. Access control lists (ACLs) at the gateway are a preventive measure to restrict communication by filtering packets, e.g., for specific network addresses. By configuring ACLs at the gateway to permit only packets from the legitimate legacy device, unauthorized devices are prevented from passing communication to the network. However, ACLs are not impenetrable. Attackers may eavesdrop on communication and spoof network addresses to match those of the legacy device, thereby bypassing the filter.

T2 Link-down Detection. Link-down detection monitors the physical interface state of a port. If the legacy link is cut or unplugged, e.g., to insert an unauthorized device, the interface state at the legacy device and the gateway changes to `down`. Monitoring for and logging such events at the gateway enables detection of unauthorized disconnection or tampering. Link-down detection is, however, unsuitable in use cases where the legacy device is frequently disconnected as part of regular operations, as this would generate a high number of false alerts.

T3 IP-ID Monitoring. IP-ID monitoring, as proposed by Kaniewski et al. [10], considers characteristics at the network layer, specifically the IPv4 Identifier header field (IP-ID) used for fragmentation. Common assignment behaviors in legacy devices include a global counter, which assigns IP-IDs sequentially for all streams. By focusing on the device-specific IP-ID assignment behavior of the legacy device, IP-ID monitoring allows to distinguish packets sent by the legacy device from packets sent by an unauthorized device. By observing the assignment in packets arriving at the gateway, it is possible to verify the expected behavior of the legacy device. Deviations from the expected behavior may indicate the presence of an unauthorized device sending packets into the network and can be reported by the gateway, functioning as a lightweight intrusion detection system.

T4 Reachability Test. The gateway can actively verify the availability and responsiveness of the legacy device by sending ICMP echo requests (pings) that are responded to with echo responses. By monitoring both the presence and timing of these responses, the gateway can detect anomalies in the device's communication behavior. Deviations from expected response times may indicate the presence of an unauthorized embedded device that inspects, forges, or delays network traffic. Since all traffic of the legacy device passes through the gateway, processing and forwarding delays introduced by such an embedded device increase the overall response time observed at the gateway. However, timing-based detection has significant limitations. Establishing a reliable baseline for the average response time and selecting an appropriate reporting threshold require extensive application-specific traffic data. For devices with high or variable traffic loads, response times may naturally exhibit high variance, complicating threshold selection. Moreover, the delays introduced by embedded devices depend on both the attack scenario and the specific hardware used, limiting general applicability.

A poorly chosen threshold may lead to false alarms or even no alarms despite the presence of an embedded device.

T5 Connectivity Test. The gateway can actively verify the connectivity of specific application services of the legacy device that operate over TCP by performing TCP SYN scans. By probing all services implemented on the legacy device, i.e., scanning its open ports, the gateway can determine whether all expected services are available. If certain services are unreachable, this may indicate that the legacy device is offline or that an unauthorized device, which does not implement these exact services, is connected to the gateway and, therefore, responds with closed ports. The set of open ports effectively serves as a fingerprint of the legacy device, reflecting its unique configuration and functional profile.

T6 Identification Request. Identification requests retrieve information specific to the legacy device. Various application protocols in the field of process automation, such as MODBUS/TCP or EtherNet/IP, but also configuration protocols, e.g., SNMP, implement requests that allow devices to be queried for identity-related information, e.g., device type, product code, or a serial number. The gateway can implement such a request and compare the received response against the expected response to confirm the identity of the connected device.

3.3 Operational Measures

Operational measures describe means that involve human interaction. In particular, operational measures can enable security incident reporting for measures that do not provide reporting means, such as physical measures.

O1 Visual Check. Visual checks rely on personnel to inspect the legacy link and its surroundings for signs of tampering or unauthorized devices. When combined with physical measures, visual checks can ensure, e.g., the integrity of placed seals. Visual checks must be carried out according to a defined schedule, e.g., at regular intervals, during scheduled maintenance, or on a sporadic basis. The effectiveness of visual checks depends on the selected schedule and resulting inspection frequency. More frequent checks reduce the window of opportunity for an attacker to conduct high-impact attacks, but increase operational effort and costs. Thus, the frequency must be balanced against the resources associated with assigning personnel to perform such checks.

4 Evaluation Framework

To identify suitable and effective measures for securing the legacy link in a given deployment context, it is essential to define criteria that enable a structured evaluation of measures with differing properties (e.g., physical, technical, and operational; preventive vs. detective). These criteria must capture, e.g., a measure's security coverage, operational feasibility, dependencies regarding the detection or prevention, as well as its associated costs. In this section, we introduce evaluation criteria that cover these aspects for comparing diverse compensating measures.

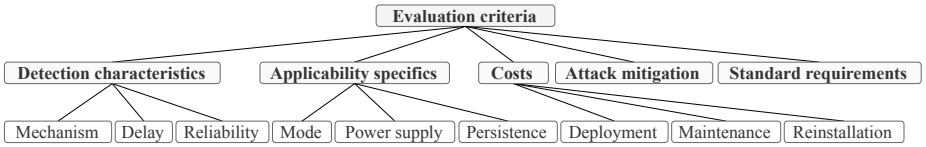

Fig. 2. Evaluation criteria.

We assess the effectiveness of measures using the following criteria, cf. Fig. 2: (1) the mechanism, delay, and reliability of detective measures, (2) applicability factors such as control mode, required power supply, and persistence, and (3) costs associated with deployment, maintenance, and reinstallation. We also evaluate (4) the effectiveness of measures in mitigating different attacks and (5) their adherence to requirements derived from security controls outlined in international standards. The following subsections are organized along these five criteria.

4.1 Detection Characteristics

Detective measures show characteristics that influence their effectiveness, e.g., how a security incident is detected, reported, and how long it takes to do so. To evaluate detective measures, we examine three key aspects: the mechanism, the delay between the occurrence of an incident and its detection, and its reliability.

Detection Mechanism. Detective measures use various mechanisms to detect and report security incidents. Technical measures use programmed logic and logs, i.e., *automated* mechanisms to detect and report a security incident, such as an invalid response or anomalous behavior. Physical measures are linked to operational means and depend on *personnel* for detection and reporting. For example, a broken seal remains undetected until the next interaction by personnel.

Detection Delay. Measures detect security incidents with different delays. Some technological measures report incidents *immediately*, i.e., in a fraction of milliseconds, e.g., link-down detection. Others report an incident after the *next automated check*, as in the case of the reachability test, connectivity test, and identification request. The period between checks must be chosen carefully: infrequently enough not to disrupt applications but frequently enough not to give an attacker a large window of opportunity, i.e., in the range of seconds. Most physical and operational measures rely on checks by personnel. Thus, the detection of an incident is delayed until the *next interaction*. Such interactions, however, happen less frequently, possibly within hours or days.

Detection Reliability. Detective measures provide varying degrees of reliability in terms of detecting a security incident and resisting manipulation. We consider a measure to be reliable if the measure cannot be bypassed by an attacker in a short period of time (i.e., seconds) and without the use of sophisticated tools and hardware. We consider most of the presented measures to be reliable, i.e., *incidents are always detected*. For example, to bypass security seals, an attacker would require an exact match to replace the broken seal; otherwise, tampering

would be detected with the next interaction. Unauthorized unplugging of the cable always triggers a link-down event. We further consider IP-ID monitoring, the connectivity test, and the identification request to be reliable, as bypassing requires an attacker to previously eavesdrop on the communication of the legacy device, which is infeasible without specific tools. IP-ID monitoring further requires an attacker to mimic the device-specific assignment behavior, and the connectivity test requires an attacker to replicate the port fingerprint. Sensor monitoring can be less reliable, depending on the deployment: *Incidents may only be often detected* as an attacker may have knowledge of the sensor placement and trick the reporting. The reachability test may even fail to detect an embedded device, i.e., *incidents are partly not detected*, as the calculated average response time may suffer from a high deviation.

4.2 Applicability Specifics

Security measures vary in their suitability for specific deployment contexts. For example, time-sensitive networks require measures that introduce no additional traffic overhead, and deployments where devices are frequently relocated or disconnected require solutions that remain persistent against device reboots. To account for these specifics, we evaluate each measure in terms of its control mode, operational requirements, and persistence to determine whether a measure can be effectively integrated into a given deployment context without introducing unintended disruptions or imposing excessive constraints.

Mode. We classify measures according to their mode, distinguishing *active* and *passive* measures. Active measures require interaction with the device, e.g., probing or request-based measures, adding traffic overhead. Passive measures do not actively interact with the device but analyze incoming traffic. However, passive approaches can introduce some latency, e.g., due to the processing required to mirror and inspect packet headers.

Required Power Supply. All technical measures *require a permanent power supply*. As a result, if both the legacy device and the gateway are disconnected from the power system, these measures can no longer prevent or detect security incidents. In deployment contexts where the legacy device is regularly removed from the network, such as mobile or temporarily deployed systems (e.g., maintenance devices), physical and operational measures should be used in a complementary manner. Alternatively, the gateway can be equipped with an emergency power supply, ensuring the continued availability of critical security functions.

Persistence. We define the persistence of a measure as its ability to resume its intended functionality after a reboot of the legacy device without generating false alarms. We consider physical and operational measures to be *persistent*, as they are not dependent on the operational state of the device. In contrast, link-down detection is *not persistent* to reboots, as the link state switches to `down` during shutdown, which may be erroneously reported as a tampering event. Similarly, IP-ID monitoring may generate false alarms if the device resets its counters after a reboot, leading to the observation of unexpected IP-IDs. We consider the

identification request to be persistent, as identifying information persists across reboots. We consider ACLs to be persistent if the filtered network addresses are either statically set or dynamically assigned consistently. Connectivity tests are persistent provided that the probed services restart automatically upon reboot.

4.3 Costs

The costs associated with deploying and operating security measures play a decisive role in their practicality. We distinguish three primary cost dimensions: deployment, maintenance, and reinstallation costs. For each dimension, we classify the costs as either low, medium, or high. Low costs are considered negligible within the overall operational cost structure; medium costs represent a noticeable but moderate factor relative to ongoing expenses; and high costs constitute a significant and separately accounted factor within the overall operational budget.

Deployment Costs. Deployment costs cover the initial effort required to purchase, configure, and integrate a measure into the existing infrastructure. For physical measures, we usually require additional hardware. Security seals and cable locks fall into the low-cost category, as their production and acquisition costs are negligible. In contrast, a customized tamper-proof enclosure entails higher production and installation costs, resulting in medium deployment costs. Technical measures typically require specific configuration. For example, IP-ID monitoring requires the determination of the device's IP-ID assignment behavior; connectivity tests necessitate the identification of all open ports. Both tasks require scanning tools, tailored setup procedures, and integration into a monitoring system, resulting in medium deployment costs. Operational measures require the casting and hiring of personnel, also resulting in medium costs.

Maintenance Costs. Maintenance costs arise from the need for periodic inspections to ensure the continued effectiveness of a measure. Low maintenance costs are associated with automated technical measures that operate without ongoing manual intervention. High maintenance costs, by contrast, occur when measures require regular physical inspections or other on-site activities such as physical measures, which must be checked by personnel to ensure their integrity.

Reinstallation Costs. We define reinstallation costs as the resources required to restore or reconfigure a measure after a security incident has occurred. We evaluate these costs in comparison to their initial deployment costs: Physical measures possibly require new hardware, especially after physical tampering. Thus, their reinstallation costs typically correspond to their deployment costs. For technical measures, reinstallation is typically less costly, as configuration parameters are already known from the initial setup, simply requiring a restart.

4.4 Attack Mitigation

We evaluate the effectiveness of the discussed measures in mitigating (preventing, detecting, or limiting the impact of) attacks targeting the legacy link. To address

the risks associated with the legacy link, we consider two factors: (i) attack capabilities and (ii) the environment and operational characteristics of the device.

Attack Capabilities In the scope of this attack model are local attacks targeting the insecure communication of the legacy device passing over the legacy link. Local attacks require an attacker to temporarily gain physical access to manipulate the infrastructure, e.g., unplug the legacy device. Out of scope are remote network attacks, as we assume that the security features of the gateway shield the legacy device from external attacks. In addition, attacks targeting the security gateway are out of scope. If the gateway is tampered with or removed undetected, efforts to secure the unsecured link with additional measures would be obsolete.

To describe the impact of the attacks in scope, we consider the security objectives of the availability of the services of the legacy device, integrity, and confidentiality of the communication of the legacy device (cf. Section 2). Further, for each attack, we distinguish *direct* measures, which explicitly prevent or detect an attack, and *indirect* measures, which provide indicators of compromise, e.g., observable deviations in system behavior or timing irregularities that may signal malicious activity. In particular, we consider the following attacks, cf. Table 3:

Physical Tampering (PT): *Disconnecting the legacy device or damaging the link.* As a result, tampering compromises the availability of the device's services. Preventive tampering protection can be achieved using cable locks and enclosures, whereas security seals enable detection. However, these physical measures rely on regular visual checks to detect tampering. Sensor monitoring and link-down detection allow for automated detection of physical tampering.

Unauthorized Logical Access (UA): *Connecting an unauthorized device to the network, either by unplugging the legacy device and connecting an unauthorized device, or by installing additional hardware.* Unauthorized access compromises integrity and, in the case of unplugging, availability. To mitigate unauthorized access attacks, measures must distinguish between packets sent by the legacy device and those sent by an unauthorized device. ACLs prevent unauthorized access by filtering packets based on source MAC or IP addresses, allowing only traffic originating from the legacy device. Indirectly, physical tampering detection measures compensate unauthorized logical access attacks and any further escalating logical access attacks.

Impersonation (I): *Replacing the legacy device with an unauthorized device, which disguises itself and its communication as legitimate on the network.* Prior to this attack, the attacker has to eavesdrop on communication to learn characteristics of the legacy device, e.g., network addresses or provided services, thereby compromising confidentiality. In addition, this attack comprises availability and integrity, as the unauthorized device forges communication. As the attack device impersonates the legacy device, ACLs cannot prevent this attack. IP-ID monitoring can reveal inconsistencies if the impersonating device fails to replicate the IP-ID assignment behavior of the legitimate device. Likewise, connectivity tests may expose differences in the open ports, while device-identification requests can uncover deviations in specific configuration values.

Man-in-the-Middle (MitM): *Embedding a malicious programmable device into the legacy link to access communication and interfere with data in transit.* As the MitM can intercept, interrupt, modify, and fabricate messages, it compromises availability, integrity, and confidentiality. Mitigating MitM attacks is particularly challenging. The reachability test may indirectly detect a MitM device if it introduces forwarding delays, causing increased response times. However, determining an appropriate detection threshold is non-trivial, as delays vary depending on the specific setup. IP-ID monitoring can detect fabricated packets generated by a MitM device that implements a different IP-ID assignment behavior, but cannot identify packets with an altered payload. Similarly, request-based measures cannot detect the MitM device, as the legacy device remains responsive.

Environment The environment where the legacy device is placed in (publicly accessible environments vs. enclosed spaces) has a further significant influence on the possibilities and risk of detection of an attack targeting the legacy link. In a publicly accessible environment, an attacker can gain unauthorized access to the legacy device with little effort. This type of environment applies, e.g., to field-level controllers that are located in unsupervised fields, sensors mounted on pipelines, or controllers as part of railway infrastructures. An enclosed space is characterized by the presence of security perimeters, such as entry controls or security surveillance, and a restricted user group. This characterization applies, e.g., to an industrial warehouse, containing diverse mobile and stationary devices. While such physical controls make it difficult for an attacker to gain unauthorized access, an attack through internal personnel remains possible. As a result, additional compensating security measures are required even in enclosed spaces.

The operational characteristics of a legacy device and the resulting window of opportunity further influence the success of attacks and the time until these attacks are disclosed. For example, critical industrial controllers operate non-stop and are, thus, continuously supplied with power, which allows for security measures that require a consistent power supply to function properly, e.g., continuous monitoring. Other mobile equipment may be only used on demand, increasing the window of opportunity to tamper with the legacy link.

4.5 Adherence to Standard Requirements

The use of legacy devices is typical in industrial environments where devices often operate over long lifetimes [8]. Industrial environments are governed by stringent security standards that define requirements, e.g., for secure design and operation [5]. To ensure applicability in regulated industries, we align the compensating measures with the requirements and security controls defined in relevant international standards. In doing so, we combine best practices with standard requirements, highlight suitable compensating measures, and identify gaps that remain unaddressed.

Security Controls Different domains have different requirements for the operation of systems. For broad adoption, we consider two widely established standards: ISO/IEC 27002 [7] and IEC 62443 [5,6].

The ISO/IEC 27000 series provides best practices for establishing and operating an Information Security Management System (ISMS) across organizations of all types and sizes. ISO/IEC 27002 specifies a comprehensive suite of commonly accepted security controls in four themes (people, physical, technological, and organizational) that serve as implementation guidance for reducing information security risks. However, these controls often assume modern device capabilities that legacy devices simply do not have. ISO/IEC 27019 [8] extends the security controls specified in ISO/IEC 27002 to the domain of process control and automation; also introducing new controls to address sector-specific requirements, including a control covering the risks arising from legacy equipment: *ENR – Treatment of legacy systems* discusses countermeasures required to protect systems against the risks arising from legacy systems without adequate security features. Proposed countermeasures include strict and appropriate network segregation, avoidance of remote access for configuration and maintenance purposes, as well as enforcement of strict access controls at network, system, and application levels. ISO/IEC 27019 further introduces *ENR – Securing process control data communication*. Several communication protocols do not include security mechanisms, while others define optional security extensions not necessarily included in all implementations. Available security features in such protocols should be enabled to fulfill the given security requirements of such communication.

The IEC 62443 series focuses on security for industrial automation and control systems, emphasizing availability, secure operation under constrained conditions, and resilience of automation systems in addition to the confidentiality and integrity goals common in IT security. IEC 62443-4-2 [6] defines technical requirements for components such as embedded devices, network components, host systems, and software applications. These component requirements (CR) are derived from the broader system requirements (SR) in IEC 62443-3-3 [5].

Derived Requirements Organizations select controls following a risk assessment process. We approach this assessment through the discussed attack model. Table 1 outlines controls from ISO/IEC 27002:2022 relevant for securing the legacy link and their mapping with IEC 62443-3-3:2019 and IEC 62443-4-2:2019. From these controls, we derive five requirements ***R1-R5*** for compensating measures:

R1 Prevent physical tampering with the legacy link. To address physical security requirements, measures must prevent unauthorized physical access, disruption, or damage to the legacy link. Cable locks and enclosures meet this requirement by physically securing the cable or enclosing it.

R2 Detect physical tampering with the legacy link. Security seals, sensor monitoring, link-down detection, and visual checks address the requirement to detect unauthorized physical access to or disruption of the link.

R3 Prevent unauthorized logical access to the network. Adequate access control requires measures to prevent unauthorized logical access to infor-

Table 1. Relevant ISO/IEC 27002:2022 controls with their mapping to ISO/IEC 62443-3-3:2019 (system requirements, SR) and ISO/IEC 62443-4-2:2019 (network device requirements, NDR) as well as their alignment with the discussed security measures.

Security control	Control excerpt	Measures
Physical controls		
7.4 Physical security monitoring NDR 3.11 Physical tamper resistance and detection	Network components must provide tamper-proofing and detection mechanisms for unauthorized physical access.	P4, P3, T2
7.12 Cabling security	Cables carrying data should be protected from interception, interference, or damage.	O1, P1, P2
7.13 Equipment maintenance	Equipment should be maintained correctly to ensure the availability, integrity, and confidentiality of information.	O1
Technical controls		
8.3 Information access restriction	Unauthorized access to information should be restricted; grant access based on, e.g., identity or device.	T1
8.5 Secure authentication	A suitable authentication technique should be chosen to substantiate the claimed identity of an entity.	T6, T3, T5
8.16 Monitoring activities SR 6.2 Continuous monitoring	Networks, systems, and applications should be monitored for anomalous behavior.	T2, T3
8.20 Networks security	Controls should be established, i.a., to safeguard the confidentiality and integrity of data passing over public networks; restrict and filter connections to the network; detect, restrict, and authenticate the connection of devices.	T1, T2, T3, T4, T5, T6
8.24 Use of cryptography SR 3.1 Communication integrity	Rules for the effective use of cryptography should be defined and implemented.	-

mation transmitted over the legacy link and the network. The ACL meets this requirement by filtering packets based on the device's source network addresses.

R4 Detect unauthorized logical access to the network. The requirement to detect unauthorized logical access (attacks ***UA***, ***I***, and ***MitM***) is addressed differently by several measures. The connectivity test identifies impersonating devices by checking for deviations in expected open ports, while the identification request validates device-specific information. IP-ID monitoring continuously checks for anomalies in the device's IP-ID assignment behavior, thereby uncovering spoofed packets. Link-down detection logs state changes at the interface, hinting at attempts to disconnect or replace the legacy device.

R5 Identify or authenticate the legacy device. Network access requirements demand the identification or authentication of the connected device. If the legacy device does not implement communication protocols with authentication or any other cryptographic features, we have to rely on compensating measures and base access decisions on device characteristics. The identification request, IP-ID monitoring, and the connectivity test enable device identification through identifying information, specific IP-ID assignment behavior, and expected open ports, respectively. These characteristics are challenging to spoof, as they require prior reconnaissance through eavesdropping or scanning.

The discussed evaluation criteria and their value options are summarized in Table 2. Based on these criteria, Table 3 provides an overview of all discussed measures along with their assessed effectiveness across these criteria.

5 Framework Application

As each security measure has inherent limitations (e.g., the ACL can be bypassed by spoofing), a holistic security concept consisting of complementary measures is required to sufficiently secure the legacy link. The resulting combination reduces the risk and increases the effort for a successful attack, forcing attackers to invest additional time, knowledge, and equipment to exploit access to the legacy link. Concerning the selection of an appropriate combination, a naive approach would be to apply all discussed measures to any use case, as not every measure is equally suited for every deployment. Rather, the selection depends on multiple factors, such as environmental constraints, device capabilities, and the operational context. In the following, we first discuss the process of applying the framework. Then, we demonstrate its application through two representative use cases. Notably, due to the sporadic nature of security incidents and the resulting lack of a viable empirical reference group, we adopt a best-practice comparison rather than an empirical assessment of incident-related data.

5.1 Application Process

The proposed framework for selecting a suitable combination of compensating security measures can be applied in four steps:

(1) Define deployment prerequisites. First, the user defines the deployment context, considering environmental and device-specific prerequisites; e.g., whether a device can tolerate a temporary interruption in the power supply.

(2) Define security objectives. Second, the user identifies the relevant security objectives for the deployment context, e.g., emphasizing logical access controls if sufficient physical protection already exists.

(3) Match individual measures based on the defined prerequisites. Third, based on the defined prerequisites, the user matches appropriate measures.

Table 2. Evaluation criteria and their corresponding value options.

Criteria		**Value options**
Detection	Mechanism	*automated*, *personnel*
	Delay	*immediately*, *next automated check*, *next interaction through personnel*
	Reliability	*always*, *often*, *partly*
Applicability	Mode	*active*, *passive*
	Power supply	*required*, *not required*
	Persistence	*persistent*, *not persistent*
Costs		*low*, *medium*, *high*
Attacks		✓ if the attack is mitigated (indirectly)
Requirements		✓ if the requirement is met

Table 3. Overview of the compensating security measures (M) with their evaluated criteria and effects. Measures are assessed against detection properties, applicability, costs, attack mitigation, and compliance with derived control requirements, cf. Table 2.

	Detection			**Applicability**			**Costs**			**Attacks**				**Requirements**				
M	Mech.	Delay	Reliab.	Mode	Power	Persist.	Deploy.	Maint.	Reinst.	*PT*	*UA*	*I*	*MitM*	*R1*	*R2*	*R3*	*R4*	*R5*
P1				pass.	n. req.	persist.	low	high	low	✓	(✓)	(✓)	(✓)	✓				
P2				pass.	n. req.	persist.	med.	high	med.	✓	(✓)	(✓)	(✓)	✓				
P3	pers.	interact.	always	pass.	n. req.	persist.	low	high	low	✓	(✓)	(✓)	(✓)		✓			
P4	auto.	immed.	often	pass.	req.	persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T1				pass.	req.	persist.	med.	low	low		✓					✓		
T2	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T3	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low			✓					✓	✓
T4	auto.	check	partly	act.	req.	persist.	med.	low	low				(✓)				✓	
T5	auto.	check	always	act.	req.	persist.	med.	low	low			✓					✓	✓
T6	auto.	check	always	act.	req.	persist.	med.	low	low			✓					✓	✓
O1	pers.	interact.	always	pass.	n. req.	persist.	med.	high	med.	✓	✓	✓	✓		✓		✓	

Table 3 serves as a formal tool for this step, enabling a comparison and selection of measures. For example, for a time-critical deployment context, we would exclude any active measures that introduce additional traffic overhead.

(4) Select remaining measures with respect to the security objectives. Finally, from the remaining measures, the user selects a minimal yet effective combination that addresses all relevant security objectives. Where multiple measures target the same objective, redundancy can be beneficial when the additional costs and efforts are acceptable, e.g., complementing operational measures with technical measures. Conversely, measures that provide redundancy but entail, e.g., significantly higher costs, can be omitted. In the final selected combination, each measure should be essential, and none can be omitted without compromising the overall security of the legacy link.

With regard to the evaluation of the final combination, the framework prioritizes measures with immediate and automated detection, persistence, and power dependencies. Costs are considered holistically. A type of attack and requirement is mitigated or met if at least one measure in the combination addresses it.

After the evaluation, Table 3 also serves as a formal tool to demonstrate that all relevant requirements and constraints have been considered, making decisions well-founded and fully traceable. If there are no suitable measures, the framework makes these gaps explicit, supporting subsequent risk assessment and decisions on whether residual risks can be accepted.

Regarding scalability, practitioners can apply the four-step process once for a specific device category or deployment use case (e.g., field-level sensors in publicly accessible zones) rather than applying the framework to every individual asset. Once an effective combination of measures is identified, the resulting security concept can be replicated across similar devices. This reduces the complexity from a per-device task to a per-type task.

5.2 Use Case 1: Industrial Outstation

We first apply the framework to a common use case in the energy utility domain.

(1) Define deployment prerequisites. We consider a DNP3 programmable logic controller (PLC) as part of an energy distribution networking system that is installed in an unsupervised outdoor area (outstation), cf. the scenario discussed by Rosborough et al. [12]. The controller is connected to a gateway that securely forwards communication to a control center, and both are placed in a secure cabinet. The outstation is not frequently visited by personnel.

(2) Define security objectives. The primary objective in this mission-critical domain is to ensure the availability of the controller. Despite the physical barrier of the cabinet, once broken into, an attacker can, e.g., disconnect the controller. Therefore, we require measures to mitigate physical tampering.

In addition, we require integrity of communication passing over the legacy link. An attacker connecting an unauthorized device could gain access to the network [12]. Manipulation of messages could also have an impact on physical processes and cause severe harm. Accordingly, we require measures to mitigate unauthorized logical access to the network and transmitted data.

(3) Match individual measures based on the defined prerequisites. Given the unsupervised environment, we focus on automated measures rather than relying on human maintenance. Considering Table 3, we exclude measures requiring detection through personnel, as well as unreliable measures that may produce false alarms, which require follow-up sightings by personnel. In Table 4, we grayed out and struck through these excluded measures.

(4) Select remaining measures with respect to the security objectives. After exclusion, the following measures remain, cf. Table 4: P1, P2, P4, T1-T3, T5, and T6. The cabinet as a kind of enclosure already prevents physical access, making an additional cable lock redundant, compare rows P1 and P2. A contact sensor securely positioned at the cabinet opening enables automated detection and reporting of unauthorized physical access, cf. columns *Detection Mechanism* and *PT* of P4, compensating for the absence of personnel. Link-down detection provides an additional detection capability, offering similar coverage

Table 4. Application of the framework, cf. Table 3, to **Use Case 1: Industrial Outstation**; measures not applicable to the use case are struck through; **selected measures** used in the combination (C: P2, P4, T1, and T6) are in bold.

	Detection			**Applicability**			**Costs**			**Attacks**				**Requirements**				
M	Mech.	Delay	Reliab.	Mode	Power	Persist.	Deploy.	Maint.	Reinst.	*PT*	*UA*	*I*	*MitM*	*R1*	*R2*	*R3*	*R4*	*R5*
P1				pass.	n. req.	persist.	low	high	low	✓	(✓)	(✓)	(✓)	✓				
P2				pass.	n. req.	persist.	med.	high	med.	✓	(✓)	(✓)	(✓)	✓				
~~P3~~	~~pers.~~	~~interact.~~	~~always~~	~~pass.~~	~~n. req.~~	~~persist.~~	~~low~~	~~high~~	~~low~~	~~✓~~	~~(✓)~~	~~(✓)~~	~~(✓)~~		~~✓~~			
P4	auto.	immed.	often	pass.	req.	persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T1				pass.	req.	persist.	med.	low	low		✓					✓		
T2	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T3	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low			✓					✓	✓
~~T4~~	~~auto.~~	~~check~~	~~partly~~	~~act.~~	~~req.~~	~~persist.~~	~~med.~~	~~low~~	~~low~~				~~(✓)~~				~~✓~~	
T5	auto.	check	always	act.	req.	persist.	med.	low	low			✓					✓	✓
T6	auto.	check	always	act.	req.	persist.	med.	low	low			✓					✓	✓
~~Ø1~~	~~pers.~~	~~interact.~~	~~always~~	~~pass.~~	~~n. req.~~	~~persist.~~	~~med.~~	~~high~~	~~med.~~	~~✓~~	~~✓~~	~~✓~~	~~✓~~		~~✓~~		~~✓~~	
C	auto.	immed.	always	both	req.	persist.	med.	low	low	✓	✓	✓	(✓)	✓	✓	✓	✓	✓

to sensor monitoring, cf. rows P4 and T2. However, sensor monitoring reports any cabinet opening, including scheduled maintenance, which may occasionally lead to false alarms. In contrast, link-down detection only triggers upon an actual link interruption, which provides delayed detection in case of an actual attack. Consequently, sensor monitoring offers earlier detection, whereas link-down detection can serve as a redundant backup mechanism if desired. The ACL limits communication to the authorized network address of the legacy device, fulfilling requirement *R3*, cf. row T1. The remaining measures for detecting unauthorized logical access through impersonation, i.e., IP-ID monitoring, connectivity test, and identification request (rows T3, T5, and T6, respectively), address the same requirements but differ in their *Detection Delay*, *Mode*, and *Persistence*. To keep maintenance low, we exclude IP-ID monitoring, as it is not persistent and, thus, requires manual checks and reconfiguration after power interruptions or scheduled reboots. Both connectivity test and identification request reliably detect unauthorized access attempts and, therefore, fulfill requirement *R4*. As DNP3 does not support authentication, full device authentication cannot be achieved. However, these measures can identify the connected device via device-specific information or port fingerprinting, thereby addressing requirement *R5*. In use cases with devices exposing many services, port fingerprinting may offer stronger identification. In this case, with the PLC providing only minimal functionality, the identification request is sufficient and places less burden on the device.

The final combination of P2, P4, T1, and T6 expands the cabinet with sensor monitoring, ACL, and the identification request. This combination effectively mitigates tampering, unauthorized access, and impersonation attacks. While not directly, the combination also mitigates MitM attacks by detecting preceding tampering activities. Thus, this combination meets all defined objectives; omitting any of the selected measures would result in unaddressed requirements.

5.3 Use Case 2: Automated Guided Vehicle

Second, we apply the framework to a mobile use case in factory automation.

(1) Define deployment prerequisites. We consider an automated guided vehicle (AGV) with an onboard PROFINET PLC that coordinates cyclic I/O exchange in real time. The PLC communicates upstream via a wireless bridge with the fleet management (cf. the scenario discussed by Stój et al. [14]). The AGV operates within an enclosed factory and transports materials between workstations. Unlike stationary installations, the AGV may become physically accessible in less-controlled areas, e.g., during loading or charging, making local access feasible for an attacker. Regarding operational prerequisites, the PLC remains powered and network-connected continuously; full power-off is typically limited to scheduled maintenance. The PLC does not provide any authentication or encryption. The wireless bridge may serve as or incorporate a security gateway responsible for upstream authentication and integrity protection.

(2) Define security objectives. The primary objective is to ensure the availability of the PLC. Since the AGV contributes to material flow, disrupting its

PLC can halt production processes and cause operational and financial damage. Thus, we require measures to mitigate physical tampering.

Further, an attacker with access to the legacy link can embed a malicious device and manipulate messages to alter AGV behavior, potentially leading to collisions or equipment damage. Observing communication may also reveal workflows (e.g., scheduling, material movement), enabling targeted sabotage or theft. As the AGV connects to multiple access points and backend services, the legacy link may serve as an entry point into the broader industry and enterprise network. Hence, we require measures that mitigate unauthorized logical access.

(3) Match individual measures based on the defined prerequisites. Given the real-time constraints of the PROFINET PLC, we exclude active measures that introduce additional traffic, cf. Table 5. We also exclude further preventive physical measures, since the AGV already operates within an enclosed environment. Accordingly, we focus on detective measures for identifying physical tampering and passive measures to detect unauthorized logical access.

(4) Select remaining measures with respect to the security objectives. The following measures remain, cf. Table 5: P3, P4, T1-T3, and O1. Among these measures, the seal, sensor monitoring, and link-down detection address the detection of physical tampering, cf. *PT* column of P3, P4, and T2. However, the seal requires the combination with visual checks to detect tampering. Depending on the defined inspection schedule, this combination either introduces high maintenance when checks are performed frequently (e.g., hourly) or results in significant detection delays if checks are limited to, e.g., maintenance intervals. Since the PLC operates continuously, we select the reliable link-down detection mechanism from these options for tampering detection. Regarding measures to prevent unauthorized logical access, the ACL restricts communication to the network addresses of the PLC and, therefore, addresses *R3*, cf. row T1. IP-ID monitoring further effectively detects unauthorized access attempts involving spoofed packets, thereby fulfilling requirement *R4*, cf. row T3. Moreover, since

Table 5. Application of the framework, cf. Table 3, to **Use Case 2: Automated Guided Vehicle**; measures not applicable to the use case are struck through; **selected measures** used in the combination (C: T1, T2, and T3) are in bold.

	Detection			**Applicability**			**Costs**			**Attacks**				**Requirements**				
M	Mech.	Delay	Reliab.	Mode	Power	Persist.	Deploy.	Maint.	Reinst.	*PT*	*UA*	*I*	*MitM*	*R1*	*R2*	*R3*	*R4*	*R5*
~~P1~~				~~pass.~~	~~n. req.~~	~~persist.~~	~~low~~	~~high~~	~~low~~	~~✓~~	~~(✓)~~	~~(✓)~~	~~(✓)~~	~~✓~~				
~~P2~~				~~pass.~~	~~n. req.~~	~~persist.~~	~~med.~~	~~high~~	~~med.~~	~~✓~~	~~(✓)~~	~~(✓)~~	~~(✓)~~	~~✓~~				
P3	pers.	interact.	always	pass.	n. req.	persist.	low	high	low	✓	(✓)	(✓)	(✓)		✓			
P4	auto.	immed.	often	pass.	req.	persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T1				pass.	req.	persist.	med.	low	low		✓					✓		
T2	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low	✓	(✓)	(✓)	(✓)		✓			
T3	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low			✓					✓	✓
~~T4~~	~~auto.~~	~~check~~	~~partly~~	~~act.~~	~~req.~~	~~persist.~~	~~med.~~	~~low~~	~~low~~				~~(✓)~~				~~✓~~	
~~T5~~	~~auto.~~	~~check~~	~~always~~	~~act.~~	~~req.~~	~~persist.~~	~~med.~~	~~low~~	~~low~~			~~✓~~					~~✓~~	~~✓~~
~~T6~~	~~auto.~~	~~check~~	~~always~~	~~act.~~	~~req.~~	~~persist.~~	~~med.~~	~~low~~	~~low~~			~~✓~~					~~✓~~	~~✓~~
O1	pers.	interact.	always	pass.	n. req.	persist.	med.	high	med.	✓	✓	✓	✓		✓		✓	
C	auto.	immed.	always	pass.	req.	n. persist.	med.	low	low	✓	✓	✓	(✓)		✓	✓	✓	✓

PROFINET lacks built-in authentication, IP-ID monitoring contributes to *R5* by identifying the legacy device based on its characteristic assignment behavior.

The resulting combination of ACL (T1), link-down detection (T2), and IP-ID monitoring (T3) mitigates physical tampering, unauthorized access, impersonation, and the prerequisites for MitM attacks. However, the combination does not address requirement *R1* (preventive physical tamper resistance), cf. Table 5. As the AGV operates in an enclosed environment with existing physical controls, additional preventive measures would only increase costs without significantly reducing risk. Removing any of the selected measures would, in contrast, introduce unacceptable gaps in the covered attack types or derived requirements.

6 Framework Extension

While this work focuses on legacy devices due to the necessity caused by their lack of built-in security features, the framework itself is designed to be generalizable. By making fewer assumptions about the capabilities of the target device, the approach remains inherently generic. Therefore, users can apply the framework to any device where compensating measures are required. Furthermore, users can extend the proposed framework to their needs and specific use cases along four axes: extending the set of measures, extending the evaluation criteria, extending the attack model, and extending the standard control mapping.

Extending the Set of Measures. Users can add new physical, technical, and operational measures to the framework. Their usage, dependencies on gateway capabilities, and potential limitations should be discussed to support deployment decisions. Users then evaluate the measures along the introduced criteria. The value options for each criterion are summarized in Table 2. Most measures can be assigned values directly based on their inherent properties. Alignment with comparable measures can further support consistent categorization.

Extending the Evaluation Criteria. The evaluation criteria can be refined or extended to reflect organization-specific policies and guidelines. For example, we deliberately leave the costs in this framework somewhat vague; users may replace these values with more fine-grained cost models that adapt to budgeting practices within their organization. Additional criteria may reflect, e.g., the maturity of a security measure in the specific domain.

Extending the Attack Model. The attack model used in this work focuses on physical tampering and unauthorized logical access to the legacy link. Users may expand or refine the model to introduce more granular attack types, e.g., differentiating spoofing from manipulation attacks.

Extending the Standard Control Mapping. The framework supports integration with standards beyond those considered in this work by aligning measures with control objectives. Users may incorporate national or sector-specific standards, such as NIST SP 800-82 [15]. Since many standardization bodies and regulatory authorities provide crosswalks to ISO/IEC 27002 controls, such mappings can be integrated into the framework with minimal effort, enabling users to adopt the framework within their compliance landscape.

7 Related Work

Several works address *security strategies for industrial systems*. Serror et al. [13] identify security challenges in IIoT and recommend cryptography and authentication, patch management, access control, network monitoring, and intrusion detection. For legacy devices, the authors recommend compensating measures, e.g., access control and monitoring. Bartman and Carson [3] discuss threat vectors for SCADA and CPS and propose countermeasures to secure communication and device access, e.g., MAC whitelisting, Ethernet link-status monitoring, and sensors. While these works provide abstract recommendations or discuss individual controls, they do not provide a comparison of their effectiveness. In contrast, to the best of our knowledge, we are the first to jointly consider physical, technical, and operational compensating measures and introduce a framework that enables their structured evaluation and comparison, allowing practitioners to assess the combined effectiveness and interchangeability of measures.

The selection of appropriate security measures is typically preceded by a *structured risk management or threat modeling process*. Such processes aim to determine the level of risk associated with system assets and to identify where countermeasures are required. Yaqoob et al. [17] introduce an Integrated Security, Safety, and Privacy (ISSP) risk assessment framework to quantify risks for networked medical legacy devices. Their framework extends NIST and ISO risk management principles by combining safety, security, and privacy into a unified quantitative model. It evaluates vulnerability and hazard likelihoods to guide the selection of security controls. Badawy et al. [2] propose a hybrid threat modeling framework for legacy industrial control systems that integrates PASTA, attack trees, and STRIDE for system-, attacker-, and risk-centric perspectives, respectively. They use a scoring system to quantify security levels and prioritize countermeasures. In contrast, we focus on the effectiveness and interaction of measures. We complement risk assessment by characterizing how individual measures act to reduce risk and by supporting the selection of combinations once the need for mitigation has been established.

Other works consider the *evaluation or prioritization of security controls*. Al-Safwani et al. [1] propose a control prioritization model based on multi-criteria decision techniques. Criteria include threat classification, severity, and remediation cost, with scores determined by experts. While the model systematically ranks technical controls, we include physical and operational controls. Further, we go beyond attack mitigation, evaluating applicability and adherence to industry standards. Tariq et al. [16] apply a fuzzy analytical hierarchy process to prioritize and select controls targeting cloud computing and wireless sensor networks. Their formalized multi-criteria method is grounded in ISO/IEC 27002:2013 and evaluates controls against criteria such as implementation time, effectiveness, risk, budgetary constraints, exploitation time, maintenance cost, and mitigation time. In contrast, we focus on compensating controls for legacy systems where constraints differ fundamentally. In addition, we consider attack mitigation, control characteristics, and compliance with IEC 62443.

8 Conclusion

Legacy devices remain a persistent challenge in industrial networks. While a security gateway can secure communication toward the network, the legacy link connecting the legacy device and the gateway remains vulnerable. As available security measures have differing properties and act on different levels (e.g., physical measures vs. operational policies) they are difficult to compare and evaluate. Consequently, securing the legacy link requires a tailored approach. We presented a framework for the structured evaluation of physical, technical, and operational measures based on five criteria: detection characteristics, applicability specifics, costs, attack mitigation, and adherence to international security standards.

Applying the framework to two representative use cases provided valuable insights: (i) an industrial outstation in the energy utility domain and (ii) an automated guided vehicle in factory automation. Despite sharing the same security objectives (availability, integrity), both use cases arrived at non-overlapping combinations of measures, demonstrating that there is no optimal combination; deployment constraints such as mobility, real-time requirements, and supervision levels also shape which measures are feasible and effective. Stricter operational constraints limit the set of applicable measures, potentially leaving attack vectors difficult to address. Notably, MitM attacks could only be mitigated indirectly by detecting physical tampering due to the inherent lack of cryptographic support in legacy hardware. In both use cases, no single measure could meet all derived requirements. The framework made this incompleteness explicit and traceable, guiding practitioners toward minimal but sufficient combinations.

The presented framework is currently limited in the sense that it does not link measure selection to a quantified risk assessment (e.g., IEC 62443-3-2). Integrating such a risk assessment would enable practitioners to prioritize measures based on assessed likelihood and impact rather than coverage alone. Further, while the current set of measures is non-exhaustive and the attack model focuses on local attacks, the framework is designed to be extensible. Ultimately, the proposed framework offers a transferable method for bridging the security gap of legacy devices. By facilitating their secure integration into modern industrial environments as well as related domains such as healthcare and transportation, the framework serves as a modular foundation for further work on securing brownfield environments.

Acknowledgments. This work has been funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK) under support code 16KN084434 and in part by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) - 528745080 - FIP 68. The authors alone are responsible for the content of the paper.

Disclosure of Interests. The authors have no competing interests to declare.

References

1. Al-Safwani, N., Fazea, Y., Ibrahim, H.: ISCP: In-depth Model for Selecting Critical Security Controls. Computers & Security **77**, 565–577 (2018)

2. Badawy, M., Sherief, N.H., Abdel-Hamid, A.A.: Legacy ICS Cybersecurity Assessment Using Hybrid Threat Modeling—An Oil and Gas Sector Case Study. Applied Sciences **14**(18), 8398 (2024)
3. Bartman, T., Carson, K.: Securing Communications for SCADA and Critical Industrial Systems. In: Conference for Protective Relay Engineers. College Station, TX, USA (2016)
4. Frauenschläger, T., Mottok, J.: Security-Gateway for SCADA-Systems in Critical Infrastructures. In: International Conference on Applied Electronics. Pilsen, Czech Republic (2022)
5. International Electrotechnical Commission: IEC 62443-3-3:2019 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels (2019)
6. International Electrotechnical Commission: IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components (2019)
7. International Organization for Standardization: ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls (2022)
8. International Organization for Standardization: ISO/IEC 27019:2024 Information security, cybersecurity and privacy protection – Information security controls for the energy utility industry (2024)
9. Kaniewski, S., Bechtel, L., Kneisel, P., Menth, M., Heer, T.: Security Gateway for Automated Micro-Segmentation and VPN Encryption in Industrial Legacy Systems. In: IEEE International Conference on Emerging Technologies and Factory Automation. Porto, Portugal (2025)
10. Kaniewski, S., Bechtel, L., Menth, M., Heer, T.: Monitoring IP-ID Behavior for Spoofed IPv4 Traffic Detection. In: IEEE International Conference on Emerging Technologies and Factory Automation. Padova, Italy (2024)
11. Khan, R., McLaughlin, K., Kang, B., Laverty, D., Sezer, S.: A Novel Edge Security Gateway for End-to-End Protection in Industrial Internet of Things. In: IEEE Power & Energy Society General Meeting. Washington, DC, USA (2021)
12. Rosborough, C., Gordon, C., Waldron, B.: All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications. In: Power and Energy Automation Conference (2019)
13. Serror, M., Hack, S., Henze, M., Schuba, M., Wehrle, K.: Challenges and Opportunities in Securing the Industrial Internet of Things. Transactions on Industrial Informatics **17**(5), 2985–2996 (2020)
14. Stój, J., Kampen, A.L., Cupek, R., Smołka, I., Drewniak, M.: Industrial Shared Wireless Communication Systems - Use Case of Autonomous Guided Vehicles with Collaborative Robot. Sensors **23**(1), 158 (2022)
15. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., et al.: Guide to Operational Technology (OT) Security (NIST SP 800-82r3) (2023)
16. Tariq, M.I., Ahmed, S., Memon, N.A., Tayyaba, S., Ashraf, M.W., Nazir, M., Hussain, A., Balas, V.E., Balas, M.M.: Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. Sensors **20**(5), 1310 (2020)
17. Yaqoob, T., Abbas, H., Shafqat, N.: Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices. IEEE Journal of Biomedical and Health Informatics **24**(6), 1752–1761 (2019)