applied sciences

MDPI

Article

# Towards Industrial Intrusion Prevention Systems: A Concept and Implementation for Reactive Protection

**Cyntia Vargas Martínez [1,2,*] and Birgit Vogel-Heuser [1]**

[1] Institute of Automation and Information Systems, Technical University of Munich, 85748 Munich, Germany; vogel-heuser@tum.de
[2] Bosch Rexroth AG, 97816 Lohr am Main, Germany
* Correspondence: cyntia.vargasmartinez2@boschrexroth.de

Received: 31 October 2018; Accepted: 27 November 2018; Published: 2 December 2018


**Featured Application: The paper presents a concept to actively and automatically respond to security intrusions in Industrial Automation Systems. It is comprised of reactive actions, and security and operational policies that consider both security and architectural trends of this kind of systems. This concept is of significance to system stakeholders that wish to increase the security of their system by implementing automatic and active protection.**

**Abstract:** System intrusions violate the security of a system. In order to maintain it, it is necessary to decrease the chances of intrusions occurring or by detecting them as soon as they ensue in order to respond to them in a timely manner. These responses are divided in two types: passive or reactive responses. Passive responses are limited to only notification and alerting; whereas, reactive responses influence the intrusion by undoing or diminishing its consequences. Unfortunately, some reactive responses may influence the underlying system where the intrusion has occurred. This is especially a concern in the field of Industrial Automation Systems, as these systems are critical and have a well-defined set of operational requirements that must be maintained. Hence, automatic reactive responses are often not considered or are limited to human intervention. This paper addresses this issue by introducing a concept for reactive protection that integrates the automatic execution of active responses that do not influence the operation of the underlying Industrial Automation System. This concept takes into consideration architectural and security trends, as well as security and operational policies of Industrial Automation Systems. It also proposes a set of reactive actions that can be taken in the presence of intrusions in order to counteract them or diminish their effects. The feasibility and applicability of the presented concept for Industrial Automation Systems is supported by the implementation and evaluation of a prototypical Reactive Protection System.

**Keywords:** industrial cyber-physical systems; cyber security; industrial automation systems; intrusion detection; intrusion prevention; reactive protection; security policies

## 1. Introduction

Over the past decade, integration of security in Industrial Automation Systems (IAS) has changed from being a commodity to a necessity. This has occurred due to the new technological advances and trends that have resulted in increased standardization and interconnection of systems (e.g., Industry 4.0 [1]), which give rise to new threats and vulnerabilities that can be exploited in order to compromise the security of such systems [2,3]. This security is comprised of a set of security policies and other security mechanisms that allow for enforcing such policies. These security policies represent a set of rules that indicate how a system is to be protected [4]. They may include but are not limited to

authorized or unauthorized behaviour regarding physical security, user and network access control, etc. [5].

The security of a system is said to be compromised when its security policies have been violated or its security mechanisms have been bypassed. These events are often referred to as *intrusions* [6]. In order to diminish or counteract the effects that such intrusions may have on the target system, it is recommended to detect them as soon as they occur. Many security solutions exist that allow for carrying out such action (e.g., File Integrity Checkers, Antiviruses, Event and User Authorization Management Systems, etc.). However, the scope of protection of some of them is limited, as they may focus on specific system components. An example of this are File Integrity Checkers (FIC). FIC are capable of detecting only intrusions that occur at a file system-level. Other solutions such as Intrusion Detection Systems (IDS) provide a wider protection scope as they specialize in detecting intrusions at a network- and host-level. However, their response actions are often limited to passively notifying or recording that an intrusion has occurred rather than actively responding to it by either blocking, stopping or modifying it.

These passive responses to intrusions often require further analysis or human intervention in order to counteract the effects of an intrusion [7], which results in delayed reactions. These delayed reactions may provide enough time for an intrusion to succeed. A successful intrusion is especially troublesome when dealing with critical systems such as industrial Cyber-Physical Systems (industrial CPS). These types of systems are automation systems comprised of a physical (i.e., control unit, sensors, actuators, etc.) and a cyber part (i.e., managing software) that allow the physical part to interact with the real world [8,9]. Hence, passive responses may not be enough to protect these systems due to the catastrophic consequences that security intrusions may have on them. Some of these consequences may negatively affect the environment around these systems and pose a great risk to normal operation resulting in monetary losses, safety concerns or political repercussions [10,11]. Hence, a security solution capable of not only detecting an intrusion but actively responding to it once it is detected in order to protect a system is often desired.

Although there exist security solutions (e.g., Intrusion Prevention Systems, Intrusion Response Systems, Security Incident and Event Management System, etc.) capable of automatically and actively responding to intrusions, their integration in IAS is often overlooked. This has occurred due to the concern that some reactive actions in the presence of intrusions may affect the operational requirements of IAS [12–14].

This paper attempts to address this concern and overcome other challenges related to reactive protection that exist in IAS through the introduction of a novel reactive protection concept. This concept represents the main contribution of this paper. It is comprised of an architecture for a Reactive Protection System capable of executing active responses automatically in the presence of intrusions. The execution of these actions does not negatively influence the operation of the IAS due to the consideration of operational policies. This concept also contemplates other security and architectural trends of IAS. More specifically, it integrates management of both security and operational policies on a network zone-basis which complies with the ISA/IEC 62443 series of Standards from the International Society of Automation (ISA) and International Electrotechnical Commission (IEC). Hence, providing a feasible and suitable solution capable of providing active and real-time protection against security intrusions. The feasibility and applicability of the presented reactive protection concept is demonstrated through a prototypical Reactive Protection System implementation and a test scenario considering a remote maintenance application.

This paper is structured as follows: Section 2 discusses in more detail challenges related to reactive protection against intrusions. Section 3 presents detailed requirements to overcome the challenges discussed in Section 2. Section 4 provides a brief overview of related work in the field of reactive protection (i.e., intrusion prevention and response) in IAS. Section 5 introduces the concept for reactive protection derived from the requirements presented in Section 3. Section 6 discusses the applicability of this concept through a detailed discussion of intrusions and attacks that can be mitigated with

it. Section 7 presents the prototypical implementation for the proposed concept. The experimental evaluation of this implementation and its results are presented in Section 8. Finally, Section 9 providing the conclusions and future work.

## 2. Challenges for Reactive Protection in Industrial Automation Systems

In order to discuss the challenges that exist for integration of reactive protection in IAS, it is important to first outline the current architectural and security trends. For this, a reference IAS architecture (Figure 1) has been derived from [15,16]. This architecture consists of five levels (from 0 to 4) corresponding to the levels of the well-known automation pyramid hierarchy (as defined by the ISA-95 standard [17]).

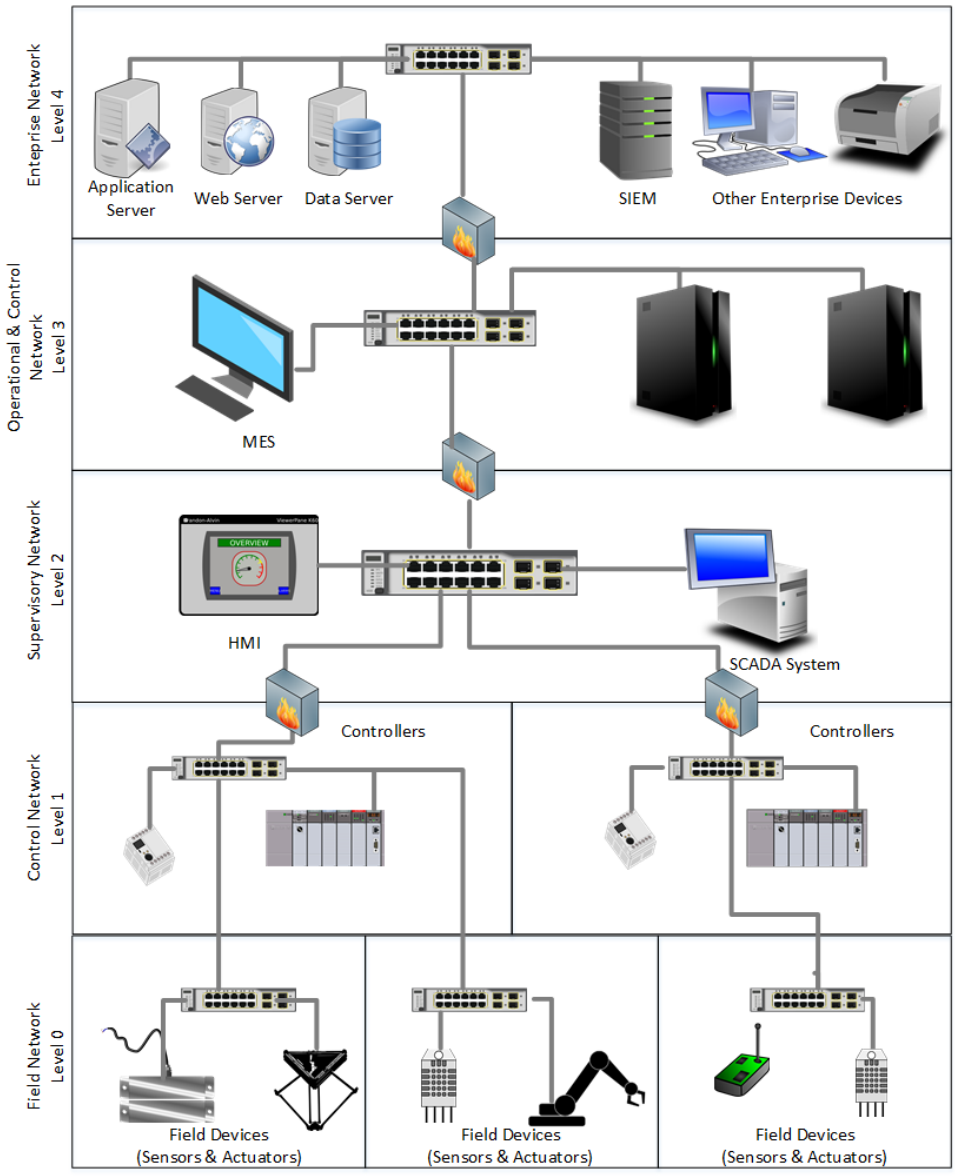


**Figure 1.** Reference Industrial Automation System Architecture derived from [15–17]. SIEM: Security Incident and Event Management; MES: Manufacturing Execution System; SCADA: Supervisory Control and Data Acquisition; HMI: Human Machine Interface.

Level 0 (i.e., Field Level) is comprised of the sensors and actuators that constitute the physical process. The devices that monitor and control local physical processes (e.g., Programmable Logic

Controllers and Remote Terminal Units) form Level 1 (i.e., Control Level). Monitoring and other management activities (i.e., alarm and alert handling) are carried out by operators at Level 2 (i.e., Supervisory Level) with support from supervisory technologies such as Supervisory Control and Data Acquisition systems (SCADA systems), Historians and Human Machine Interfaces (HMI). Level 3 (i.e., Operations Level) manages production work flows. Manufacturing and Execution Systems (MES) are popular at this level. Finally, Level 4 (i.e., Information Level) is comprised of IT systems that support the everyday operations of the organization and its business activities.

Furthermore, each of these levels may also be divided into subnetworks and distributed across different geographical locations. This distribution and the wide amount of components that constitute an IAS pose challenges to their management and security. For this, multiple solutions that integrate both centralized management and security capabilities have been integrated into IAS. Two of the most popular solutions are Security Incident and Event Management (SIEM) technologies and Operational Technology (OT) Management systems.

SIEM technologies are widely used in the IT field [18]. They allow for monitoring system components and manage security events and alerts through the aggregation, analysis and reporting of security information. Some of these SIEM technologies have included capabilities that facilitate Industrial Control System operation and management, which have made them suitable for IAS [15]. OT Management systems provide similar capabilities to that of SIEM technologies, however, they are more focused to IAS-specific operations such as control network monitoring and risk management (e.g., Industrial Defender Automation Systems Manager (ASM) [19]).

Both SIEM technologies and OT Management systems centralize their analysis and visualization components. SIEM technologies are often deployed at level 4 (i.e., Information Level), whereas OT Management systems are often deployed at levels 2 and 3 (i.e., Supervisory Level and Operations Level). In order for these technologies to provide protection to lower levels of the automation hierarchy, it is necessary that they provide capabilities that allow them to monitor network and components located at these lower levels or that they are capable of receiving information from other security solutions located at these network levels. Some of the security solutions capable of providing this information are databases, Antiviruses, Intrusion Detection Systems (IDS) (both for enterprise and industrial networks) and Intrusion Prevention Systems (IPS) [15].

Unfortunately, although the consolidation of these centralized security management technologies (i.e., SIEM technologies and OT Management systems) and their complementary security solutions allow for effectively detecting and alerting about system intrusions; the scope of their supported preventive capabilities (i.e., actions capable of blocking, disrupting, modifying, delaying and/or stopping an intrusion) may not cover lower levels of the automation hierarchy (i.e., levels 0–2). This occurs as these prevention capabilities are often provided by security solutions whose active response scope does not consider specific characteristics of IAS. Furthermore, there exist concerns related to the integration of active responses in IAS due to the fear of them potentially affecting the correct operation of the IAS [12–14] by either affecting its availability, performance or interrupting the communication with components located at higher levels of the system hierarchy (e.g., SIEM technologies, OT Management Systems, SCADA Systems, etc.). Therefore, the current industrial architectural and security trends pose a challenge for the integration of reactive protection in IAS.

## 3. Requirements for Reactive Protection in Industrial Automation Systems

The aim of the presented concept is to derive a feasible solution capable of actively protecting IAS against intrusions. Hence, it is necessary to identify and align inherent requirements from the reactive protection solution and other requirements from the industrial field (i.e., architectural and operational requirements). These requirements have been abstracted from the discussion of challenges performed in Section 2, as well as literature [7,20,21] in the field of industrial security provided by authorities such as the National Institute of Standards and Technology (NIST) and the SANS Institute.

### 3.1. Configurability and Automatic or Semi-Automatic Reactions to Intrusions (R1)

Human intervention when responding to intrusions often provides certain disadvantages that translate into increased costs and a higher vulnerability for the system. Higher costs are related to the human effort required to analyze an intrusion in order to select and execute an appropriate responsive action. The increased vulnerability emerges from the time interval between the detection of the intrusion and the execution of its response. During this time, the intrusion continues taking place and it could even be completed successfully. Hence, it is necessary to decrease the amount of human intervention required by automating some of the tasks commonly carried out by it. In [7,22], it is highlighted that IPS and Intrusion Response Systems (IRS) may require human tuning in order to decide which preventive actions to enable/disable for which type of alert. This tuning ensures that undesired reactive actions that may compromise the behaviour of the underlying system are not executed. Hence, providing higher assurance that allows for (semi-) automating the analysis and execution tasks—thus allowing pertinent and (near-) real-time reactions to intrusions.

### 3.2. Compliance with the ISA/IEC 62443 Series of Standards (R2)

The ISA/IEC 62443 series of Standards [23] are considered the future de facto reference standards for security in IAS [24]. One of the integral concepts of this series is the segmentation of the IAS network into different security zones. This allows to group components into sets that share similar security requirements. Hence, allowing to manage their security policies and mechanisms on a zone-to-zone basis. This allows for protecting zones against unauthorized access by minimizing possible security risks through the consideration of the least-privilege and white-listing principles. These principles are often achieved by controlling and limiting the communication among zones in order to only allow the communication that is necessary for the operation of the IAS. This is often performed by integrating network segmentation devices (e.g., industrial Firewalls or industrial IoT Gateways) and implementing security policies and security solutions in order to enforce such policies.

### 3.3. Ensure Correct Operation of the Underlying Automation System (R3)

During operation, IAS must meet three important operational requirements [25,26]: real-time capabilities, high availability and high performance. Failing to meet these requirements may negatively affect the reliability and safety of such systems. Hence, it is important that any additional components not related to the automated process itself do not negatively influence these requirements. This can be performed through the identification of the critical components that must be contemplated and the constraints or conditions that ensure their normal or expected operation.

### 3.4. Multi-Platform Support and Interoperability with Preexisting Solutions (R4)

Due to the advances resulting from the fourth industrial revolution, a wide range of system platforms and devices exist in the market of industrial solutions [27]. This requires that new solutions are capable of being deployed in such components in order to prove their competitiveness. Additionally, it is also important that they are capable of interacting with other components from different vendors [28]. This allows for exploiting their full potential by complementing certain features (e.g., active responses) with those of preexisting solutions in order to enhance their capabilities. Both interoperability and platform independence ensure that system integrators can select products that best fit their needs without the concern of being dependent on the manufacturer—hence providing more flexibility during the design phase of the IAS.

## 4. Related Work

Research in the field of intrusion detection in IAS has been extensive [25,26,29]. Most of it has focused on the detection of intrusions at the network level by implementing multiple anomaly detection approaches (e.g., automatic generation of Deterministic Finite Automation [30], One-Class

Support Vector Machine [31,32], among other Machine Learning approaches [32,33]). However, few of these contributions have considered active responses in the presence of intrusions, as their scope is often limited to the detection accuracy of its implemented approaches.

Hence, this section discusses related work in the field of IAS that have integrated these types of responses. The analysis of approaches implemented in this related work is clustered according to the specific system attributes that are affected due to the active response: network traffic or communication and individual IAS component or configuration. Furthermore, in order to identify gaps that are addressed by the presented contribution, the fulfillment of the requirements presented in Section 3 has been evaluated in each of the analyzed works.

### 4.1. Reactive Actions in Network Traffic or Communication

Active responses that affect network traffic or communication are commonly used to stop an intrusion or attack from reaching its target by either blocking-, modifying- or dropping network traffic. At this stage, it is unclear whether or not the intrusion has been successfully mitigated before its consequences have taken place in the IAS. The most common approach to execute this action is the integration of an inline component over the communication path. This component can be a commercial or open source product such as a Firewall or Network IDS, or another security component with similar capabilities.

In [13], an industrial Firewall system with intrusion detection capabilities is presented. This system is comprised of four different blocks: packet collection and control block, network layer access control block, application layer access control block and policy and alert management block. Both network- and application layer access control blocks constitute an access control mechanism comprised of four different filters, each of which analyzes different information regarding the network traffic. Based on this analysis and the policies located in the policy and alert management block, it is decided whether or not a network packet is allowed through the system. The packet collection and control block is in charge of executing this action by either delivering or blocking the network packet. Another approach that has benefited from the prevention capabilities of Firewalls is presented in [34]. In this contribution network attacks against Cyber-Physical Systems (CPS) are detected and prevented by implementing a hybrid approach using statistical analysis with fuzzy logic. This approach is capable of detecting anomalies that have been discovered in network packets that have passed through a firewall. Any packet with anomalies is discarded. The commercial IDS Silent Defense by Security Matters [35] also provides active responses in the presence of intrusions by dynamically adding new firewalls rules to an industrial Firewall (i.e., mGuard by Phoenix Contact) in order to block incoming network traffic.

Other approaches have also benefited from prevention capabilities supported by IDS. In [36], an anomaly-based Multi-Agent IDS is presented. This IDS implements an enhanced ant-based clustering approach for identification of intrusions and is comprised of six types of agents (i.e., monitoring agents, decision agents, action agents, coordination agents, user interface agents and registration agents). The preventive capabilities of the presented IDS are carried out by the action agents. These agents are capable of performing passive responses (i.e., log and notify of security-related events such as intrusions), as well as active responses (i.e., packet filtering and attack redirection towards a Honeynet). In [37], the open source Network IDS Snort [38] is used to detect and prevent intrusions in MODBUS RTU/ASCII traffic. In order to provide preventive capabilities, Snort is implemented in its inline mode which allows it to drop traffic according to special drop rules.

### 4.2. Reactive Actions in Individual IAS Components or Configurations

Active responses that affect individual IAS components or configurations are commonly used to counteract the effects of an intrusion. This means that at this stage the intrusion has already succeeded and its consequences affect the IAS. A wide range of approaches exist to execute these actions. This occurs due to the specificity of each of the individual IAS components and the configurations.

In [39], a dynamic response system for protection of SCADA systems is presented. This response system monitors and analyzes data related to the performance of both the physical process and the SCADA system in order to detect intrusions. This analysis implements signature-based and anomaly-based intrusion detection using forecasting models (i.e., AutoRegressive Integrated Moving Average) and classifiers (i.e., Naive Bayesian). Once an intrusion has been detected, the response system evaluates four criteria in order to select an active response with low impact to the IAS and its operational requirements. The evaluated criteria are: enhancement of security (C1), operational costs (C2), maintenance of normal operations (C3), impacts on properties, finance and human lives (C4). From this criteria, C4 is the one that defines whether or not human intervention is necessary to execute an active response. Although five active responses are supported by the response system (i.e., dropping malicious commands, termination of physical processes, replacement of compromised devices, one time authentication and isolation of compromised devices), only two of them can be executed without human intervention: dropping of malicious commands and one time authentication.

Another approach for protection of smart grid nodes is presented in [40]. This approach is based on game models and evaluates the impact of the behaviour of both the attacker and defender in order to select appropriate active responses to counteract the effects on an intrusion. These responses are executed by human users and are comprised of the following: cut off the energy of a sensor or maintain correct data and valid nodes by discarding data from malicious nodes and updating routing tables to exclude bad sensor nodes.

In [41], a protection approach for CPS is presented. This approach is based on a multi-layer architecture that considers special requirements for CPS. The layers of this architecture are the following: IT security, active protection, intrusion tolerance and physical security. Detection of intrusions and their corresponding active responses are supported by the intrusion tolerance layer. In this layer, intrusion detection is performed through model-based anomaly detection and supported by an impact assessment. The selection of the appropriate active responses is determined through a security strategy that integrates a game process. These responses are comprised of dynamic reconfiguration of system components.

Additional work regarding reactive responses in the presence of intrusions has been made within the context of the CockpitCI project [42]. This project focuses on the improvement of resiliency and dependability of Critical Infrastructures (CIs) through the identification of- and immediate response in the presence of security events (e.g., intrusions). This is performed by evaluating the possible consequences and impact (i.e., by evaluating the risk) of such security events and, in case it is necessary, alerting the operators in order to implement timely containment strategies (i.e., passive and active responses). Some of these strategies may execute automatic reactions. However, to the best of our knowledge, these reactions are mostly focused on ensuring the resiliency of the automation system in the presence of faults, rather than targeted attacks. An example of a preventive action mentioned in the literature is the restart of a component.

### *4.3. Comparison of Related Approaches and Identification of Research Gaps*

All previously presented approaches that integrate active responses in the presence of intrusions for IAS are compiled and rated in Table 1 according to their fulfillment of the requirements presented in Section 3. As it can be observed, none of these approaches are capable of fulfilling all these requirements.

Contributions that present approaches that support active responses that affect network traffic or communication are often ambiguous with regards to whether or not they are capable of maintaining the operational requirements of IAS (i.e., *R3*). Similar ambiguity is found with regards to multi-platform support and interoperability with preexisting solutions (i.e., *R4*) in contributions presenting approaches that support active responses that affect individual IAS components and configurations. This occurs, as the mechanisms to execute active responses are often system- or device-specific.

Furthermore, it can be observed that approaches that support active responses that affect network traffic or communication are more likely to integrate concepts related to the ISA/IEC 62443 series of Standards (i.e., *R2*). This higher compliance is supported, as many security components that aid in the execution of active responses already consider some of the concepts and trends related to industrial networks integrated in these Standards. On the other hand, approaches that support active responses that affect individual IAS components and configurations often neglect these aspects.

Moreover, although automatic and semi-automatic execution of active responses is supported by most of these approaches, they provide low configurability (i.e., *R1*). This occurs due to the predominant preference of integrating model-based approaches that allow for decreasing their configuration efforts.

Thus, a research gap is the lack of a security solution capable of providing configurable and automatic active protection against intrusions that ensures the correct operation of the underlying automation system while taking into consideration the following: current architectural and security trends defined by the ISA/IEC 62443 series of Standards, multi-platform support and interoperability with other security solutions.

**Table 1.** Overview of related approaches for reactive responses in Industrial Automation Systems (IAS) and ratings using Requirements for reactive protection in IAS.

| Approaches | R1 | R2 | R3 | R4 | Active Response |
|---|---|---|---|---|---|
| Kim et al. [13] | + | + | o | + | Packet filtering for access control |
| Nurjahan et al. [34] | + | + | o | + | Block incoming connections or drop network traffic |
| Security Matters [35] | + | ++ | o | + | Dynamically add Firewall rules |
| Tsang et al. [36] | o | - | o | o | Packet Filtering and Redirection of Attacks towards a Honeynet |
| Morris et al. [37] | + | o | o | ++ | Drop network traffic |
| Chen et al. [39] | + | - | ++ | o | Drop malicious commands, terminate physical processes, replace or isolate compromised devices and one time authentication |
| Hewett et al. [40] | o | - | o | o | Cut energy to sensor, discard data from malicious node, update routing tables |
| Huang et al. [41] | + | - | ++ | - | Dynamic reconfiguration of system components |
| CockpitCI [42] | o | ++ | ++ | o | Restart of a component |

**++**: fulfilled, **+**: partially fulfilled, **-**: not fulfilled, **o**: unclear; **R1**: Configurability and automatic or semi-automatic reactions to intrusions, **R2**: Compliance with the ISA/IEC 62443 series of Standards, **R3**: Ensure correct operation of the underlying automation system, **R4**: Multi-platform support and interoperability with preexisting solutions.

## 5. Reactive Protection Concept for Industrial Automation Systems

This section presents a concept of reactive protection for IAS from which a Reactive Protection System is derived. This concept addresses the requirements discussed in Section 3. Special attention is given to its suitability for generic IAS architectures (i.e., Figure 1) and its consideration of concepts presented in the ISA/IEC 62443 series of Standards.

First, the scope of protection coverage provided by the Reactive Protection System is presented. This includes pre-requirements and expected protection capabilities. Afterwards, the components that constitute the Reactive Protection System are presented. Finally, a deeper discussion is given regarding the security and operational policies, as well as reactive actions that can be considered by the presented concept taking into account well-known architectural and operational trends of real automation systems.

### *5.1. Pre-Requirements and Limitations of the Reactive Protection System*

The presented system is capable of executing active responses. These responses are referred to as *reactive actions* in this work, as they occur as active responses to specific security events (i.e., intrusions). In order to do so, it is necessary that the information regarding these events be provided to the Reactive Protection System. This information can be provided by third-party components that monitor and analyze system information in order to detect intrusions such as Network or Host IDS [25,26,43], SIEM technologies [18] and other event correlation systems [44]. Due to this reason, the presented system is not defined as an IPS, as it lacks the ability to capture and analyze the information in order to detect intrusions and generate security-related events.

Hence, the capabilities of the presented Reactive Protection System are limited to analysis of security-related events identified or detected by third-party components. Based on this analysis, the system decides whether or not an appropriate reactive action is possible. Provided that this action is feasible (i.e., supported by the system and does not affect the operation of the underlying automation system), the system enacts it. This may result in either the reactive action being fully executed by the Reactive Protection System itself, or the Reactive Protection System providing the information necessary to another component capable of executing it, which may result in the prevention of an intrusion.

### *5.2. Components of the Reactive Protection System*

The presented Reactive Protection System is comprised of four different components as observed in Figure 2: Configuration Module, Policy and Action Knowledge Base, Active Response Module and Communication Module. This architecture was designed taking into consideration the requirements for reactive protection in IAS discussed in Section 3. An overview of this is provided in Table 2.

This system can be deployed at each network segment located in levels 0–2 of the automation hierarchy (Figure 1) in order to manage its policies (i.e., security and operational policies) and provide security through reactive protection in the presence of intrusions.

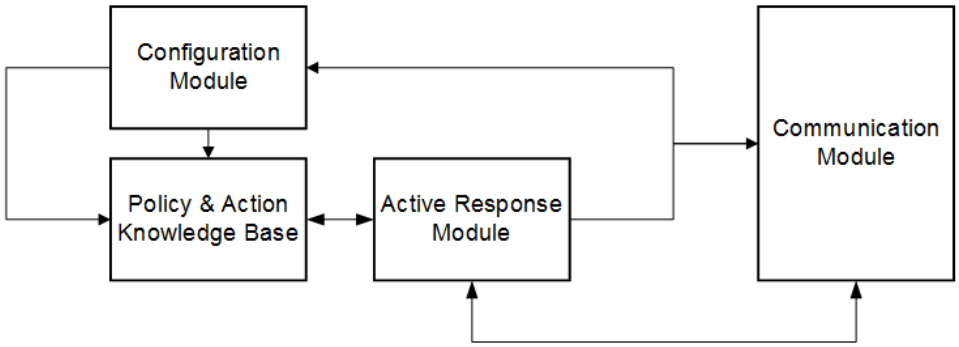


**Figure 2.** System components of the Reactive Protection System.

**Table 2.** Mapping between Requirements and Reactive Protection System Components.

| System Component | R1 | R2 | R3 | R4 |
|---|---|---|---|---|
| Communication Module | ✓ | | | ✓ |
| Configuration Module | ✓ | | | |
| Active Response Module | ✓ | ✓ | ✓ | |
| Policy & Action Knowledge Base | | ✓ | ✓ | |

**R1**: Configurability and automatic or semi-automatic reactions to intrusions, **R2**: Compliance with the ISA/IEC 62443 series of Standards, **R3**: Ensure correct operation of the underlying automation system, **R4**: Multi-platform support and interoperability with preexisting solutions.

The following subsections describe each of the components of this Reactive Protection System in more detail.

#### 5.2.1. Communication Module

The *Communication Module* provides the communication capabilities of the presented system. It receives security events from third-party components. These events are forwarded to the *Active Response Module* for analysis. Provided this analysis results in the execution of an action that requires providing information to third-party components in order to disrupt or counteract an intrusion, this module also delivers the information required by such components. An example of this is the following. The *Active Response Module* receives information of a Denial of Service (DoS) attack being carried out. After this information has been analyzed, it has been selected to add a new rule to a Firewall located on another device. Hence, the *Active Response Module* provides the information required to add such rule to the *Communication Module*, which later forwards it to the corresponding device.

This module is also capable of receiving Reactive Protection System-specific configuration information, which allows for remotely configuring it. This configuration information is comprised of security and operational policies, as well as information required to tune the reactive actions. This provides high configurability and interoperability as defined by *R1* and *R4* in Section 3.

#### 5.2.2. Configuration Module

The *Configuration Module* validates the configurations of the Reactive Protection System. This validation verifies that new or updated configurations do not conflict with preexisting ones. These configurations are comprised of security and operational policies, as well as action-related configurations. These action-related configurations allow for tuning reactive actions. After these configurations have been validated, they are stored in the *Policy & Action Knowledge Base*. On the other hand, configurations related to runtime execution of the reactive system are also applied to the *Active Response Module*. This provides configurability as defined by *R1* in Section 3.

#### 5.2.3. Active Response Module

The *Active Response Module* receives and analyzes security events from third-party components through the *Communication Module*. The analysis of these security events is performed through consultation with the *Policy & Action Knowledge Base* using association-based approaches (e.g., rule-based [45]). Once a security event has been identified as a violation to the corresponding segment security policies (i.e., identified as an intrusion), the *Active Response Module* verifies whether or not there exists an appropriate reactive action to counteract such event. If an associated reactive action is identified, the *Active Response Module* validates whether the action violates the segment operational policies contained within the *Policy & Action Knowledge Base*. Provided that no operational policy is violated, the *Active Response Module* executes the appropriate action. This provides (semi-) automatic reactions in the presence of intrusions that do not influence the operation of the IAS as mandated by *R1* and *R3* defined in Section 3. It also provides compliance with the ISA/IEC 62443 series of Standards (i.e., *R2*), by enabling the execution of mitigation strategies suggested by these Standards.

#### 5.2.4. Policy and Action Knowledge Base

The *Policy & Action Knowledge Base* is comprised of the non-volatile security and operational policies that constitute the network segment reactive protection, as well as other configurations of the Reactive Protection System. The operational policies represent constraints that must be maintained in order to ensure the correct operation of the automation system. On the other hand, the security policies allow for validating whether a security event received from the *Communication Module* compromises the security of the respective zone (i.e., violates the segment security policies). Security policies may have corresponding reactive actions that allow for disrupting, blocking or counteracting in other ways the security intrusion identified from the security event information—hence providing compliance with

the ISA/IEC 62443 series of Standards (i.e., *R2*) and ensuring the correct operation of the underlying automation system (i.e., *R3*).

### 5.3. Security Policies, Operational Policies and Reactive Actions in Real-Life Automation Systems

The foundation for the presented concept for reactive protection are current architectural trends in IAS and the security and operational policies, as well as reactive actions suitable for these trends.

Modern industrial networks are often divided into segments and segregated [20]. This improves their performance, facilitates their management and increases their security [20,46]. The ISA/IEC 62443 series of Standards has included and further refined these concepts. It has also considered operational policies and the management of security policies on a zone-to-zone basis critical to maintain the security of IAS. This series of standards, as well as guidelines presented in [20], especially highlight the importance of security mechanisms located at the edge of each network zone.

Considering the aforementioned architectural and security trends, a classification of security and operational policies, as well as possible reactive actions are presented in the following subsections. It is important to highlight that the policies and actions that may suit specific IAS should be analyzed on a case-to-case basis. However, in this section, they are presented in a more general way in order to outline the scope of the opportunities that the presented concept provides.

First, security policies are derived from security requirements explicitly discussed in ISA/IEC 62443-3-3 (i.e., ISA/IEC 62443 Part 3-3 System security requirements and security levels). This standard part has been considered as it provides a set of well-defined security requirements that should be considered by system integrators in order to protect the correct operation of their systems [47]. Afterwards, operational policies are derived from guidelines [20] that present a better understanding of the behaviour of automation systems and the impact security may have on them. Following this, possible reactive actions are discussed. These reactive actions are derived from the security policies themselves, as well as suggestions provided by the aforementioned security standards and guidelines for IAS. Finally, a discussion regarding how security-, operational policies and reactive actions provide network segment reactive protection is provided.

#### 5.3.1. Security Policies

The following classes of security policies have been identified based on four different components that constitute a system: communication, computer resources, users and sessions, as well as services. A fifth class has been integrated in order to represent well-known events that require immediate attention. These policies have been selected, as they are relevant for IAS and provide opportunities for reactive actions that may be integrated into the reactive protection concept presented in this work.

- **Communication Management (S1):** These policies define constraints related to allowed or disallowed communication among system components. These policies often consider communication-specific attributes such as source and destination addresses (i.e., IP addresses, MAC addresses), logical port numbers, etc. This class allows for providing security solely based on characteristics from the communication without considering more detailed information such as user- or service-specific information.
- **Computational Resource Management (S2):** These policies define constraints related to computational resources found in the automation system. These policies often consider resources that can be measured on a system-, multi-device- or device-specific level. Examples of these resources are the following: network load, RAM, ROM and CPU usage, etc.
- **User Access Control and Session Management (S3):** These policies are related to the identification and authentication of users, devices or other entities that possess an identity, as well as the sessions and other events resulting from such authentication. Specific policies of this category may include but are not limited to constraints related to identity, authentication and

session information (e.g., number of failed authentication attempts, authentication and session status and other detailed information).

- **Service Management (S4)**: These policies define allowed or disallowed services or protocols, as well as their configurations. They do not consider user-specific information regarding the use of such services.
- **Incidents (S5)**: These policies represent well-known conditions that require immediate action. Some of these are the following: malware detection and vulnerability detection.

The aforementioned classification allows for defining simple and straightforward policies. Although multiple security policy languages and standards exist [48], the presented concept does not consider one specifically. This is done in order to provide ambiguity that may allow in the future to adapt this concept for any desired language or standard. Hence, in this concept, policies are considered as abstract rules. This is possible as policies often contain information that address the following questions [49]: *what*, *who*, *when* and *where*. Furthermore, most policy languages are based on two different paradigms [48]: *Event-Condition-Action* or *Condition-Action* paradigms.

From these two paradigms, the most suitable for the reactive protection concept presented in this work is the *Event-Condition-Action* paradigm, as it requires an *Event* element that triggers the execution of the *Action*. In the presented concept, an *Event* is any security event received by the Reactive Protection System from third-party components. A *Condition* is comprised of the security constraints that must be met (e.g., service A must not be running). Finally, an *Action* may be any reactive action that helps meet the identified *Condition* or that helps counteract the effects of an intrusion.

In addition, this simple policy classification allows for further building more complex policies that may merge two or more classes. This is done, as it may be possible that the information regarding the security event provided to the Reactive Protection System comes from simple or more complex security solutions. Examples of this case are the following: simple security event information may be received from a simple Syslog [50] client located on a device. The event information provided by this client may be limited to only a notification that contains timing information and simple event information (e.g., service A has started running). This case may fall into the *S4* policy class. On the other hand, more complex security event information may be received from an IDS that provides not only the status change of the service, but also additional information such as the source of the change (e.g., user Y has started service A). Hence, this example may fall into the *S4* and *S3* classes.

#### 5.3.2. Operational Policies

The following classes of operational policies have been identified based on four critical assets of automation systems: communication, services, performance and configurations.

- **Communication Availability (O1)**: These policies focus on defining the state of communication that should always be maintained and never be interrupted or influenced. This communication is represented by communication-specific attributes as those described in *S1*. However, these policies focus solely on communication required to perform the automation and management tasks of the system (e.g., communication from device A to device B must always be maintained).
- **User Access and Service Availability (O2)**: These policies define conditions regarding user access and services that must always be met. These conditions are necessary to carry out the automation or management tasks. This class differs from *O1* as more specific information about a service is provided (e.g., user A must always have access to service X).
- **Performance Constraints (O3)**: These policies define conditions regarding performance that must be maintained throughout the whole automation system or on multiple or specific devices of it. The measure of performance should be provided by a third-party component (e.g., Network load must not exceed the threshold T).
- **Configuration Constraints (O4)**: These policies define conditions regarding configurations that must be maintained. These conditions ensure the correct operation of the automation system and

hence, are often related to automation devices (e.g., firmware version X must be installed in all devices type Z).

The aforementioned classes allow for defining policies that help meet the performance and availability requirements for IAS as defined in [20] and considered in *R3* from Section 3.

It is also important to highlight that, although these policies are similar to the security policies mentioned above, they are not the same. Security policies are obtained from security requirements, whereas operational policies are derived from operational requirements. Additionally, a security policy violation is a result of something endangering the system (e.g., intrusion), whereas an operational policy violation may result from other non-security related events (e.g., faults). Furthermore operational policies focus solely on requirements or conditions from the automation system itself and not other non-automation related system components.

#### 5.3.3. Reactive Actions

The following classes of reactive actions have been derived by identifying possible countermeasures to violations of the aforementioned security policies. These actions constitute the *Action* element of the aforementioned security policies:

- **Block User Account (A1):** A user account is blocked. This may result in failure during authentication.
- **Revoke User Privileges (A2):** Privileges belonging to a user account are revoked. This may result in failed authorization to carry out certain actions or access certain services.
- **Communication Session Termination (A3):** A communication session is either locked or terminated based on session-specific information (e.g., user participating on the session).
- **Communication Termination (A4):** An active communication is terminated based on communication-specific attributes (e.g., protocol, logical port, routing addresses, etc.).
- **On-demand Analysis (A5):** An analysis of specific system components is carried out on-demand. Examples of this analysis may be on-demand audits, scans or other types of check (e.g., antivirus check).
- **On-demand post-intrusion configuration and information collection (A6):** After an intrusion has been detected, a change is made in the current configuration and state of an asset. Additionally, information that may be used by third-party components for further analysis may be collected from certain system components (e.g., event logs are collected).

Execution of each of these actions without consideration of the aforementioned operational policies may influence the operational requirements of IAS (e.g., real-time capabilities, high performance and availability).

Furthermore, it is important to highlight that the reactive protection concept presented in this work does not necessarily require the full execution of the reactive actions to be carried out by the Reactive Protection System. This system can only prepare the information necessary to execute the action and later on forward it to an appropriate component that has the features to do so. Examples of this may be the following: blocking of a user account or revocation of user privileges may be carried out by a user management system. Communication may be terminated through one of the communication parties (e.g., Virtual Private Network session termination on either a server or client) or by a third-party component (e.g., adding a new firewall rule dynamically). A network scan may be done by a firewall. Finally, a log collection may be carried out by a log collection and management system.

#### 5.3.4. Network Segment Reactive Protection

Security policies and reactive actions are capable of providing protection against intrusions. However, their suitability for IAS may be questioned. In order to address this concern, it is necessary to also consider the operational policies. For this, the presented concept suggests the consideration of

both operational and security policies on a zone-to-zone basis. This allows for providing decentralized protection to the automation system. Another advantage of this decentralized approach is that it allows for analyzing security events from multiple sources (e.g., third-party security solutions)—hence meeting *R4* defined in Section 3.

Figure 3 presents the process that is carried out by the Reactive Protection System presented in this work. This process starts with the reception of a security-related event. This event may be received from a third-party component over the network. Afterwards, this event is analyzed in order to validate whether or not a network segment security policy has been violated. If a violation has occurred, then an appropriate reactive action is chosen. If the reactive action is supported by the Reactive Protection System, then it is evaluated against the segment operational policies. If the reactive action violates an operational policy, it is not executed and this result is logged. On the other hand, if the reactive action does not violate any operational policy, the reactive action is executed.

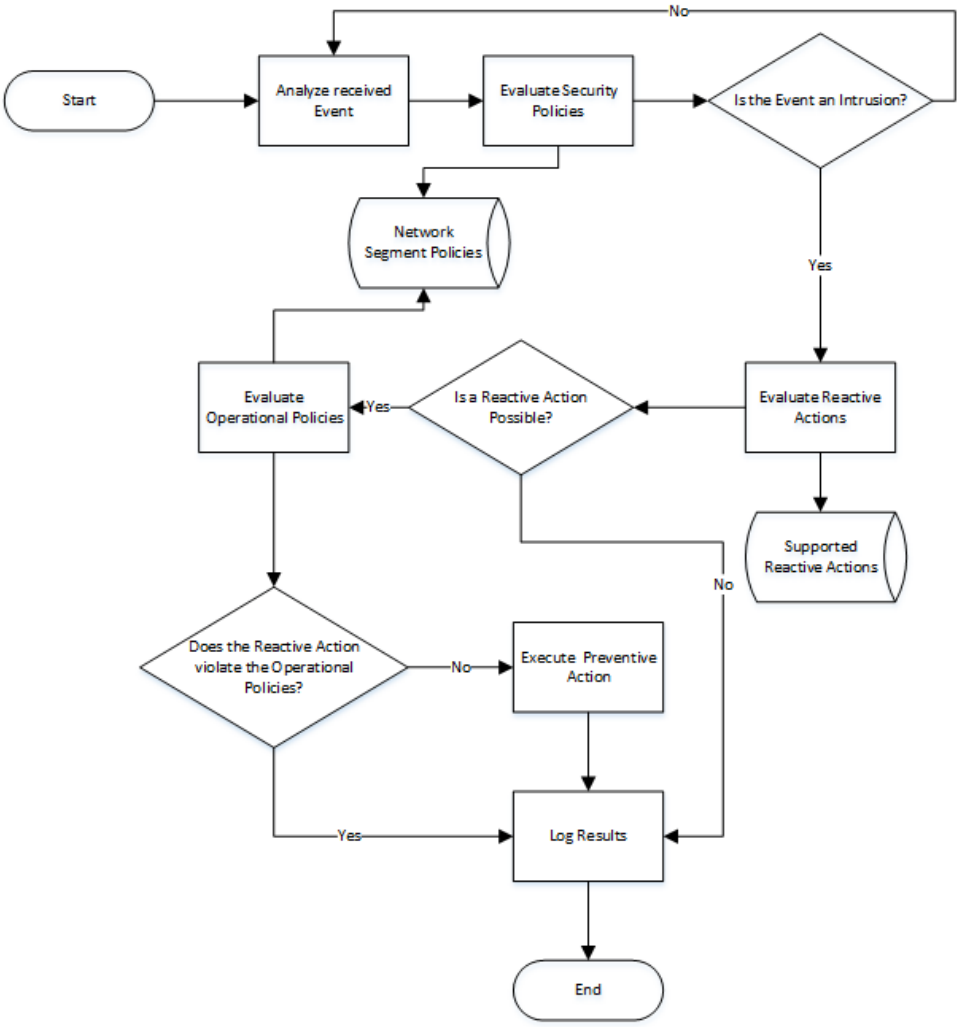


**Figure 3.** Information flow of the presented concept for reactive protection.

As it has been observed, this concept ensures that no reactive action will be executed if it compromises the operation of the automation system as long as the operational policies are well-defined. Although this requires human effort for its configuration, it provides the advantage of being able to react to intrusions without human intervention—hence providing a quick response in the presence of intrusions during normal operation of the system (*R1* defined in Section 3).

## 6. Reactive Protection System Applicability

In the previous section, a concept for a Reactive Protection System was presented. During this concept discussion, a system architecture and a set of guidelines were provided from which a Reactive Protection System, its reactive actions and security and operational policies can be designed. In order to clarify the applicability of this concept, this section presents a discussion regarding its integration in IAS. This includes a discussion of its architectural deployment and interaction with other system components. It also presents a set of security policies, intrusions and reactive actions that can be supported by this system. Finally, a discussion regarding its significance and challenges is given.

### *6.1. Integration in Industrial Automation Systems*

In order to demonstrate how the Reactive Protection System can be integrated into an IAS, the IAS reference architecture (Figure 1) has been modified and extended (Figure 4) in order to integrate security components and architectural schemes commonly used for industrial networks.

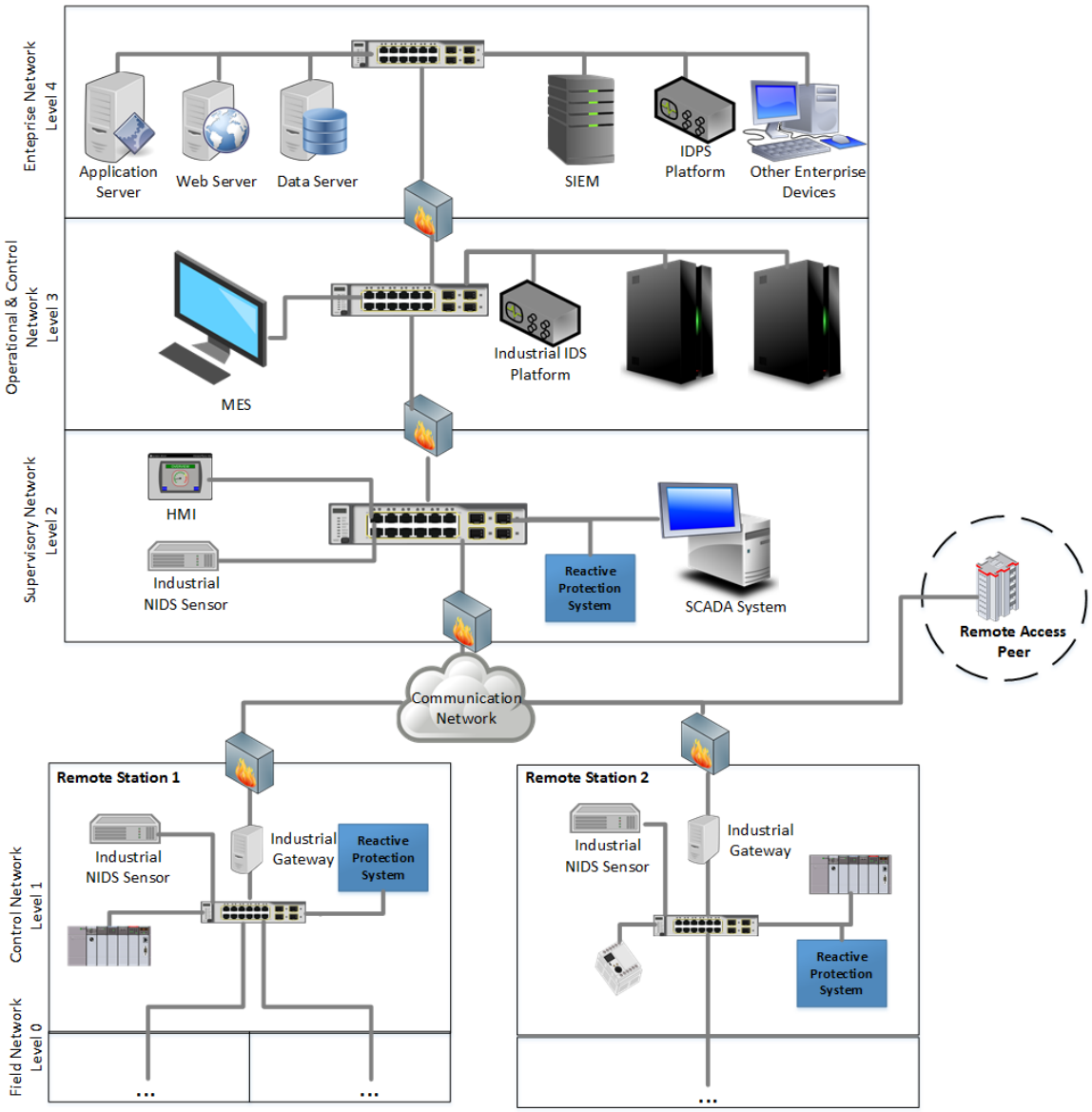


**Figure 4.** Extended Reference IAS Architecture (Figure 1) with remote access and security components.

An Intrusion Detection and Prevention System (IDPS) has been integrated into the Enterprise Network (Level 4). This IDPS allows for monitoring this network in order to identify intrusions occurring at this level. On the other hand, an Industrial Network IDS has been integrated in the Industrial Control Network (Levels 1, 2 and 3). This Industrial Network IDS consists of a centralized platform located in the Operational and Control Network that analyzes information provided by sensors located at lower levels (i.e., Supervisory and Control Networks).

The Field and Control Networks have been divided into two remote stations. This has occurred in order to represent a distributed IAS. Moreover, an Industrial Gateway (also known as IoT Gateway) has been deployed in each of these remote stations. Industrial Gateways are a new trend in IAS that has been gaining popularity over the past years [51–53]. They are devices that allow for *"establishing and maintaining a secure, robust, fault-tolerant connection between the cloud, and the edge devices to collect and aggregate device data and to manage the device"* [54]. These devices may also provide extended capabilities depending on their manufacturer.

A Remote Access Point for the Supervisory and Control Networks has been integrated. This occurs as remote service access is a common application in IAS, especially in distributed IAS. Examples of this are the following: remote software updates [55], remote patch management and maintenance [21], remote programming, parametrization, monitoring and diagnosis [20,56], etc.

An abstract Communication Network represents the communication between the remote stations, the Supervisory Network and the Remote Access Peer. This Communication Network can be any of the following: the Internet, a Wide Area Network (WAN), a Local Area Network (LAN), etc.

Finally, a Reactive Protection System is located in each network zone at the Control and Supervisory Levels (i.e., Levels 1 and 2).

As discussed in Section 5, the Reactive Protection Systems receive security-related events from third-party security components located in the IAS. These events may refer to an intrusion or another security violation. After a Reactive Protection System receives a security-related event, it analyzes it in order to verify whether or not a segment security policy for its corresponding network zone was violated. If a security policy violation occurred, it verifies whether or not a reactive action is possible (i.e., is supported by the Reactive Protection System and does not violate any of its zone operational policies). If a reactive action is possible, then it executes it or provides the necessary information to a third-party security component. The third-party security components that may provide security-related events information to the Reactive Protection System or that may execute reactive action in the extended IAS architecture are the following: SIEM, IDPS Platform, Industrial IDS Platform, Industrial Gateway or Firewalls. More security components can be embedded in other IAS devices such as Engineering Workstations; however, they are neglected in this architecture in order to provide more clarity and simplicity for discussion.

An example of an interaction between a Reactive Protection System and third-party security components is the following: the Industrial IDS has detected abnormal behaviour in the Remote Station 1 communication which it notifies to the Reactive Protection System located at the Remote Station 1. This Reactive Protection System contains a security policy with a supported reactive action that handles such event. This reactive action refers to a device scan to be performed by the Industrial Firewall located in Remote Station 1. Hence, the Reactive Protection System provides the information necessary to the Industrial Firewall in order to perform such scan. This scan may potentially identify an ongoing or a successful intrusion, which provides an opportunity to counteract its effects.

### 6.2. Security Policies and Intrusions

Following the approach presented in Section 5.3.1 and the extended reference IAS architecture and its components (Figure 4), fifteen security policies have been derived. Table 3 describes each of these policies and to which security policy class each of them belongs. It also presents for each of these policies a corresponding security-related event example. This example provides a source device

(i.e., third-party security component that detected the intrusion or collected the security-related event information) and a small description of a security-related event.

These policies and event information are represented in natural language in order to provide a simple and clear description of each of them. However, for their technical implementation, it is recommended to use one of the many policy languages and event formats that exist [48,57].

As it can be observed from Table 3, an Industrial Network IDS can provide information regarding communication, user and service events (i.e., *S1*, *S4*). One example of this is the identification of a new Firmware version being downloaded into a PLC. Once the Reactive Protection System is notified of this event by the Industrial Network IDS, it verifies its network zone security policies. This verification may result in the identification of a security policy that is violated (i.e., *SP9*), which would result in a reactive action (i.e., active response) being necessary.

**Table 3.** Examples of Security Policies (SP) and their security-related events.

| **Security Policies** | | | **Security-Related Events** | |
|---|---|---|---|---|
| **Class** | **Number** | **Description** | **Source Device** | **Description** |
| S1 | SP1 | Disabled Debug Port *123* in Devices of Type *T1* (PLCs) | Industrial Network IDS | Enabled Debug Port *123* on Device *A* of Type *T1* |
| | SP2 | *X* maximum number of TCP connections for all IP Addresses on all ports | | *X* + 1 simultaneous TCP connections |
| S2 | SP3 | Disable all USB ports in Device *A* | Host Device | USB dongle plugged-in in Device A |
| | SP4 | Maximum RAM Usage Threshold *T%* for Device *A* | | *T* + 1% RAM Usage in Device *A* |
| | SP5 | *X* MB Maximum Audit Storage for Device *A* | | *X* + 1 MB Audit storage in Device *A* |
| S3 | SP6 | *X* maximum failed Login attempts per User over a period of *T* seconds | User Management | User with username *N2* failed to login *X* + 1 times within a period of $T - 1$ seconds |
| | SP7 | *X* maximum failed connection attempts per Device over a period of *T* seconds | Specific Service | Device *A* failed to connect *X* + 1 times within a period of $T - 1$ seconds |
| S4 | SP8 | Maintenance of Device *A* enabled between *XX:00* and *YY:00* hours | Host Device | Device A Firmware Update completed at *YY:01* hours |
| | SP9 | Firmware version *X* on all devices of type *T1* | Industrial Network IDS | Firmware Version $X - 1$ on Device A of type *T1* |
| | SP10 | Patch version *X* on all devices of type *T2* | | Patch Version $X - 1$ on Device A of type *T2* |
| | SP11 | No PLC Application Download when PLC Application is running | PLC Programming Application | PLC Application download succeeded on Device *A* while PLC status running |
| | SP12 | No PLC Application Download with FTP | Industrial Network IDS | PLC Application downloaded to IP *X.X.X.X* with FTP |
| S5 | SP13 | Vulnerability detected | Firewall Port Scan | Buffer Overflow vulnerability detected in Application *P1* in Device *A* |
| | SP14 | Malware Detected | Workstation Antivirus | Malware *ABCDE* Detected in Device *A* |
| | SP15 | Unauthorized Wireless Device Detected | Industrial Network IDS | Unauthorized Wireless Device with MAC *FGHIJ* |

**S1**: Communication Management, **S2**: Computational Resource Management, **S3**: User Access Control & Session Management, **S4**: Service Management, **S5**: Incidents.

This active response is independent from any other response (i.e., active or passive) that may be supported by the Industrial Network IDS. It is the choice of the system integrators and security experts to decide which responses are appropriate in the presence of which events; hence, this has to be configured and defined before the deployment of the IAS or during maintenance.

An advantage of the Reactive Protection System is that it is also capable of complementing other components that do not provide a high degree of sophistication and analysis like an Industrial Network IDS. An example of this is the security policy *SP4* that validates a RAM usage threshold. Its corresponding security-related event can be received from a Host Device and not a sophisticated security solution. This event may be provided by a simple client application that monitors the RAM usage on the host device or a Host IDS.

After discussion of the security policies, their corresponding intrusions are presented in Table 4. These intrusions are comprised of security attacks and other events (e.g., misuses and misconfigurations) in IAS that may threaten the security of the system (i.e., violate the security policies). They have been derived from [34,58].

It is important to highlight that some of these intrusions may violate more than one security policy. Hence, it is necessary to properly configure both the security policies, and their reactive actions in order to avoid conflicts (e.g., one intrusion generates two security policy violations that executes two conflicting reactive actions).

Both DoS and SYN Flood attacks (*I1* and *I3*) may result in a big amount of simultaneous connections and an overhead in the performance of the targeted device (i.e., violates *SP2* and *SP4*). In wireless devices, a Jamming attack (*I2*) may be caused by an unauthorized wireless device (i.e., violating *SP15*). A Brute Force Attack (*I4*) and misuse in user authentication by users (*I8*) may exceed the maximum amount of login or connection attempts (i.e., violating *SP6* and *SP7*).

**Table 4.** Mapping between examples of intrusions and their corresponding security policies.

| Intrusions | | Security Policies | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **#** | **Name** | **SP1** | **SP2** | **SP3** | **SP4** | **SP5** | **SP6** | **SP7** | **SP8** | **SP9** | **SP10** | **SP11** | **SP12** | **SP13** | **SP14** | **SP15** |
| I1 | DoS | | ✓ | | ✓ | | | | | | | | | | | |
| I2 | Jamming | | | | | | | | | | | | | | | ✓ |
| I3 | SYN Flood | | ✓ | | ✓ | | | | | | | | | | | |
| I4 | Brute Force Attack | | | | | | ✓ | ✓ | | | | | | | | |
| I5 | Malware Injection | ✓ | | ✓ | ✓ | | | | | ✓ | ✓ | | ✓ | | ✓ | |
| I6 | Buffer Overflow | | | | | | | | | | | | | ✓ | | |
| I7 | Malicious PLC App. Download | | | | | | | | ✓ | | | ✓ | ✓ | | ✓ | |
| I8 | Misuse of Service & User Account | | | | | | ✓ | ✓ | ✓ | | | ✓ | | | | |
| I9 | Misuse of Computational Resources | | | | ✓ | ✓ | | | | | | | | | | |
| I10 | Misconfiguration | ✓ | | ✓ | | ✓ | | | | | ✓ | | ✓ | ✓ | | |

**SP1**: Enabled Debug Port *123* on Device *A* of Type *T1*, **SP2**: $X + 1$ simultaneous TCP connections, **SP3**: USB dongle plugged-in in Device A, **SP4**: $X + 1\%$ RAM Usage in Device *A*, **SP5**: $X + 1$ MB Audit storage in Device *A*, **SP6**: User with username *N2* failed to login $X + 1$ times within a period of $T - 1$ seconds, **SP7**: Device *A* failed to connect $X + 1$ times within a period of $T - 1$ seconds, **SP8**: Device A Firmware Update completed at *YY:01*, **SP9**: Firmware Version $X - 1$ on Device A of type *T1*, **SP10**: Patch Version $X - 1$ on Device A of type *T2*, **SP11**: PLC Application download succeeded on Device *A* while PLC status running, **SP12**: PLC Application downloaded to IP *X.X.X.X* with FTP, **SP13**: Buffer Overflow vulnerability detected in Application *P1* in Device *A*, **SP14**: Malware *ABCDE* Detected in Device *A*, **SP15**: Unauthorized Wireless Device with MAC *FGHIJ*.

On the other hand, Malware (*I5*) may open undesired logical and physical ports (i.e., violating *SP1* and *SP3*) providing a backdoor for intruders. It may also consume undesired computational resources of the target device resulting in exceeding predefined thresholds (i.e., violating *SP4*) and download malicious software (i.e., violating *SP9*, *SP10*, *SP12* and *SP14*). Similarly, malicious software can be downloaded into the PLC by violating security policies describing maintenance time, configurations and other circumstances (i.e., *SP8*, *SP11*, *SP12* and *SP14*). Misuse of computational resources may result in violation of security policies related to maximum threshold of both RAM usage and audit storage (i.e., violating *SP4* and *SP5*). Finally, misconfigurations in the system components may result in violation of security policies similar to those done by the Malware. Undesired services, logical and

hardware ports can be used (i.e., *SP12*, *SP1* and *SP3*). The audit storage threshold can be bypassed (i.e., *SP5*). Vulnerable software components can be installed on the target device providing opportunities for malicious users (i.e., *SP10* and *SP13*).

### *6.3. Reactive Actions in the Presence of Intrusions*

From the aforementioned security policies and intrusions (Tables 3 and 4), it is known that security-related event information analyzed by the Reactive Protection System can be provided by third-party components. Similarly, the Reactive Protection System can provide information to these components in order to execute the reactive actions required by each security policy.

In order to mitigate and counteract the intrusions presented in Table 4 ((i.e., *I1–I10*), fifteen possible reactive actions have been derived. These reactive actions have been derived from the literature review performed in Section 4, the guidelines presented in Section 5.3.3 and the empirical knowledge of the third-party security components outlined in Figure 4.

Table 5 presents these reactive actions, their corresponding third-party security components capable of executing them and the intrusions that each of them help counteract or mitigate. It is important to highlight that these reactive actions are executed according to the security and operational policies of the Reactive Protection System. An action is executed only if a security policy has been violated, it has an associated reactive action and this action does not violate an operational policy.

**Table 5.** Mapping between examples of intrusions and their corresponding reactive actions.

| **Reactive Actions** | | | | **Intrusions** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Class** | **#** | **Description** | **Device** | **I1** | **I2** | **I3** | **I4** | **I5** | **I6** | **I7** | **I8** | **I9** | **I10** |
| A1 | RA1 | (Temporarily) block User Account | User Management | | | | ✓ | | | | ✓ | | |
| A2 | RA2 | Revoke User Privileges | | | | | ✓ | | | | ✓ | | |
| A3 | RA3 | Session Lock | Application Server, User Management | | | | ✓ | | | | ✓ | | |
| | RA4 | VPN Session Termination | VPN Endpoint | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | |
| A4 | RA5 | Traffic Redirection | IDS | ✓ | ✓ | ✓ | ✓ | | | | | | |
| | RA6 | Rate Limiting | Firewall, Application Server | ✓ | ✓ | ✓ | ✓ | | | | | | |
| | RA7 | New Dynamic Firewall Rules | Firewall | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | |
| A5 | RA8 | Scan Devices on Network | Router, Firewall | | | | | ✓ | ✓ | | | | |
| | RA9 | Antivirus Scan | Antivirus | | | | ✓ | ✓ | | | | | |
| | RA10 | Device Audit | Industrial Network IDS, SIEM | | | | ✓ | ✓ | | ✓ | | | ✓ |
| A6 | RA11 | Back Up Restore | Industrial Network IDS | | | | | ✓ | | ✓ | | | ✓ |
| | RA12 | Component Restart | Host | | ✓ | | | | | | | | ✓ |
| | RA13 | Disable USB Physical Ports | | | | ✓ | | | | | | | |
| | RA14 | Device Reconfiguration | | | | | | | | | | | ✓ |
| | RA15 | Collect Logs or Audit Records | Log Management System, SIEM | | | | | | | | | ✓ | ✓ |

**I1**: DoS, **I2**: Jamming, **I3**: SYN Flood, **I4**: Brute Force Attack, **I5**: Malware Injection, **I6**: Buffer Overflow, **I7**: Malicious PLC Application Download, **I8**: Misuse of Service & User Account, **I9**: Misuse of Computational Resources, **I10**: Misconfiguration; **A1**: Block User Account, **A2**: Revoke User Privileges, **A3**: Communication Session Termination & Communication Termination, **A4**: On-demand Analysis, **A5**: On-demand post-intrusion information collection.

Brute Force attacks, misuses caused by users and communication sessions (i.e., *I4* and *I8*) can be mitigated by a User Management System. This system may block a user account, revoke its privileges or lock a session (i.e., *RA1*, *RA2* and *RA3*). An application server can also lock or block a session. After

the Reactive Protection System has performed any of these actions, it may be necessary for a human to analyze whether or not it is required to undo these changes (i.e., unblocking a user).

Traffic redirection and Rate Limiting (i.e., *RA5* and *RA6*) supported by some IDS, Firewalls and Application Servers help mitigate intrusions that increase the network rate (i.e *I1*, *I2*, *I3* and *I4*). This is especially important in IAS, as real-time capabilities may be affected by high network traffic on ethernet-based networks.

Antiviruses, Routers, Firewalls, Network IDS and event management systems (*RA8*, *RA9* and *RA10*) for both the enterprise and industrial network may provide audit and scanning capabilities that help analyze system components in more detail. This is especially useful in the presence of Malware and Brute Force Attacks (*I5* and *I4*) in order to verify whether the intrusion has succeeded and, in case it has, verify whether or not it has spread or achieved its goal (i.e., compromised a system component).

Industrial Network IDS may also provide capabilities to perform a back up of- and restore configurations (i.e., *RA11*) specific to IAS components. This may help remove malicious software (i.e., *I5* and *I7*) or correct misconfigurations (i.e., *I10*). Other misconfigurations on the host device *I10* can be remedied by software of the host device itself (e.g., *RA14*) or by log and event management systems (i.e., *RA15*).

Finally, Firewalls and VPN Endpoints (i.e., *RA4* and *RA7*) also are capable of mitigating intrusions related to communication (i.e., *I1*, *I2*, *I3* and *I4*). They are also capable of protecting IAS components (i.e., *I7* and *I8*), as they are widely used in the industry (as observed in Figure 4).

### *6.4. Discussion*

As it was observed from the table of security policies, intrusions and reactive actions (i.e., Tables 3–5); the concept for Reactive Protection System provides flexibility in order to integrate new policies and reactive actions. It also can be adapted in order to operate with other security solutions found in an IAS in order to extend these features. This flexibility and adaptability allow for automatically executing reactive actions.

Unfortunately, it is important to keep in mind that the automatic execution of reactive actions provided by this concept is linked to a trade-off between configurability and automation of the reactive actions. This means that the more detailed the configuration of the system is, the more effective its automatic response is. Although this requires a big amount of effort before deploying the system, it is important to consider that IAS has a long lifetime and, therefore, their reconfiguration and maintenance does not occur often. The analysis and selection of this trade-off should be performed between the system integrators and security experts in order to find the appropriate balance.

## 7. Implementation

The Reactive Protection System prototype has been implemented in an Industrial IoT Gateway device from Bosch Rexroth AG (Lohr am Main, BY, Germany) [59]. The architecture of this device consists of an Open Source Linux distribution and an integrated Java Virtual Machine (JVM) that enables deployment of Java applications via the Open Services Gateway Initiative (OSGi Framework) [60].

The OSGi Framework [61] allows for managing and implementing Java applications. It provides a platform with modular architecture that allows for managing applications as independent components called bundles. Bundles are able to interact with one-another thanks to the OSGi Framework through the publication and subscription of services they provide. The OSGi Framework also allows for managing their dependencies and versions that allows for controlling the visibility of their services and components and decreasing management complexity.

Hence, the prototype has been programmed in Java and deployed in the OSGi environment. The main features of the prototype for reactive protection are the following:

- Configurability of operational and security policies, as well as the status of the reactive system through a graphical user interface.

- The following security policies are supported: maximum number of login attempts and anomalous network traffic.
- The following operational policies are supported: communication availability based on specific IP Address or subnetwork.
- The following reactive protection action is supported: termination of opened Virtual Private Network (VPN) connections in order to protect against identified intrusions.
- Communication supports the following: Syslog [50] over User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and Transport Layer Security (TLS); and Common Event Format (CEF) [57,62].

The VPN Client belongs to the set of applications provided by Bosch Rexroth AG within the context of its IoT Gateway. Furthermore, the interaction between the prototypical Reactive Protection System and the VPN Client is possible thanks to the OSGi framework.

## 8. Evaluation of Feasibility and Applicability of the Reactive Protection Concept

The feasibility and applicability of the presented concept has been evaluated in two ways. At first, a Scenario often found in industrial systems, its related adversarial model and the specifics regarding its emulation are presented. From this scenario, a set of use cases are derived. These use cases demonstrate the applicability of the presented concept by considering the prototypical Reactive Protection System and describing the different results that can be obtained based on different configurations. Afterwards, the fulfillment of the four requirements (i.e., *R1–R4*) presented in Section 3 is verified. This verification is performed through the derivation of four Hypotheses that prove the feasibility of the presented concept. The discussion of these hypotheses are further substantiated with the Use Case Scenarios presented.

### *8.1. Scenario and Adversarial Model*

In order to validate the presented reactive protection concept, a real-life scenario derived from the reference IAS architecture (Figure 4) is presented. This scenario is shown in Figure 5. It presents a simplified remote maintenance application case.

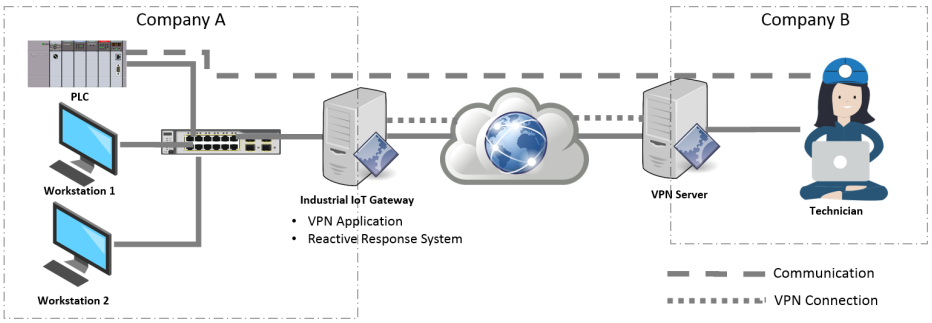


**Figure 5.** Simplified Industrial Scenario of a Remote Maintenance Application derived from the reference IAS architecture (Figure 4).

In the presented scenario, there exist two companies: *Company A* and *Company B*. The automation system is located at the site of *Company A*; this is represented by a Programmable Logic Controller (*PLC*), and two engineering workstations (*Workstation 1* and *Workstation 2*). A technician located on the site of *Company B* wishes to perform maintenance on devices located at the *Company A* site. In order to perform maintenance in a secure manner, a Virtual Private Network (VPN) connection is established between these two sites. The VPN end point on the *Company A* site is represented by a Bosch Rexroth *IoT Gateway*. As discussed in the previous section, the *IoT Gateway* contains a VPN

Client application that allows it to establish a connection to the endpoint located at the *Company B* site—hence allowing it to establish a direct connection to the computer of the *Technician*. On the other hand, the end point on the *Company B* site can be any device that is capable of providing the same functionality as a VPN server.

For this use case, it is assumed that the credentials required to setup the VPN connection have already been provided. It is also assumed that the VPN configurations are protected against unauthorized modifications.

The adversarial model contemplated for this scenario is comprised of external threats that may propagate through the secure VPN connection towards the automation system located at the site of *Company A* (e.g., Slammer worm [63]) or misuse from the part of the *Technician*.

### 8.2. Emulation of Test Scenario

Emulation of the aforementioned Scenario is carried out in the following. Two Local Area Networks (LAN) are defined. In *LAN A*, the industrial automation components are located. This being represented by a *PLC* and a Personal Computer (*PC*). The *Industrial IoT Gateway* device contains the VPN Client application and also the Reactive Protection System. It is also configured with two different IP addresses, each of them corresponding to *LAN A* and *LAN B*, respectively. Furthermore, the security events to be analyzed by the Reactive Protection System are generated on the *PC*. This *PC* contains a Java application developed for the sole purpose of Common Event Format message generation. In real-life, these event messages would be generated by a third-party security solution. However, the Java application is used for the prototypical application and its evaluation in order to simplify the test process. The VPN server runs on a Raspberry Pi located in *LAN B*. The two parties of the VPN Connection are the *Industrial IoT Gateway* and the *Raspberry Pi*. Through the VPN Connection any communication is possible (e.g., PLC Application download). For this test scenario, it is represented by a simple communication between a user located in *LAN B* and the *PLC* located in *LAN A*. An overview of this setup is presented in Figure 6.

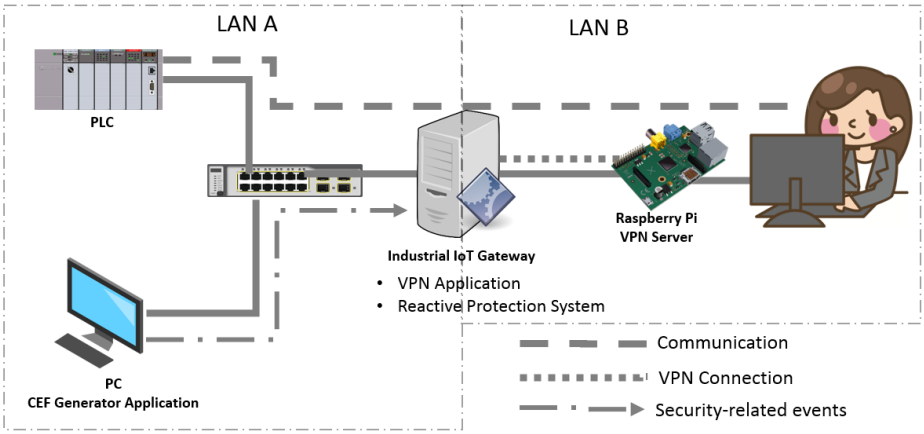


**Figure 6.** Emulation of an industrial scenario of a remote maintenance application Figure 5. LAN: Local Area Network.

### 8.3. Scenario Use Cases

From the aforementioned scenario, three use cases are derived. In each of these three use cases, the same security policy is violated.

The security policy supported by the Reactive Protection System prototype, as discussed in Section 7, refers to the surpassing of the maximum number of failed login attempts allowed (e.g., User fails to log in to the PLC multiple times). In order to trigger the analysis performed by the prototypical Reactive Protection System (i.e., Figure 3), the CEF generator application located in the

PC sends a CEF message. This CEF message contains information that allows the Reactive Protection System to identify the security policy being violated.

Once the Reactive Protection System identifies that a- and which security policy has been violated, it verifies whether a reactive action is possible to counteract this policy violation. For this type of policy violation, the Reactive Protection System supports the termination of active VPN connections. The execution or rejection of such action depends on the operational policies. The following use cases present different configuration alternatives for these operational policies, which result in different outcomes for the Reactive Protection System. For the purpose of this evaluation, a VPN connection between *LAN A* and *LAN B* is initiated.

**Use Case 1:** In this use case, an operational policy exists that defines that communication between two parties must always be available. These parties are defined through their IP addresses. These IP addresses are identified as members of the opened VPN connection and hence the reactive action is not executed.

**Use Case 2:** This use case is similar to Use Case 1. However, in this use case, the operational policy indicates the availability for communication for a specific subnetwork and not specific IP addresses. During validation of the operational policies, it is identified that the IP address of one of the parties of the VPN connection is located in this subnetwork and hence the reactive action is not executed.

**Use Case 3:** In this use case, none of the aforementioned policies exist and hence the reactive action is carried out. This means that the active VPN connection is closed. If the lack of operational policies was intentional and does reflect the operational requirements of the automation system, then the termination of the VPN connection does not influence the operation of the underlying system. However, if the neglect of operational policies was non-intentional, this could increase an availability issue in the system that could potentially generate a fault in the IAS.

### *8.4. Hypotheses*

In order to prove the feasibility of the presented concept, the fulfillment of the requirements presented in Section 3 must be verified. In order to do so, four hypotheses have been derived. In the following, these hypotheses are presented. The discussion regarding their proof is supported by the prototypical implementation presented in Section 7 and the aforementioned use case scenarios. The mapping between hypotheses and the requirements they verify is presented in Table 6.

**Table 6.** Mapping between hypotheses and requirements.

| Hypothesis Number | Hypothesis | Requirement |
|---|---|---|
| 1 | Conditions required to meet operational requirements (High Performance, Availability and Real-time capabilities of an automation system can be defined as operational policies | R3 |
| 2 | Harmonization between security and operational policies ensure that reactive actions in the presence of intrusions do not affect the correct operation of the underlying automation system | R2 |
| 3 | Reactive security measures, as opposed to only passive, can be executed automatically to help counteract possible intrusions in IAS | R1 |
| 4 | Implementation of a Reactive Protection System on a network segment-basis improves the security and reliability of IAS | R4, R2 |

**R1**: Configurability and automatic or semi-automatic reactions to intrusions, **R2**: Compliance with the ISA/IEC 62443 series of Standards, **R3**: Ensure correct operation of the underlying automation system, **R4**: Multi-platform support and interoperability with preexisting solutions.

**Hypothesis 1.** *Conditions required to meet operational requirements (high performance, availability and real-time capabilities) of an automation system can be defined as operational policies.*

Policies are often referred to as rules, conditions or constraints that must be maintained [4]. Hence, operational requirements may be also defined as policies. In the presented concept, these operational policies were defined by identifying critical assets that constitute an automation system. From these assets, a classification of operational policies was derived. This derivation was achieved by analyzing cases or conditions related to these critical assets in which the main operational requirements of IAS could be negatively affected (i.e., high performance, availability and real-time capabilities). Each of the classes defined in this classification describes in detail the information that such policies may contain. Additionally, a few examples are provided (Section 5).

The applicability of these policies was evaluated through the aforementioned scenario. Furthermore, by deriving these policies from critical assets related to operational requirements in IAS, it is ensured that, by considering these policies, these requirements are met—hence fulfilling *R3* defined in Section 3. Hence, the hypothesis that operational requirements of an automation system can be defined as operational policies can be defined as true.

**Hypothesis 2.** *Harmonization between security and operational policies ensure that reactive actions in the presence of intrusions do not affect the correct operation of the underlying automation system.*

In Section 5, security and operational policies applicable for IAS were presented. These security policies were derived from the ISA/IEC 62443 series of Standards, hence fulfilling *R2* defined in Section 3. Furthermore, from these security policies, reactive actions that could counteract the effects of intrusions were also identified. Although consideration of both security policies and reactive actions are capable of protecting against intrusions, their implementation in IAS could potentially affect the correct or expected operation of the underlying automation system.

Hence, the concept for reactive protection presented in Section 5 not only considers security policies and reactive actions, but also considers operational policies. By doing so, the validation of operational policies ensures that no reactive action that could negatively influence the operation of the automation system is executed. However, in order for this concept to be effective, it is necessary that the defined security and operational policies do reflect the real security and operational requirements. Neglecting or overlooking either of them may result in decreased protection against intrusions or it could also negatively affect the main operational requirements of the automation system. During the discussion of evaluation of the use case scenarios, the possible effects of such event were observed with *Use Case 1*, *Use Case 2* and *Use Case 3*. Hence, the hypothesis that appropriate definition of security and operational policies ensures that reactive actions do not negatively influence the correct operation of the automation system is proven to be true.

**Hypothesis 3.** *Reactive security measures, as opposed to only passive, can be executed automatically to help counteract possible intrusions in IAS.*

As previously discussed in Section 3, common responses in the presence of intrusions are passive. Any active countermeasure is often carried out by a human expert, which results in delayed responses. In order to address this issue (i.e., fulfill *R1*), the presented concept derived a set of reactive actions (i.e., Sections 5 and 6) that provide active protection for automation systems in the presence of intrusions. These reactive actions are automated through the configuration and harmonization of security and operational policies. Although at first human effort is required for their configuration, once the Reactive Protection System is deployed; no other human intervention is necessary as long as the policies remain suitable for the requirements of the automation system—hence automating their execution. This was demonstrated in *Use Case 3*, where the VPN Connection is automatically terminated—hence proving this hypothesis to be true.

**Hypothesis 4.** *Implementation of a Reactive Protection System on a network segment-basis improves the security and reliability of IAS.*

From the analysis of current architectural and security trends in IAS (Sections 1 and 3), it was observed that network segmentation is widely used in IAS. This occurs as network segmentation allows for facilitating the management of system components, as well as improving the security of the system. These improvements are achieved by allowing to group system components into zones based on their security requirements and other requirements derived from their design and operation.

The concept presented in this work exploits these advantages by considering also the network segmentation approach in order to provide protection against intrusions. This is performed by first deriving security policies from the ISA/IEC 62443 series of Standards (i.e., hence fulfilling *R2* from Section 3). Afterwards, it suggests the deployment of a Reactive Protection System whose knowledge base is built from security and operational policies that apply to a specific network segment and its system components. It also presents a set of reactive protection actions capable of protecting the corresponding network segment. These reactive actions may be capable of the disrupting of counteracting intrusions, which in return may increase the security of the automation system. A system with high and effective security decreases the chances of intrusions being able to disrupt its normal behaviour—hence improving its reliability.

Furthermore, the presented concept also allows interoperability with preexisting security solutions. This is performed through the reception and analysis of security events from third-party components (i.e., fulfilling *R2* from Section 3). This concept does not depend on any specific event format or protocol. Hence, implementations from this concept have flexibility when choosing them. This has been demonstrated with the prototypical Reactive Protection System implemented in this work (Section 7). Hence, the hypothesis that following a network segment approach for reactive protection increases the security and reliability of IAS is proven to be true.

## 9. Conclusions and Future Work

Passive responses in the presence of intrusions are predominant in the field of security solutions for IAS due to the concerns that exist that reactive responses may negatively affect the operation of the automation system. This often requires that any reactive countermeasure be carried out by a human, which results in delayed responses. This increases the vulnerability of the system and provides a window of opportunity for the intrusion to succeed and hence negatively influence the system.

In this paper, a concept for a system that allows for reactively and automatically responding to intrusions is presented. This concept addresses the aforementioned concerns, which results in a suitable and feasible reactive protection alternative for IAS.

This concept was first conceived by identifying four requirements related to intrusion prevention solutions and other architectural and security trends for industrial systems. From these requirements, the foundation for the presented concept was laid out. This foundation is comprised of security and operational policies, as well as reactive actions that can potentially counteract intrusions.

The system resulting from this concept is capable of analyzing security events received from other system components (e.g., third-party security solutions). These events are analyzed in order to identify security policy violations. Once a policy violation has been detected, an appropriate reactive action is selected. Before the execution or triggering of such action, the operational policies are validated. This ensures that only reactive actions that do not violate the operational policies of the underlying automation system are carried out. This means that, as long as the defined security and operational policies represent the true requirements and constraints of the automation system, the reactive actions will not negatively affect it. Furthermore, it is important to highlight that the scope of protection provided by the presented concept allows for protecting the automation system and its components at a network segment-level. This complies with current architectural and security trends of IAS. Moreover, the presented concept provided guidelines that can be followed in order to identify security policies, reactive actions and components to execute these actions.

The application of these guidelines and concept was illustrated with a reference IAS architecture and application, and a set of example security policies and reactive actions that highlighted the potential

of the presented concept. Additionally, the evaluation of the presented concept was performed as followed. First, a prototypical Reactive Protection System was implemented. In order to test its feasibility and applicability, a real-life scenario was defined, from which use cases were derived. These use case scenarios were emulated with a test setup where the prototype was deployed. Afterwards, to further support the evaluation of feasibility, four hypotheses were derived and proven. These hypotheses allowed for verifying that the requirements presented in Section 3 were fulfilled. The results of these evaluations have shown that the presented concept is suitable and feasible for IAS.

Future work will focus on the improvement of the prototypical implementation. This includes extending the capabilities by allowing remote configuration of the Reactive Protection System and enriching the security and operational policies knowledge base. Another important aspect is to further enhance the interoperability with other security solutions, which will allow for adding support for more reactive protection actions (e.g., add new firewall rules). Furthermore, alternatives to improve the usability of the configuration for security and operational policies will be researched. Currently, the configuration of security and operational policies has to be manually carried out by a human operator with knowledge regarding the operation of the automation system and its security. Although this may require significant configuration effort (depending on the complexity of the system and its policies), the presented concept provides a feasible and suitable alternative for active protection against intrusions. The trade-off between configuration effort and automatic protection should be further discussed between the system stakeholders.

**Author Contributions:** Conceptualization, C.V.M. and B.V.-H.; Methodology, C.V.M. and B.V.-H.; Software, Validation and Investigation C.V.M.; Writing—Original Draft Preparation, C.V.M. and B.V.-H.

**Funding:** This work was supported by the German Research Foundation (DFG) and the Technical University of Munich (TUM) in the framework of the Open Access Publishing Program.

**Conflicts of Interest:** The authors declare the following facts which may be considered as potential conflicts of interest. Cyntia Vargas Martínez is currently a PhD student under the employment of Bosch Rexroth AG. Both authors have submitted an invention report for review that considers the reactive protection concept presented in this work.

## References

1. Weyer, S.; Schmitt, M.; Ohmer, M.; Gorecky, D. Towards Industry 4.0—Standardization as the crucial challenge for highly modular, multi-vendor production systems. *IFAC-PapersOnLine* **2015**, *48*, 579–584. [CrossRef]
2. Koutepas, G.; Giannopoulos, G.; Mitsiara, A. Cyber Security Trends and Their Implications in ICS: Mid-Year Report 2016. Available online: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC103512/lbna28187enn.pdf (accessed on 22 September 2018).
3. Kaspersky Lab ICS CERT. Threat Landscape for Industrial Automation Systems: H1 2018. Available online: https://ics-cert.kaspersky.com/media/H1_2018_ICS_REPORT_ENG.pdf (accessed on 1 October 2018).
4. Security Requirements for Cryptographic Modules: FIPS PUB 140-2: Federal Information Processing Standards Publication. 2001. Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf (accessed on 1 October 2018).
5. Schneider, F.B. Enforceable security policies. *ACM Trans. Inf. Syst. Secur.* **2000**, *3*, 30–50. [CrossRef]
6. Kissel, R. *Glossary of Key Information Security Terms: NISTIR 7298*; Diane Publishing: Collingdale, PA, USA, 2011, doi:10.6028/NIST.IR.7298r2.
7. Scarfone, K.; Mell, P. Intrusion Detection and Prevention Systems. In *Handbook of Information and Communication Security*; Stavroulakis, P., Stamp, M., Eds.; Springer Berlin Heidelberg: Berlin/Heidelberg, Germany, 2010; pp. 177–192, doi:10.1007/978-3-642-04117-4_9.
8. Karnouskos, S.; Colombo, A.W.; Bangemann, T. Trends and Challenges for Cloud-Based Industrial Cyber-Physical Systems. In *Industrial Cloud-Based Cyber-Physical Systems: The IMC-AESOP Approach*; Colombo, A.W., Bangemann, T., Karnouskos, S., Delsing, J., Stluka, P., Harrison, R., Jammes, F., Lastra, J.L., Eds.; Springer International Publishing: Cham, Switzerlands, 2014; pp. 231–240, doi:10.1007/978-3-319-05624-1_11.

9. Jazdi, N. Cyber physical systems in the context of Industry 4.0. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–4. [CrossRef]
10. Karnouskos, S. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In Proceedings of the IECON 2011—37th Annual Conference of IEEE Industrial Electronics, Melbourne, VIC, Australia, 7–10 November 2011; pp. 4490–4494. [CrossRef]
11. Nasser, M.; Ahmad, R.; Yassin, W.; Hassan, A.; Zainal, Z.; Salih, N.; Hameed, K. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*. [CrossRef]
12. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Im, E.G.; Pranggono, B.; Wang, H.F. Multiattribute SCADA-Specific Intrusion Detection System for Power Networks. *IEEE Trans. Power Deliv.* **2014**, *29*, 1092–1102. [CrossRef]
13. Kim, B.K.; Kang, D.H.; Na, J.C.; Chung, T.M. Abnormal traffic filtering mechanism for protecting ICS networks. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 31 January–3 February 2016; pp. 436–440. [CrossRef]
14. Yüksel, Ö.; den Hartog, J.; Etalle, S. Reading Between the Fields: Practical, Effective Intrusion Detection for Industrial Control Systems. In Proceedings of the 31st Annual ACM Symposium on Appliec Computing, Pisa, Italy, 4–8 April 2016; Ossowski, S., Ed.; ACM: New York, NY, USA, 2016; pp. 2063–2070. [CrossRef]
15. ICS CERT. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Available online: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (accessed on 12 November 2018).
16. Sauter, T.; Soucek, S.; Kastner, W.; Dietrich, D. The Evolution of Factory and Building Automation. *IEEE Ind. Electron. Mag.* **2011**, *5*, 35–48. [CrossRef]
17. Scholten, B. *The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing*; ISA: Research Triangle Park, NC, USA, 2007.
18. Ab Rahman, N.H.; Choo, K.K.R. A survey of information security incident handling in the cloud. *Comput. Secur.* **2015**, *49*, 45–69. [CrossRef]
19. Schneider Electric. Industrial Defender: Security, Compliance, and Change Management Solution. Available online: https://www.schneider-electric.com/en/product-range-download/61675-industrial-defender/ (accessed on 29 November 2018).
20. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology, Computer Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011, doi:10.6028/NIST.SP.800-82.
21. Stouffer, K.K.; Falco, J. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*; Department of Homeland Security, Control systems security Program, National Cyber Security Division: Washington, DC, USA, 2016.
22. Foo, B.; Glause, M.W.; Howard, G.M.; Wu, Y.S.; Bagchi, S.; Spafford, E.H. Intrusion Response Systems: A Survey. In *Information Assurance*; Qian, Y., Ed.; The Morgan Kaufmann Series in Computer Security; Elsevier: Amsterdam, The Netherlands; Morgan Kaufmann: Boston, MA, USA, 2008; pp. 377–412.
23. Piggin, R. Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. In Proceedings of the IET Conference on Control and Automation 2013: Uniting Problems and Solutions, Birmingham, UK, 4–5 June 2013; pp. 1–6. [CrossRef]
24. Knowles, W.; Such, J.M.; Gouglidis, A.; Misra, G.; Rashid, A. Assurance Techniques for Industrial Control Systems (ICS). In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, Denver, CO, USA, 16 October 2015; Ray, I., Thomas, R., Cardenas, A.A., Eds.; ACM: New York, NY, USA, 2015; pp. 101–112. [CrossRef]
25. Garitano, I.; Uribeetxeberria, R.; Zurutuza, U. A Review of SCADA Anomaly Detection Systems. In *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*; Corchado, E., Snasel, V., Sedano, J., Hassanien, A.E., Calvo, J.L., Slezak, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 357–366.

26. Zhu, B.; Sastry, S. SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy. In Proceedings of the 1st Workshop on Secure Control Systems (SCS), Stockholm, Sweden, 12 April 2010; Volume 11, p. 7.
27. Kagermann, H. Change Through Digitization—Value Creation in the Age of Industry 4.0. In *Management of Permanent Change*; Albach, H., Meffert, H., Pinkwart, A., Reichwald, R., Eds.; Springer Fachmedien: Wiesbaden, Germany, 2015; pp. 23–45, doi:10.1007/978-3-658-05014-6_2.
28. Blowers, M.; Iribarne, J.; Colbert, E.J.M.; Kott, A. In Conclusion: The Future Internet of Things and Security of Its Control Systems. In *Cyber-security of SCADA and Other Industrial Control Systems*; Colbert, E.J.M., Kott, A., Eds.; Springer International Publishing: Cham, Switzerlands, 2016; pp. 323–355, doi:10.1007/978-3-319-32125-7_16.
29. Mitchell, R.; Chen, I.R. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Comput. Surv.* **2014**, *46*, 1–29. [CrossRef]
30. Goldenberg, N.; Wool, A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2013**, *6*, 63–75. [CrossRef]
31. Cruz, T.; Maglaras, L.A.; Jiang, J. Integrated OCSVM mechanism for intrusion detection in SCADA systems. *Electron. Lett.* **2014**, *50*, 1935–1936. [CrossRef]
32. Maglaras, L.A.; Jiang, J. Intrusion detection in SCADA systems using Machine Learning Techniques. In Proceedings of the 2014 Science and Information Conference (SAI), London, UK, 27–29 August 2014; pp. 626–631. [CrossRef]
33. Ponomarev, S.; Atkison, T. Industrial Control System Network Intrusion Detection by Telemetry Analysis. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 252–260. [CrossRef]
34. Nurjahan; Nizam, F.; Chaki, S.; Al Mamun, S.; Kaiser, M.S. Attack detection and prevention in the Cyber Physical System. In Proceedings of the 2016 International Conference on Computer Communication and Informatics, Coimbatore, India, 7–9 January 2016; pp. 1–6. [CrossRef]
35. Security Matters. Phoenix Contact's mGuard Integration with Silent Defense. Available online: https://www.secmatters.com/hubfs/Security_Matters-March2017/PDF/Solution-Brief-SecurityMatters-and-Phoenix-Contact.pdf (accessed on 1 October 2018).
36. Tsang, C.H.; Kwong, S. Multi-Agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction. In Proceedings of the 2005 IEEE International Conference on Industrial Technology (ICIT), Hong Kong, China, 14–17 December 2005; pp. 51–56. [CrossRef]
37. Morris, T.; Vaughn, R.; Dandass, Y. A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences (HICSS), Maui, HI, USA, 4–7 January 2012; pp. 2338–2345. [CrossRef]
38. Roesch, M. Snort: Lightweight intrusion detection for networks. In Proceedings of the Lisa '99: 13th Systems Administration Conference, Seattle, WA, USA, 7–12 November 1999; Volume 99, pp. 229–238. Available online: http://static.usenix.org/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf (accessed on 1 October 2018).
39. Chen, Q.; Abdelwahed, S. A Model-based Approach to Self-Protection in SCADA Systems. In Proceedings of the 9th International Workshop on Feedback Computing, Philadelphia, PA, USA,17 June 2014. Available online: https://www.usenix.org/conference/feedbackcomputing14/workshop-program/presentation/chen (accessed on 25 September 2018).
40. Hewett, R.; Rudrapattana, S.; Kijsanayothin, P. Cyber-Security Analysis of Smart Grid SCADA Systems with Game Models. In Proceedings of the 9th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 8–10 April 2014; Abercrombie, R.K., McDonald, J.T., Eds.; ACM: New York, NY, USA, 2014; pp. 109–112. [CrossRef]
41. Huang, S.; Zhou, C.J.; Yang, S.H.; Qin, Y.Q. Cyber-physical System Security for Networked Industrial Processes. *Int. J. Autom. Comput.* **2015**, *12*, 567–578. [CrossRef]
42. CockpitCI. Cybersecurity on SCADA: Risk Prediction, Analysis and Reaction Tools for Critical Infrastructures. Available online: https://cordis.europa.eu/docs/results/285/285647/final1-final-report-publishable-summary.pdf (accessed on 1 October 2018).
43. Hurd, C.M.; McCarty, M.V. A Survey of Security Tools for the Industrial Control System Environment. Available online: https://www.osti.gov/servlets/purl/1376870 (accessed on 1 October 2018).

44. Ficco, M. Security Event Correlation Approach for Cloud Computing. *Int. J. High Perform. Comput. Netw.* **2013**, *7*, 173. [CrossRef]
45. Inayat, Z.; Gani, A.; Anuar, N.B.; Khan, M.K.; Anwar, S. Intrusion response systems: Foundations, design, and challenges. *J. Netw. Comput. Appl.* **2016**, *62*, 53–74. [CrossRef]
46. Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. SCADA security in the light of Cyber-Warfare. *Comput. Secur.* **2012**, *31*, 418–436. [CrossRef]
47. Candell, R.; Stouffe, K.; Anand, D. A Cybersecurity Testbed for Industrial Control System. 2014. Available online: https://www.nist.gov/publications/cybersecurity-testbed-industrial-control-systems (accessed on 20 October 2018).
48. Han, W.; Lei, C. A survey on policy languages in network and security management. *Comput. Netw.* **2012**, *56*, 477–489. [CrossRef]
49. Diver, S. Information Security Policy: A Development Guide for Large and Small Companies. Available online: https://www.sans.org/reading-room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies-1331 (accessed on 25 October 2018).
50. Gerhards, R. *The Syslog Protocol: RFC 5424*; IETF Trust: Reston, VA, USA, 2009, doi:10.17487/RFC5424.
51. Al-Fuqaha, A.; Khreishah, A.; Guizani, M.; Rayes, A.; Mohammadi, M. Toward better horizontal integration among IoT services. *IEEE Commun. Mag.* **2015**, *53*, 72–79. [CrossRef]
52. Datta, S.K.; Bonnet, C.; Nikaein, N. An IoT Gateway Centric Architecture to Provide Novel M2M Services. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 514–519. [CrossRef]
53. Zolotová, I.; Bundzel, M.; Lojka, T. Industry IoT Gateway for Cloud Connectivity. In *IFIP International Conference on Advances in Production Management Systems*; Advances in Production Management Systems: Innovative Production Management Towards Sustainable Growth; Umeda, S., Nakano, M., Mizuyama, H., Hibino, H., Kiritsis, D., von Cieminski, G., Eds.; Springer International Publishing: Cham, Switzerlands, 2015; Volume 460, pp. 59–66, doi:10.1007/978-3-319-22759-7_7.
54. Sinha, S.R.; Park, Y. Creating Smart Gateway. In *Building an Effective IoT Ecosystem for Your Business*; Sinha, S.R., Park, Y., Eds.; Springer International Publishing: Cham, Switzerlands, 2017; pp. 37–47, doi:10.1007/978-3-319-57391-5_3.
55. Vogel-Heuser, B.; Ocker, F. Maintainability and evolvability of control software in machine and plant manufacturing—An industrial survey. *Control Eng. Pract.* **2018**, *80*, 157–173. [CrossRef]
56. Urias, V.; van Leeuwen, B. Experimental Methods for Control System Security Research. In *Cyber-Security of SCADA and Other Industrial Control Systems*; Colbert, E.J.M., Kott, A., Eds.; Springer International Publishing: Cham, Switzerlands, 2016; pp. 253–277, doi:10.1007/978-3-319-32125-7_13.
57. ArcSight Inc. *Common Event Format: Event Interoperability Standard*; ArcSight Inc.: Sunnyvale, CA, USA, 2006.
58. Zhu, B.; Joseph, A.; Sastry, S. A Taxonomy of Cyber Attacks on SCADA Systems. In Proceedings of the 4th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), Dalian, China, 19–22 October 2011; pp. 380–388. [CrossRef]
59. Bosch Rexroth AG. IoT Gateway: Get ready for Industry 4.0! Available online: https://www.boschrexroth.com/en/xc/products/product-groups/electric-drives-and-controls/industrial-iot (accessed on 1 October 2018).
60. Tavares, A.L.; Valente, M.T. A gentle introduction to OSGi. *ACM SIGSOFT Softw. Eng. Notes* **2008**, *33*, 8. [CrossRef]
61. The OSGi Alliance. OSGi Core. Available online: https://osgi.org/download/r6/osgi.core-6.0.0.pdf (accessed on 25 October 2018).
62. ArcSight Inc. Common Event Format. Available online: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/CORP_KNOWLEDGEBASE/78000/KB78712/en_US/CEF_White_Paper_20100722.pdf (accessed on 25 October 2018).
63. Moore, D.; Paxson, V.; Savage, S.; Shannon, C.; Staniford, S.; Weaver, N. Inside the slammer worm. *IEEE Secur. Priv. Mag.* **2003**, *1*, 33–39. [CrossRef]