

Integrated Protection of Industrial Control Systems from Cyber-attacks: the ATENA Approach

F. Adamsky¹, M. Aubigny², F. Battisti³, M. Carli³, F. Cimorelli⁴, T. Cruz⁵,
A. Di Giorgio⁴, C. Foglietta³, A. Galli⁶, A. Giuseppi⁴, F. Liberati⁴, A.
Neri³, S. Panzieri³, F. Pascucci³, J. Proenca⁵, P. Pucci⁶, L. Rosa⁵, R. Soua¹

Abstract

Industrial and Automation Control systems traditionally achieved security thanks to the use of proprietary protocols and isolation from the telecommunication networks. Nowadays, the advent of the Industrial Internet of Things poses new security challenges. In this paper, we first highlight the main security challenges that advocate for new risk assessment and security strategies. To this end we propose a security framework and advanced tools to properly manage vulnerabilities, and to timely react to the threats. The proposed architecture fills the gap between computer science and control theoretic approaches. The physical layers connected to Industrial Control Systems are prone to disrupt when facing cyber-attacks. Considering the modules of the proposed architecture, we focus on the development of a practical framework to compare information about physical faults and cyber-attacks. This strat-

¹Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

²itrust consulting, Luxembourg

³Department of Engineering, Roma Tre University, Italy

⁴CRAT- Consortium for the Research in Automation and Telecommunication, Italy

⁵Centre for Informatics and Systems, University of Coimbra, Portugal

⁶Leonardo S.p.A, Italy

egy is implemented in the ATENA architecture which has been designed as an innovative solution for the protection of critical assets.

Keywords: Critical Infrastructures, Cyber-Physical Attacks, Security, Industrial IoT, SCADA Systems, Industrial and Automation Control Systems

1. Introduction

The security of critical services has been granted for a long time through the restriction of their communication networks, and the deployment of specific and proprietary technologies (protocols, devices, software, ...): the so called air-gap principle. However, the recent ongoing adoption of common technology (such as the Internet protocol), the increase in the number of interconnections between different types of networks, and the emergence of sophisticated cyber attacks [1] have jeopardized this security strategy and risen the need of novel standardization and technical practices.

Therefore, it is not possible to solve security issues by taking into account only a single Critical Infrastructure (CI) (i.e., essential service or domain) but it is fundamental to consider a set of interconnected infrastructures, such as power grid, water distribution network, gas pipelines and telecommunications.

Supervisory Control and Data Acquisition (SCADA) systems for CIs are frequently deemed vulnerable due to a mix of mindset preconceptions, design faults, and insecure technologies [2]. Moreover, Industrial Automation and Control Systems (IACS) security requires a domain-specific security approach that cannot be effectively achieved through the straightforward adoption of

Information and Communications Technology (ICT) security mechanisms, tools and techniques [3].

Similarly, for Security Information and Event Management (SIEM)-based IACS security solutions, they were found to be lacking in scalability and cyber-physical awareness; moreover they over-rely on ICT-oriented solutions. In fact, Industrial Internet of Things (IIoT) requires the use of event processing mechanisms able to scale beyond the capacity of existing conventional SIEM systems, which are frequently based on correlation engines with constrained or inexistent scaling capabilities. The complexity of protecting CIs is increased due to the existence of dependencies among physical equipments of essential services. The lack of awareness about the physical side effect of cyber-attacks compromises the supervision and/or the control of the physical processes thus leading to cascading effects. Finally, ICT-oriented approaches, such as perimeter-based defense, have proven to be inadequate to protect IACS [4].

It is also worth noticing that vulnerability management is usually a long process and many known vulnerabilities often remain unpatched for long periods even in CIs for many reasons. Mostly it is due to old legacy software/hardware and non automated updating procedures, but also for the need of a scheduled maintenance window, to avoid service disruption. During this period of time, CI's owners continue to rely on vulnerable hardware and software. New solutions were devised to decrease the impact of cyber-threats through timely warning of the stakeholders and by forcing them to react in time. However, the current vulnerability management system solutions still have several limitations. Most of them are related to specific sectors

to grant their commercial sustainability and this is not applicable in the case of large infrastructures. Besides this, technical deployment constraints are often difficult to adapt to the specific CI environment. Finally, many solutions have limited connection to other security systems such as risk assessment and monitoring tools [5, 6]. Actual regulations, national standards, or guidelines are only suggestions and checklists for critical services providers. They do not supply a platform for detecting cyber threats and evaluating their consequences on the physical process allowing also reaction capabilities [7].

An effective solution to ensure an adequate level of resiliency while accommodating the diffusion of new technologies into CIs, is presented in the ATENA project [8]. It is focused on the definition of ad-hoc methodologies for controlling physical flow efficiency while improving resilience of interconnected CIs against Cyber-Physical attacks. These objectives are achieved by developing:

- New anomaly detection algorithms and risk assessment methodologies specifically designed for a distributed Cyber-Physical environment. Traditional computer security focuses on how to protect information. Here, a novel perspective is adopted, considering how attacks affect estimation, control and monitoring algorithms, how they affect the plant, and the decision made by the human operators.
- A suite of integrated ICT networked components for detection and reaction in presence of adverse events. They are devised to define a resilient control system according to the security-by-detection paradigm. The Software Defined Network (SDN) is used to redirect the malicious network traffic and to protect the system.

The ATENA architecture, presented in this paper, provides a framework for the development of these tools in a scalable and distributed way to cope with the IIoT challenges.

The rest of the paper is organized as follows: Section 2 presents previous related works, Section 3 illustrates the overall Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures (ATENA) system architecture, while Sections 4 – 6 detail each component. Finally, in Section 7 the discussion on future developments are presented and the conclusions are drawn.

2. Related work: the logic behind the ATENA project

The ATENA architecture is based on the outcomes of both the MICIE [9] and the CockpitCI [10] projects. The goal of the aforementioned projects is the development of a security platform for inter-dependent CIs. These projects present evolving solutions with respect to the previous one according to the development of the state-of-the-art. The ATENA architecture addresses the new challenges arising with the advent of the IIoT paradigm. In the following, an overview of the MICIE and of the CockpitCI projects is presented.

The FP7 MICIE project aims at increasing operators' situation awareness by evaluating the consequences of faults originated in different interconnected infrastructures through the analysis of the dependencies. The MICIE platform is composed by three main elements: the Risk Predictor (RP), the Secure Mediation GateWay (SMGW) and the adaptors. The RP contains a simplified model of the interconnected infrastructures by considering devices

and services. It is able to assess the risk when a fault in an equipment arises and if a predefined quality of service is not provided to customers. The SMGW is devoted to secure the messages between RP and adaptors, and between RPs implemented in different CIs. The adaptors ensure information gathering from the control centers to check if an attack (or fault) took place or not. MICIE adopts a distributed architecture: each control center has an adaptor and a RP. The SMGW is implemented in order to reduce the protocol overhead.

The FP7 CockpitCI project is based on the MICIE platform and targets the implementation of new capabilities. It introduces the Perimeter Intrusion Detection System (PIDS) that is able to detect cyber-attacks, and to understand their consequences on physical devices and services. The core of the PIDS [11] is a correlation and/or event processing engine which is fed by a distributed set of security probes, according to most conventional SIEM architectures for IACS protection. The PIDS architecture reflects a vision geared towards conventional IACS, mostly confined within a production unit (such as a factory) or a mono-scope, homogeneous distributed domain. Within each protected IACS domain, a PIDS instance is deployed to detect coordinated cyber-attacks. This can be done by collecting, aggregating and correlating evidences gathered through probes deployed in the CI.

The PIDS agents are able to encapsulate customized third party modules (e.g., the Snort NIDS [12] or the OSSEC HIDS [13]), which are integrated using coupling modules), as well as components specifically developed for CockpitCI (e.g., the Shadow Security Unit (SSU) [10], the SCADA Honey-pot [14] [15], Host Output Traffic Control, or the Vulnerability, Behaviour

and Exec checker agents [11]). The RP in CockpitCI represents an improvement with respect to the one developed in MICIE. It considers the effect of cyber attacks on devices and on services and assesses the consequences of cyber threats on physical devices. Also the SMGW capabilities are improved. This enhanced version is able to deep inspect a larger amount of data and traffic passing through the considered CIs. Finally, the adaptors were improved in terms of scalability and flexibility.

The main drawback of the CockpitCI approach is the fact that it is mainly hardwired into the RP and therefore misses flexibility and the ability to deal with the different security threats. Thus, the CockpitCI architecture is not suitable for the IIoT paradigm. As an example, the PIDS was not designed for the emerging generation of IIoT IACS. Indeed, constrained devices such as sensors, Radio-Frequency IDentification (RFID) tags and smart meters, can autonomously gather critical information, interact with other devices and send collected information to distant central entities thus highlighting the potential vulnerabilities and threats. The absence of horizontal scaling capabilities in PIDS, made it unsuitable to cope with the data flow processing scale (in terms of event volume and rate) required to monitor a massively distributed infrastructure. Nevertheless, the CockpitCI platform and its possible improvements are the starting point for the ATENA architecture capabilities. Each module is improved, considering the IIoT and overcoming the previous limitations. The ATENA architecture can perform actions on physical processes and on telecommunications, considering the human-in-the-loop. Therefore, new modules (e.g., mitigation module and the orchestrator) are introduced to handle the interaction with the operators.

3. The ATENA High-Level Architecture

The ATENA architecture aims at improving the security of the IACS. Specifically, it addresses the well known security issues generated by both the presence of CI interdependencies (e.g., threat propagation and cascading effects) and IACS or SCADA complexity (e.g., presence of interconnected/interoperable distributed devices, sensors and actuators). Moreover, it faces the new challenges arising from the growth of the interconnection among infrastructures outside the single plant thanks to the development of the IIoT paradigm. Finally, it exploits the new communication approaches, such as SDN and Network Function Virtualization (NFV), able to efficiently monitor and control devices and data traffic.

The ATENA system proposes to address the following novelties:

- The enforcement of the *prevent-detect-react* approach by: (i) expanding the results in the state-of-the-art in the field of detection and risk assessment; (ii) introducing the ability to evaluate and suggest the most secure configuration of the used asset, in order to assure the achievement of the desired security level in normal operational mode; (iii) developing real-time reaction strategies to mitigate the consequences of detected treats.
- The introduction of the so-called Software Defined Security, to bring the results and innovation of SDN in the field of CIs by supervising their control, operational and corporate networks.
- The introduction of a distributed Intrusion and Anomaly Detection System (IADS) to cope with the distribution of the functionalities in

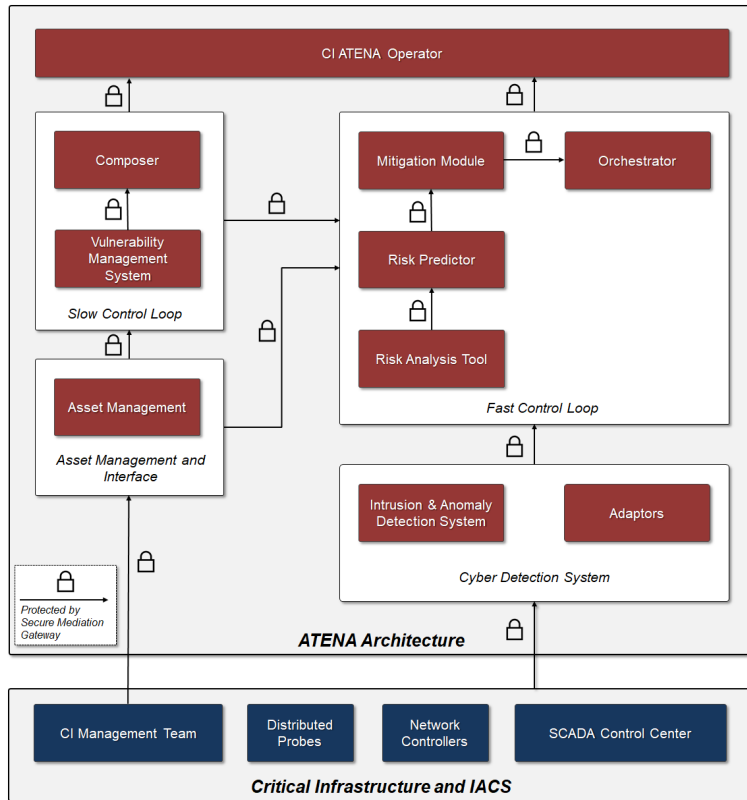


Figure 1: ATENA functional architecture with the four main functional blocks.

modern CIs and to detect physical anomalies caused by cyber attacks.

To achieve ATENA goals, a set of interconnected security components has been designed in order to innovate models, methodologies and algorithms for security management. The overall ATENA architecture is sketched in Figure 1 and it is composed by four main functional blocks:

- The *Assets Management and Interface* represents the interface between the ATENA system and both the CI and the IACS. This module is devoted to filter and to normalize the data provided by the SCADA

control room and forward them to the remaining modules of ATENA system. The processed data contributes to form the *knowledge base* together with the information on CI assets and procedures supplied by the CI management team operator.

- The Cyber Detection System (CDS) collects information from distributed probes, the ICT component and the SCADA system to determine and, eventually, notify anomalies in the behavior or the state of the CI.
- The *Slow Control Loop* exploits and addresses the information about vulnerabilities and/or anomalies arisen in CI and recorded in the knowledge base. The vulnerabilities of CI are detected and notified by periodic scans of the CI configuration. This module is able to suggest to the CI operator the proper configurations of the equipment and services to guarantee a desired security level.
- The *Fast Control Loop* computes the current and predicted risk level for the CI. This information is used to evaluate proper mitigation actions to prevent faults and attacks. It provides the mitigation actions as a decision support system for the CI operators. Thereafter, the human decisions are directly actuated on the proper field.

All communications between the modules of the ATENA system, the CI and the IACS are secured by the use of a SMGW. It grants adequate and strict security policies for both exposed services and data exchange (e.g., data encryption protocol, trusting schemes between communication counterparts) to prevent data interception or modification and to protect the trading of

sensitive information within the infrastructure. Furthermore, it allows authorized personnel to perform control and management operations by using access control mechanisms (e.g., identity and access management, accounting, audit). The SMGW guarantees the resiliency of the whole system by preventing a faulty part to affect or shatter the overall functionalities. It is realized in a scalable environment in order to be able to avoid performance degradation when a substantial increase in the data throughput of the infrastructure occurs. It is worth noticing that the SMGW is designed to provide scalability at component level in order to be added to the system in a dynamic and non-intrusive way.

To get insights about how the different modules interact, let us consider a Man In the Middle Attack (MITM) on a communication link between a SCADA component and a SCADA server. The probe installed on the communication link provides the detection layer with information about the attack activity. The data are analysed and classified according to a priority ranking. They are further refined with details on their reliability and potential targets to provide input for the Fast Control Loop. The Risk Analysis Tool (RANT) assesses the threat level for each component according to the security parameters. It also computes the risk level by cross-matching the threat of the targets with the level of vulnerability retrieved from the vulnerability management system in the Slow Control Loop. The output of the RANT, i.e., the current risk of the components, is analyzed by the RP that is able to infer the potential cascading effect at operational level: it provides different scenarios to help the operator in defining the most reliable reaction strategy. At the same time, some countermeasures (e.g, data encryption on

the attacked communication link) are automatically set up to protect the system.

4. Cyber Detection System

The main component of the CDS is the Intrusion and Anomaly Detection System (IADS). The IADS constitutes an Heterogeneous Intrusion Detection System (HIDS) which is responsible for the cyber-security detection capabilities of the ATENA framework, by continuously monitoring the protected infrastructure to detect anomalous behavior or evidence of ongoing attacks.

The IADS architecture is based on the dominant SIEM paradigm which became popular after the first security incidents with considerable societal impact and visibility, such as the Stuxnet worm [1], the WannaCry Ransomware [16], and Flame [17]. Its architecture, illustrated in Figure 2, includes several components, namely: different types of probes, that provide the HIDS with security and safety-related evidence and data; a Domain Processor per scope, implemented by a Message Queuing system; a distributed SIEM, for evidence analysis.

The IADS is designed to decouple evidence-gathering, event transport and processing capabilities in a multi-layer model with several distinct stages.

Beside the aforementioned components, the platform includes a Management subsystem, as well as a Forensics and Compliance Auditing (FCA) module, designed to record and persist digital evidence retrieved from the cyber-analysis layer. Moreover, other sources such as service logs, Authentication Authorization and Accounting (AAA) sessions or physical access control systems are present for forensics and compliance auditing purposes.

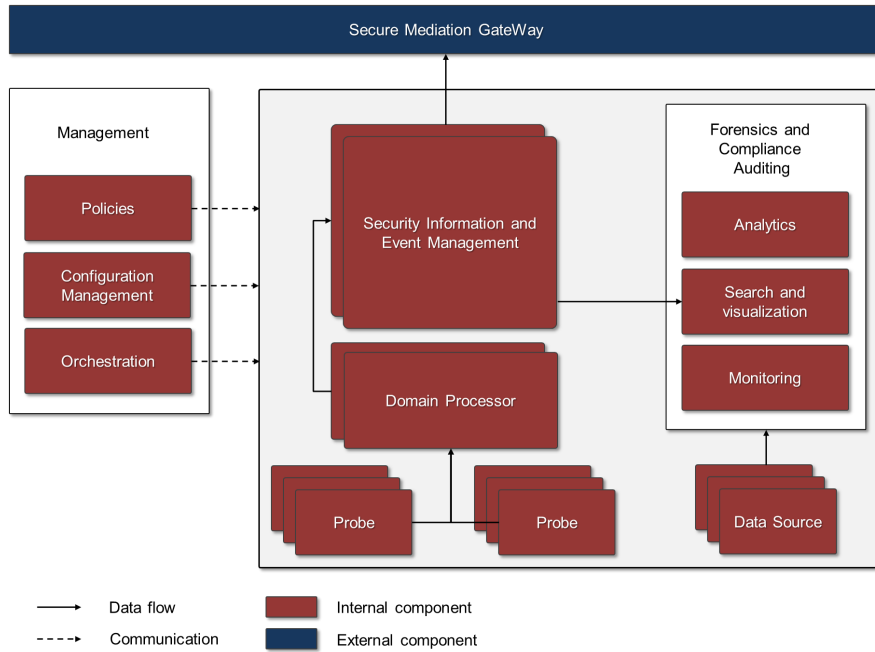


Figure 2: The IADS architecture of the ATENA project.

The output of the IADS Big-Data SIEM (containing information about analysis results or detected security issues) feeds the RANT and the RP module, via SMGW.

This information is encoded using the Intrusion Detection Message Event Format (IDMEF) (see RFC 4765 [18]), an experimental, vendor-independent standard for interchange of intrusion detection related events, enabling communication between different security infrastructures or involved actors. Moreover, IDMEF addresses several problems related to the representation of intrusion detection alert data by providing an homogeneous and normalized data model, which can be extended.

4.1. Probes

Probes or agents⁷ represent the lowest level of the IADS architecture, providing the detection capabilities, collecting evidence and providing event feeds regarding suspicious activities, to the cyber-physical layer. Several types of network, device and host security agents, and data sources are supported, as well as specific cyber-physical probes, such as the shadow security unit [11]. Events are generated using a custom format, supported by a flexible data model and encoding technique – this has the benefit of providing a normalized communication mechanism, designed for efficiency. Another reason for this approach has to do with the unsuitability of using already established formats, such as the Intrusion Detection Message Event Format (IDMEF - see RFC 4765 [18]) or the Incident Object Description Exchange Format (IODEF - see RFC 5070 [19]), which are either too complex (implying a significant overhead) or not expressive enough for the needs of the internal IADS probe communication mechanisms (however, IDMEF is indeed used for encoding IADS events exchanged with other ATENA components, a scope where it fulfills its originally intended role).

Third-party data sources are integrated as probes, by means of adaptors, whose purpose is to normalize data feeds and implement the client side for the interface between the detection agents and the IADS. In ATENA we can distinguish mainly between three types of agents:

- Statistical protocol probes: they capture different statistical attributes and send them to the domain processor. These statistical attributes

⁷We will use the term probes and agents interchangeably.

have been successfully used to identify network protocols [20, 21]. The statistical analysis uses different attributes to create a unique fingerprint of the flow and it is able to distinguish between compressed or encrypted protocols and clear-text protocols.

- Software Defined Network assisted probes: SDN is used to automate the deployment of virtualized probes (that are technically Virtual Network Functions), which can be launched according with the IADS needs. This allows the security operator for the IACS to instantiate and deploy probes across the network infrastructure, chosen from a library of available templates. This is effectively an NFV-based scenario where each probe is hosted within its own virtual environment (a container), with SDN providing traffic steering capabilities.
- Network signature agents: these agents are used to combine the advantages from signature-based detection techniques with the advantages from machine learning detection from the domain processor. A signature-based Intrusion Detection System (IDS) is adopted as a stand-alone agent which receives signatures from the IADS platform and sends all detected events through the data streaming platform.

4.2. Domain Processors

Domain Processors pre-process the information gathered from the probes, in order to reduce noise and aggregate events before their analysis. Domain processors are ideally deployed near the probe deployment points, where all relevant evidence for the IADS is collected. Despite their capabilities, Domain processors are more focused on mitigating and reducing data streaming

noise with a minimum overhead rather than analyzing the data itself. The domain processors implement the service-side endpoints for the probe interfaces.

4.3. The Distributed Big Data SIEM

The Distributed Big Data SIEM implements the main analytics capabilities for the IADS, encompassing two types of data modules: streaming (fast path, for online event stream processing) and batch processing (slow path, for slow jobs that may take time to complete). Moreover, the SIEM algorithms can be optionally fed with topology and eventually also asset information obtained from asset management tools or databases.

5. Slow Control Loop

The Slow Control Loop performs periodic scans of the CI configuration to address the detected vulnerabilities. It is organized in two modules: the Vulnerability Management System and the COMPoser (COMP). The former evaluates long-term vulnerabilities, while the latter provides off-line security.

5.1. Vulnerability Management System

This module protects IT systems in the period from the detection of new vulnerabilities to the implementation of the corresponding patch. This module detects threats linked to potential vulnerabilities and increases the awareness level of the operational teams when no cyber-attack is running. These tasks are crucial for computing the risk level of nodes, of services, and of the whole monitored system.

The VMS provides the following functionalities:

- The main functionality of the VMS is to score the vulnerability level of assets according to an extended Common Vulnerability Scoring System (CVSS). The VMS assesses the vulnerability level of components either by regularly and automatically querying it into an official database of vulnerabilities (e.g., National Vulnerability Database (NVD) [22], Common Vulnerabilities and Exposure (CVE) [23] database) or by using specific tools to infer the potential vulnerability of components (i.e. non-officially scored by a Computer Security Incident Response Team (CSIRT) [24] or by security experts). Moreover, ATENA project foresees to develop a Dark/Deep Net Analysis System, able to retrieve information on the vulnerability in the dark/grey market, or by specifically testing systems using automatic vulnerability scan systems or hardware/software configuration integrity control systems. The use of alternative sources to retrieve information allows setting up a dedicated database of vulnerabilities including both official, situational (e.g., bad configuration) and potential vulnerabilities:
- The creation of an interface for neighbouring CIs owners and for registered CSIRT, in order to report new vulnerabilities according to incident management of CIs or malware analysis in a confidential and dedicated manner. This functionality is useful to report vulnerabilities in supporting services in case of interdependent CIs and to increase the awareness level of the operators.
- The retrieval of cyber-threats information by means of IADS to update the vulnerability state of components according to the current situation

(e.g., the detection of a security breach in the perimeter increases the vulnerability of specific components previously protected).

- The visualization of the vulnerability state of the components to alert operators.
- The transmission of information to the COMP to improve the long-term mitigation strategies (e.g., hardening of security policy, management of patching campaigns).
- The transmission of vulnerability information to the fast control loop to assess the current risk of the CI.

It is worth noticing that the Vulnerability Management System (VMS) is integrated in the overall ATENA architecture and it is based on a well-known rating framework (i.e. Common Vulnerability System (CVS)) and on the relative taxonomies. Thus, it is able to feed the other modules, as well as standardized vulnerability database, in a proper manner.

5.2. Composer

The COMP module grants the off-line security by means of two functionalities. First it quantifies the current CI security level according to properly defined metrics; second, given the potential threats and countermeasures, it computes the optimal CI configuration to assure a desired, static, security level, exploiting the approach of composable security introduced in [25, 26].

Security can be achieved by exploiting four levels of information: assets to be protected, menaces/threats affecting these assets, countermeasures to mitigate the menaces, desired security level and context.

The COMP aims at extending the composable security framework to the cyber-physical domain. It takes into account component lifespan, physical consequences of cyber-attacks and the corresponding countermeasures. The COMP is organized in two modules:

- The Metrics Evaluator (ME) module evaluates the security level of a given configuration, based on the assets to be protected, the affecting menaces and the available countermeasures;
- The Optimal Configuration Computation (OCC) module computes the optimal configuration of CI elements that satisfies the target security level and the desired context. In particular, this module uses the metrics quantification capabilities offered by the ME to associate a security level to each potential system configuration. Then, according to proper optimization or heuristic-based algorithms, the OCC module ranks and sorts these configurations (i.e. candidate solutions) to identify the one that optimizes: the security level vs the desired one, and the actual context vs the desired one.

6. Fast Control Loop

The Fast Control Loop encompasses the human-in-the-loop paradigm. It is devoted to identify risks, evaluate the propagation of threats, support the operators in the selection of the reaction strategy, and implement the human decision. This is achieved by ad-hoc defined modules, namely, the RANT, the RP, the mitigation module and the orchestrator.

6.1. Risk Analysis Tool

This module assesses the current risk, based on the detection of cyber-threats and on the analysis of the vulnerabilities of the infrastructure components. The objective is to provide a risk oversight interface. To this end, the RANT provides five operations:

1. The encoding of the risk key metrics: a dedicated interface to CIs security is responsible to encode the initial risk key metrics of components, functional services or nodes according to the organizational measures in place, e.g. the impact value of availability loss for a specific node;
2. The extraction of the current vulnerability metrics of each component from the VMSs;
3. The forwarding from the detection layer (IADS) of the event information and the computation of the state of current cyber-threats;
4. The transmission of reliable information on the current risk for each node to the RP;
5. The provision of both a global and node level view of the risk.

The RANT assesses the risk in terms of service dependability according to a three-level rating (High/Medium/Low). The dependability criteria is considered as a weighted trade-off function of the following security criteria: availability, integrity, confidentiality, maintainability, and safety properties of the elementary services provided by the considered node. The assessed risk is forwarded to ATENA modules (e.g., RP).

6.2. Risk Predictor

The main objective of the RP is to assess the current situation and to envisage the consequences of adverse events, due to the existence of interdependencies among CIs.

The RP is a software platform (CISIApro), based on the Mixed Holistic Reductionist (MHR) approach [27]. MHR is a reference framework in which each infrastructure is divided into single components, services and holistic nodes. Components represent the reductionist level; they decompose the infrastructure into sections that can be affected by faults or cyber-threats. Services are considered as aggregated values of the components. Holistic nodes consider the system under analysis as a whole.

The RP is implemented as an agent-based simulator. Each component of the CI (i.e., device, service or macro-component) is represented by an agent. The agents are interconnected by using directed links in order to exchange information. Each agent receives resources and faults/threats from upstream agents and sends resources and faults/threats to downstream agents, and its state is represented by the operative level, i.e. the ability to properly produce its outputs.

The RP can manage the malfunctioning of a single component, the consequences of natural events or the impacts of cyber-threats. The RP evaluates the risk related to components and services by predicting the availability of crucial services.

The RP could run in a distributed fashion: in this case several CISIApro engines and databases are maintained up-to-date by exchanging only a small portion of information (e.g., the quality of service).

The output of the RP is a real-time assessment of the risk level associated to assets and its uncertainty; it is used in the mitigation phase for countermeasures ranking.

6.3. Mitigation module

The mitigation module, based on the risk level computed by the RP, provides the operator with a list of the optimal countermeasures to be used in the current state, or to be applied to update the “reaction trajectory” as the state evolves. To this end, it improves the decision process by considering both the current and future states of the system. Moreover, it considers the cascading effects among interconnected infrastructures and the impact of cyber-threats [28]. The mitigation module is designed as a set of algorithms that suggests the reaction strategy to CI operators, based on multiple criteria.

Envisaged reaction algorithms include:

1. Reconfiguration of network services according to the orchestrator module;
2. Physical network topology reconfiguration, to prevent and react to adverse events by restoring the service [29];
3. Optimal control, to schedule in a more efficient way critical interconnected equipment [30].

Based on the output of the mitigation module, the operator takes its decision and applies it through the SCADA control centers and through the orchestrator module.

6.4. *Orchestrator*

The orchestrator is a distributed framework designed for dynamically managing the telecommunication infrastructure from a security point of view. The aim of this module is to virtualize the security functions and to separate control and data planes, as usually done in SDN. It is based on a central logic unit, and several units deployed in the CI, including firewalls, SDN routers, and SDN switches.

The services provided by the orchestrator are:

- Dynamical association between orchestrator and controlled units;
- Dynamical management of trust relationships among orchestrator and application logic based on mutual authentication and continuous monitoring of application logic reputation;
- Isolation of each security domain based on interfaces enabling the use of a minimal set of operations and communications between different domains;
- Adoption of trusted component.

Basically, the orchestrator takes inputs from the mitigation module and, under the supervision of the operator, applies the best security reaction strategy on the telecommunication network implementing a Software Defined Security (SDS) approach as shown in Figure 3. As introduced in [31], SDS is a framework mimicking the SDN approach that has been successfully being applied for managing communications networks. The main goal of SDS is the decoupling of the control and the operation part of a security system by

exploiting virtualization of security techniques. This approach has been applied to IoT networks [32] and to SDN-based 5G networks [33]. In ATENA, this concept is extended to the monitoring of the telecommunication networks as well as to the monitoring of high level information shared through the CI network.

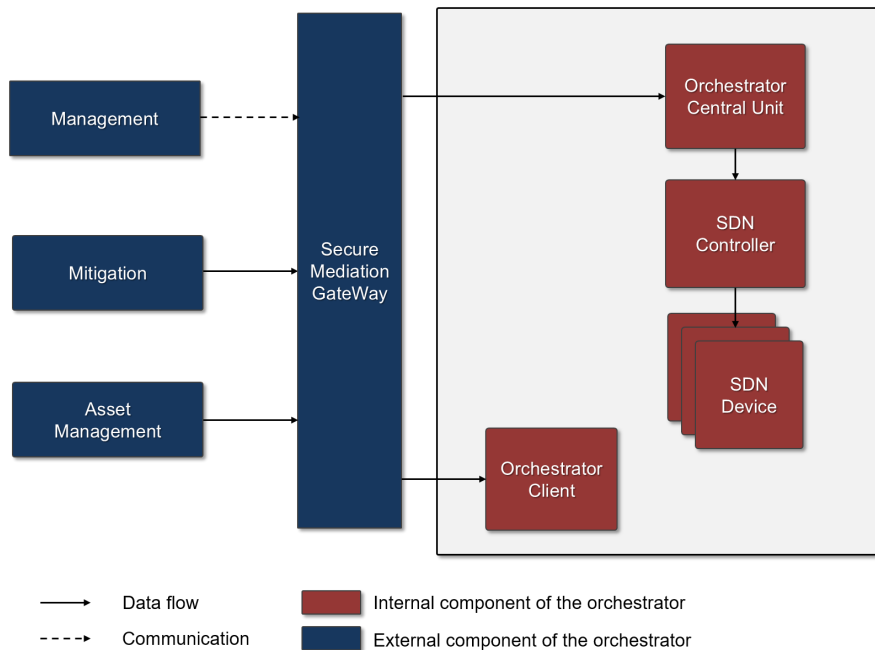


Figure 3: The orchestrator architecture of the ATENA project.

7. Discussion and Conclusions

This paper presents a novel logical security framework for IACs. This has been designed in the ATENA project, based on the outcome of previous projects and the state-of-the-art. The main modules of the architecture are the IADS, the Slow Control Loop, and the Fast Control Loop. These modules

are interconnected through the SMGW that grants the security of the shared information.

A prototypal release of SMGW was designed in the MICIE project, and was improved in the CockpitCI framework. In this case, it played a central role in achieving security awareness by sharing information on detected cyber-attacks between interdependent CIs. In ATENA, the SMGW is further improved. It assures the secure, efficient and reliable exchange of data within the entities belonging to the same or a different CI. It also shares information arising from both local and remote entities, to increase the resilience level of the whole system. Moreover, the SMGW is responsible for intercepting and handling every message generated by the ATENA modules (or from components not in the ATENA platform), by filtering anomalous messages and routing them to the right end-points.

The ATENA IADS adopts an integrated approach which takes into account aspects such as safety, reliability, availability and cost of ownership and operation, thus overcoming the limitations in the state-of-the-art. The domain processors, message queue brokers and the Big Data SIEM functional modules are designed with built-in scale-out capabilities. This makes it possible to fine-tune each IADS deployment to the needs of the protected infrastructure (i.e. number of events, sources, multiple domains), while maintaining the ability to accommodate further growth.

The main feature of the Vulnerability Management system is the ability to retrieve information from both official and alternative sources in order to set up a complete dedicated database of potential vulnerabilities.

Modeling and analyzing CI interdependencies is a broad research area

that generates many tools and methodologies [34]. The RP is innovative from different perspectives [35]. It is fed by real data generated from the control centers of the different CIs, so it evaluates the consequences of adverse events on a regular basis, usually on a second-based scale. It collects information from the IADS on actual threats and maps them into risks by means of the RANT. It explicitly considers the Quality of Service (QoS) of each CI; therefore, it assesses the consequences of faults and cyber threats not only on devices but also on the provided service to the customers. In this way, ATENA proposes a beyond-the-state-of-the-art reaction module. It counteracts incidents, and provides a dynamic and closed-loop response. It provides proactive features to the operator by suggesting countermeasures to be implemented in case of threats and attacks.

The ATENA architecture will be validated into the Hybrid Environment for Development and Validation (HEDVa) testbed provided by Israel Electric Corporation (IEC) as an hybrid operational environment. The HEDVa is a distributed environment with multi-tenant capabilities for the simultaneous coexistence of different lab environments, and the integration of emulated scenarios and physical components. The HEDVa was developed to overcome the issues related to validation of research projects. For example, in the CockpitCI project, it supported the development and validation of models for cyber-attack detection and mitigation mechanisms. In the ATENA project, the HEDVa supports the definition of larger case studies where interdependencies among different CIs and within the same CI are considered.

Acknowledgements

This work has been carried out within the framework of the H2020 ATENA project [8], which is aimed at developing ICT networked components for the detection of and reaction to adverse events in the context of cyber-physical security for CI, the authors express their gratitude to all the partners and teams involved in the consortium.

References

- [1] D. Kushner, The real story of stuxnet, *IEEE Spectrum* 50 (2013) 48–53.
- [2] C. Alcaraz, G. Fernandez, F. Carvajal, *Security Aspects of SCADA and DCS Environments*, Springer Berlin Heidelberg, 2012.
- [3] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. R. Sadeghi, M. Maniatakos, R. Karri, The cybersecurity landscape in industrial control systems, *Proceedings of the IEEE* 104 (2016) 1039–1057.
- [4] M. M. Ahemd, M. A. Shah, A. Wahid, Iot security: A layered approach for attacks defenses, in: *2017 International Conference on Communication Technologies (ComTech)*, pp. 104–110.
- [5] M. Cheminod, L. Durante, A. Valenzano, Review of security issues in industrial networks, *IEEE Transactions on Industrial Informatics* 9 (2013) 277–293.
- [6] A. Chattopadhyay, A. Prakash, M. Shafique, Secure cyber-physical systems: Current trends, tools and open research problems, in: *Design*,

- Automation Test in Europe Conference Exhibition (DATE), 2017, pp. 1104–1109.
- [7] D. Urbina, J. Giraldo, A. A. Cardenas, J. Valente, M. Faisal, N. O. Tippenhauer, J. Ruths, R. Candell, H. Sandberg, Survey and new directions for physics-based attack detection in control systems, US Department of Commerce, National Institute of Standards and Technology (2016).
- [8] ATENA Consortium, ATENA: advanced tools to assess and mitigate the criticality of ict components and their dependencies over critical infrastructures, <https://www.atena-h2020.eu>, 2016.
- [9] P. Capodiecici, S. Diblasi, E. Ciancamerla, M. Minichino, C. Foglietta, D. Lefevre, G. Oliva, S. Panzieri, R. Setola, S. De Porcellinis, F. Delli Priscoli, M. Castrucci, V. Suraci, L. Lev, Y. Shneck, D. Khadraoui, J. Aubert, S. Iassinovski, J. Jiang, P. Simoes, F. Caldeira, A. Spronska, C. Harpes, M. Aubigny, Improving resilience of interdependent critical infrastructures via an on-line alerting system, in: COMPENG 2010 - Complexity in Engineering.
- [10] T. Cruz, J. Barrigas, J. Proenca, A. Graziano, S. Panzieri, L. Lev, P. Simoes, Improving network security monitoring for industrial control systems, in: Integrated Network Management (IM), 2015 IFIP/IEEE Int. Symposium on, pp. 878–881.
- [11] T. Cruz, L. Rosa, J. Proenca, L. Maglaras, M. Aubigny, L. Lev, J. Jiang, P. Simoes, A cyber security detection framework for supervisory control

- and data acquisition systems, *IEEE Transactions on Industrial Informatics* 12 (2016) 2236 – 2246.
- [12] M. Roesch, Snort: Lightweight Intrusion Detection for Networks., in: *Proceedings of LISA '99: 13th Systems Administration Conference*, volume 99, pp. 229–238.
- [13] Trend Micro, Inc., Open source security, <http://www.ossec.net>, 2017.
- [14] P. Simões, T. Cruz, J. Proença, E. Monteiro, Specialized honeypots for SCADA systems, in: M. Lehto, P. Neittaanmäki (Eds.), *Cyber Security: Analytics, Technology and Automation*, volume 78 of *Intelligent Systems, Control and Automation: Science and Engineering*, Springer International Publishing, 2015, pp. 251–269.
- [15] P. Simões, T. Cruz, J. Gomes, E. Monteiro, On the use of honeypots for detecting cyber attacks on industrial control networks, in: *12th European Conference on Information Warfare and Security (ECIW 2013)*.
- [16] CERT-MU, The WannaCry ransomware, <http://cert-mu.govmu.org/english/documents/white%20papers/white%20paper%20-%20the%20wannacry%20ransomware%20attack.pdf>, last visited: November 2017.
- [17] S. Zhioua, The middle east under malware attack dissecting cyber weapons, in: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, pp. 11–16.
- [18] H. Debar, D. Curry, B. Feinstein, The intrusion detection message exchange format (rfc 4765) (2007).

- [19] R. Danyliw, J. Meijer, Y. Demchenko, The Incident Object Description Exchange Format, RFC 5070, RFC Editor, 2007. <http://www.rfc-editor.org/rfc/rfc5070.txt>.
- [20] C. Köhnen, C. Überall, F. Adamsky, V. Rakocevic, M. Rajarajan, R. Jäger, Enhancements to Statistical Protocol IDentification (SPID) for Self-Organised QoS in LANs, in: ICCCN 2010 Track on Network Algorithms, Performance Evaluation and Theory (NAPET) (ICCCN 2010 NAPET), Zurich, Switzerland.
- [21] E. Hjelmvik, W. John, Statistical Protocol IDentification with SPID: Preliminary Results, in: sourceSwedish National Computer Networking Workshop.
- [22] National Institute of Standards and Technology, U.S. Department of Commerce, Nvd: National vulnerability database, <https://nvd.nist.gov/>, 2017.
- [23] US-CERT, U.S. Department of Homeland Security, Cve: Common vulnerabilities and exposures, <https://cve.mitre.org/>, 2017.
- [24] CSIRT, Computer security incident response team, <http://www.csirt.org/>, last visited: November 2017.
- [25] A. Fiaschetti, A. Morgagni, M. Panfili, A. Lanna, S. Mignanti, Attack-surface metrics osstmm and common criteria based approach to composable security in complex systems, WSEAS Transactions on Systems (2015).

- [26] A. Fiaschetti, V. Suraci, F. D. Priscoli, The shield framework: How to control security, privacy and dependability in complex systems, in: 2012 Complexity in Engineering (COMPENG). Proceedings, pp. 1–4.
- [27] S. D. Porcellinis, S. Panzieri, R. Setola, Modelling critical infrastructure via a mixed holistic reductionistic approach, *International Journal of Critical Infrastructures* 5 (2009) 86–99.
- [28] D. Masucci, C. Palazzo, C. Foglietta, S. Panzieri, Enhancing decision support with interdependency modeling, volume 485, 2016.
- [29] D. Masucci, C. Foglietta, C. Palazzo, S. Panzieri, Improved multi-criteria distribution network reconfiguration with information fusion, in: FUSION 2016 - 19th International Conference on Information Fusion, Proceedings.
- [30] S. Imbrogno, C. Foglietta, C. Palazzo, S. Panzieri, Managing decisions for smart grid using interdependency modeling, in: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016.
- [31] L. Yanbing, L. Xingyu, J. Yi, X. Yunpeng, Sdsa: A framework of a software-defined security architecture, *China Communications* 13 (2016) 178–188.
- [32] F. Olivier, G. Carlos, N. Florent, New security architecture for iot network, *Procedia Computer Science* 52 (2015) 1028 – 1033. The 6th International Conference on Ambient Systems, Networks and Technologies

(ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015).

- [33] X. Liang, X. Qiu, A software defined security architecture for sdn-based 5g network, in: 2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), pp. 17–21.
- [34] G. Stergiopoulos, E. Vasilellis, G. Lykou, P. Kotzanikolaou, D. Gritzalis, Classification and Comparison of Critical Infrastructure Protection Tools, Springer International Publishing, Cham, pp. 239–255.
- [35] C. Foglietta, C. Palazzo, R. Santini, S. Panzieri, Assessing cyber risk using the CISIApro simulator, volume 466, 2015.