Noname manuscript No.
(will be inserted by the editor)

Smart Behavioural Filter for Industrial Internet of Things

A Security Extension for PLC

Giovanni Corbò · Chiara Foglietta · Cosimo Palazzo · Stefano Panzieri

Received: date / Accepted: date

Abstract We are currently experiencing the fourth industrial revolution. This is what the German government initiative, first, has identified with 'Industry 4.0'. The manufacturing future will be marked and will go through the new automation technologies that are being introduced with Industrial Internet of Things (I2oT). Industrial Control Systems (ICSs) are exploiting I2oT for reducing costs and improving efficiency. However, ICSs are already jeopardized by an increasingly large set of threat vectors. Those threats are used by malicious actors to misuse physical Critical Infrastructures that usually are vital services for well-being. I2oT implementation increases the threat surface, generating new possible vulnerabilities.

Information Technology (IT) classical approaches to cyber attacks cannot be applied to ICS due to their extreme differences from main priorities to resource constrains. Therefore, innovative approaches and equipment must be developed to suit with ICS world. In this paper, a Smart Behavioural Filter (SBF) for the PLCs (Programmable Logic Controllers) is proposed aiming to secure the PLC itself against logic attacks, that are stealth for other more classical security approaches. An example of the considered logic attacks is many open and close commands towards a valve in a short time. Those logic attacks are usually a sequence of well-formed packets in which the content

The research paper is partially supported by the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 700581 (ATENA - Advanced Tools to Assess and Mitigate the Criticality of ICT Components and Their Dependencies over Critical Infrastructures) www.atena-h2020.eu

G. Corbò
University "Roma TRE", Via della Vasca Navale 79, 00146 Rome, Italy
E-mail: corbo.giovanni@gmail.com

C. Foglietta, C. Palazzo, S. Panzieri
University "Roma TRE", Via della Vasca Navale 79, 00146 Rome, Italy
E-mail: chiara.foglietta@uniroma3.it, cosimo.palazzo@uniroma3.it, stefano.panzieri@uniroma3.it

represents an anomalous and unpredicted behaviour. This smart field equipment can react in short time to cyber attacks isolating the PLC, communicate with other equipment like itself and increasing in general the resilience of the physical system. It can also generate alarms for the local Intrusion Detection System (IDS).

The proposed equipment has been developed and validated in a real testbed within the FP7 CockpitCI project and H2020 ATENA project.

Keywords Industrial Control System · Security · Logical Filtering · Industrial Internet of Things (I2oTs) · Industry 4.0

1 Introduction

Critical Infrastructures (CIs) are a vital set of physical systems for our wellbeing. Among them, we remember power grids, telecommunications, water pipelines and transport networks. Those geographically distributed physical processes are continuously monitored and controlled by means of Industrial Control Systems (ICSs). ICSs are typically mission-critical applications with a high-availability requirement and they include SCADA (Supervisory Control And Data Acquisition) systems, PLCs (Programmable Logic Controllers) and DCSs (Distributed Control Systems). SCADA systems are usually composed of a set of networked devices, such as sensors, actuators, controllers and communication equipment. The SCADA server gathers real-time data from PLCs and issues control commands (i.e., open or close electrical switches) towards field devices to control the physical process.

Due to the cyber-physical interaction, a cyber incident involving ICSs can have a direct effect on the physical world, as demonstrated by the Stuxnet worm attack that turned off a centrifuges' control system in a nuclear plant [9]. Stuxnet provided proof-of-concept and demonstrated the feasibility of a cyber attack to change the physical processes. Highly-skilled attackers can be the most harmful, causing a loss of observability, controllability or eventually the loss of power in the physical system. In this paper, a highly-skilled attacker is a person with multiple capabilities: the ability to stealthy penetrate within a telecommunication network and the ability to discover the physical process controlled by means of the network.

Nowadays, the ICSs faced new challenges due to the increase of interconnected devices and due to the use of standard hardware, software and network. The separation of ICS and Information Technology (IT) worlds is becoming fuzzy due to operational efficiency and cost reduction. Cloud infrastructure and Industrial Internet of Things (I2oT) have been integrated within ICS. This new paradigm increases the resilience of the physical process, but brings with it an increasing cyber threat exposure. On October 2016, a series of Distributed Denial of Service (DDoS) attacks caused widespread disruption of legitimate internet activity in the US. [**?**] This attacks have been perpetrated by means of a large number of unsecured internet-connected digital devices,

the vast Internet of Things. The same problem can also appear in an industrial environment where sensors and actuators can act differently than expected.

In [8], the various type of attacks on SCADA systems have been grouped into network protocol and application protocol attacks. In the network protocol attacks, the hacker exploits weak points of network protocols, such as Modbus TCP/IP, that have several serious vulnerabilities [7]. The common types of those attacks are Denial of Service (DoS), scan and host discovery. Application protocol attacks can cause damage to field devices by sending out improper commands, because authentication or cryptographic mechanisms are not supported. In general, application protocol attacks use unconventional commands at irregular interval, substituting the regular and predictable sets of commands used for communication between SCADA servers and field devices. In both cases, these attacks are preceded by some steps of information gathering devoted to finding vulnerability security flaws in the network.

Network segmentation following IEC 62443 [13] is the best practice for SCADA system security and takes advantage of SCADA-aware firewalls and multiple layers of defence, the so-called Defence in Depth approach. This approach can be extended till the PLC, implementing a firewall for each PLC.

In this paper, we consider a highly-skilled attacker able to gain the access of a SCADA network and to disrupt the physical process before the intrusion is detected by sending syntactically and semantically valid command but with an harmful power due to their sequence. A false logic attack, as in [11,10], is invisible to most of the Intrusion Detection Systems (IDSs), because it uses well-formed packets with a content that is allowed even if a logic constraint is violated. An example of false logic attack is a sequence of opening and closing commands to a valve. The proposed appliance can be applied to I2oT field, because it is low resource consuming and can be integrated into each firmware device to protect the device from external bad commands or requests.

1.1 Contributions

The contribution of this paper is threefold. Although a host-based intrusion detection system for anomaly behaviour is not new, its use within a SCADA network is still a research area that is far from being completely explored. The appliance presented in this paper is a behavioural filter that must be inserted between each Remote Terminal Unit (RTU) or Programmable Logic Controller (PLC) and the field network to intercept packets carrying incorrect or dangerous commands. ITo properly act, the Smart Behavioural Filter (SBF) must be undetectable and transparent for an external actor. In this paper, we describe it as external appliance respect to a PLC, but the best solution is to integrate this SBF within the PLC, such as an Ethernet-based module integrated with the SBF appliance.

The device (i.e., SBF) communicates with other similar appliances and with a possible local Intrusion Detection System (IDS) through an additional security channel for transmitting or receiving alert messages. The proposed

solution is a radio frequency channel invisible to an external actor connected through Ethernet. Since the bandwidth is wide enough to send alert messages, the channel is encrypted to reduce security vulnerabilities.

The SBF is also a reaction tool: when the network is attacked, messages coming from IDS can increase its own security level to protect the behind PLC enforcing strict controls on all incoming connections.

This component can be seen as the last frontier in each Industrial Internet of Things device, where the SBF can improve the resilience without affecting the device efficiency and with reduced costs.

1.2 Paper Organization

The paper is organized as follows: Section 2 surveys the literature of the appliances for anomaly behaviour; in Section 3 the ecosystem made of several smart appliances in a SCADA network is described in order to provide an overall picture of the main functionalities; in Section 4 the Smart Behavioural Filter (SBF) is detailed in terms of functionalities and design; Section 5 is devoted to implementation and to first results; finally, conclusions and future works are in Section 6.

2 Related Works

A SCADA system is considered a critical control system since it monitors and controls the performance and availability of other critical infrastructures, such as transport systems, energy suppliers, water treatment systems or communication systems.

During the last years, several defence approaches have been studied. One of the first recommendation is to segment the SCADA network from the enterprise one using suitable firewalls to protect PLCs/RTUs from unauthorized requests that originate from outside the field. [12] In time-critical systems, firewalls must be carefully introduced for reducing additional packet latency. Filtering unwanted traffic by means of a firewall can increase the network performances. [14]

Firewall are classified into two categories: packet filtering and application firewall. Packet filtering has been recommended as an effective way to protect field devices from network protocol attacks. This appliance monitors incoming and outgoing packets and allows them to route or drop based on filtering rules using layer three and four on OSI model. [8]

An application firewall (or proxy server) is placed between a client application and a server, acting as an intermediary never allowing a direct connection between them. [3] The application firewall adds the capability of examining specific application traffic, such as FTP services, OPC servers or others. Coverage for SCADA applications is limited and performance impact is typically greater than other firewall types. The benefits of using this method are important because the application firewall is the only thing exposed to untrusted

traffic. The disadvantage of the approach is that it must be tuned to each application allowed. [**?**]

In this paper, we present an advanced filter for detecting false logic attacks, realised as a module of a classic PLC. A false attack [11] considers two different possibilities:

- False data values, where the attacker changes the data coming from sensors, see the literature related to false data injection [5]. This type of attack will be included in the future improvements of the appliance;
- False logic commands, where the attacker changes the logic of the control commands. This type of attack is the focus of this paper.

In [11, 10], the feasibility of a false logic attack is modelled considering the case of two valves that can be opened or closed. Two logic constrains are considered: (1) they cannot be both in open state, and (2) valve 1 should be opened before valve 2. The results of this paper demonstrate how a traditional Intrusion Detection System (IDS) is not able to effectively protect the physical process. The Smart Behavioural Filter (SBF) can detect the violation of a logic constraint implemented as a rule. The detection capabilities of the SBF are similar to the ones actually presented in BRO-IDS [2].

The SBF is also able to react to a cyber attack already inside the network or to increase security level in event of threats. The concept is coming from the automation world where the system must react to disturbance at least in steady state. Network Function Virtualization provides new opportunity to design mitigation solutions, as in [6]. In this case, the reaction approach is based on increasing the security level of the PLC by means of the SBF.

In the following Section, the ecosystem is detailed. The smart ecosystem is realized using a set of Smart Behavioural Filters (SBFs) placed just in front of the PLCs that can interact between them and with a local IDS using an additional radio-frequency channel. The aim is to describe how SBFs can interact one with each other and how they can react to cyber threats.

3 Smart Ecosystem

In Fig. 1, the architecture of the smart ecosystem is depicted. The Smart Behavioural Filter filters the commands coming from the SCADA system through a set of rules and analyses the information coming from the other elements of the smart ecosystems to react in event of identified anomaly. The SBF has three channel:

1. A legacy channel for receiving/sending command packets from and to the SCADA system;
2. An additional channel for communicating with the PLC/RTU to send authorized commands;
3. An additional channel for exchanging messages with the other SBFs or with an IDS. This channel has been realised using radio-frequency module.

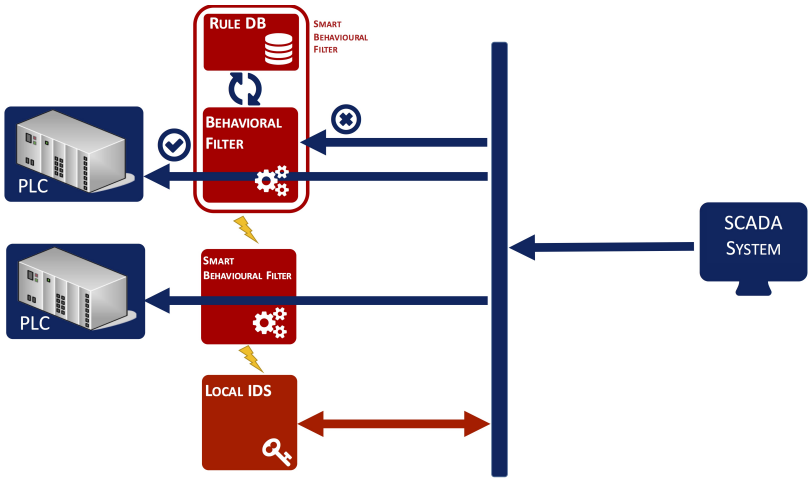

Fig. 1 system diagram of the smart ecosystem, where blue icons represent the legacy SCADA system and the red ones represent the elements of the smart ecosystem.

The first additional channel for communicating with the PLC/RTU must guarantee the transparency of the SBF and the undetectability of the PLC/RTU itself: the SBF substitutes the PLC/RTU and the SCADA system talks with the SBF, believing it is the PLC/RTU behind. In this way, the SBF is working as a firewall for the PLC/RTU.

The second additional channel for communicating with the other SBFs or with a local IDS is a radio frequency module, allowing for mesh networks. This radio frequency channel adds new vulnerabilities, but has the advantage to be not easily detected by an external actor coming from an Ethernet connection. The possible solution is to use cryptographic solutions in the exchange of messages due to the small amount of information without affecting the velocity.

The aim of this ecosystem is a local and fast reaction to advanced cyber attacks. The SBF that intercepts a false logic attack blocks the commands and then can send an alarm to the IDS and to other near SBFs using the radio frequency. In this way, the SBF can increase the alert level and therefore augment the security controls in event of cyber attacks to other near facilities. The SBF can also be the last possible frontier against a cyber attack.

4 Smart Behavioural Filter (SBF)

Traditional RTUs/PLCs send to the SCADA server the actual data coming from sensors, receive commands to be translated for the actuators and execute fast and real time control strategies related to the physical process. The difference between a PLC and an RTU is usually hard to find especially because their functionalities overlap with each other. In this paper, we use both the terms RTU and PLC for identifying a remote controller which communicate

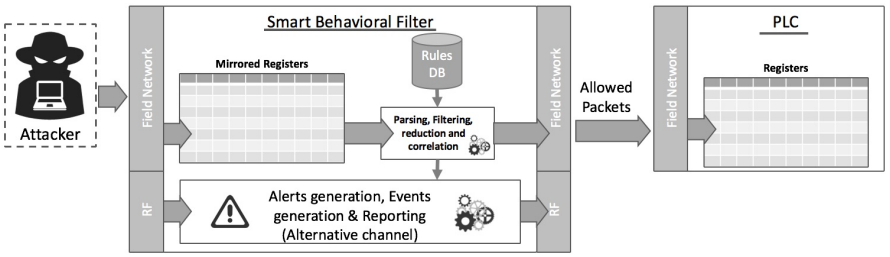

Fig. 2 Diagram of the Smart Behavioural Filter

with the SCADA server. The PLC is able to detect the disconnection of sensors or actuators.

The Smart Behavioural Filter (SBF) wants to add a new class of logical errors, detected directly by the PLC. Those errors are usually malicious cyber attacks but can also be generated from unintentional commands coming from an operator. These false logic errors are, among the others: contradictory instructions, dangerous or out of the normal operating cycle, or abnormal sequence of operations. This action can be also realised by means of an IDS, but analysis of the behaviour is easier to realise within the PLC.

The Smart Behavioural Filter (SBF) intends to create a further security element for industrial control systems. This new appliance element was created as a security system at application level which can work on industrial communication protocols. The technological solutions implemented in the SBF are mostly known and simple to apply but the smart combination (i.e., detection and reaction) allows us to get a very interesting and innovative element in the context of industrial security.

The SBF, in Fig. 2, is made of two main modes: the passive and the reactive one. The first concept is related to the filtering action, mainly related to logical constraints. The second one is related to the response and mitigation action: an SBF can cooperate with other SBFs in event of an attack, and can eventually change its operating mode until the complete isolation from the external world.

To filter packets, PLC registers and coils have been mirrored within the SBF to understand the impact of the received commands. The first important cyber security feature of SBF concerns the capability to create a kind of SandBox (a virtual controlled environment) that replicates the information system of a PLC. In those circumstances, a hypothetical intruder, which enters the SCADA network, believes he is changing the registers/coils value into the PLC performing successfully the cyber attack but without have any effect on system thanks to the SBF. The Ethernet module of the PLC is securely connected to the Ethernet module of the SBF, that substitute the PLC port. In this way, the SBF can guarantee to be undetectable to an intruder, who beliefs to communicate with the original PLC as in presence of a honeypot.

SBF implements a rule-based filtering, able to understand the effects of specific commands thanks to a set of rules. Those rules have been hard-wired

into the SBF starting from the knowledge of the physical processes. For a Medium Voltage power grid, the SCADA system reconfigures the physical network after a permanent failure, in well-define scheme. Therefore, the reconfiguration is a sequence of commands sent from the SCADA control system to the PLCs connecting the electrical switches. The possible reconfiguration procedures are modelled within the set of possible rules inside the SBF. The SBF is an application-level behavioural filtering performing an anomaly detection highly specialized in its own operative context.

To be an active appliance, each SBF is equipped with its own Radio Frequency (RF) module able to create a mesh-network between all the PLCs/RTUs with SBFs and with a possible local IDS. The radio frequency module has a limit due to the distance of the transmission channel. This RF element, in combination with the SBF, establishes a redundant wireless network between PLCs/RTUs of the same system and then a further preferential (or alternative) communication channel where transmits system alerts.

The system alerts can eventually activate specific rules that increase the security status of the PLC. The security status can require a higher level of authentication in performing specific commands. In the worst case, the PLC can be isolated from outside world for a limited amount of time to avoid a more dangerous situation and preserve the physical process actuators.

The additional radio frequency channel creates a new security issue, but it is invisible to a hacker which penetrates in the classical telecommunication network. The additional channel can exploit secure communications, such as encryption, due to the small dimension of the exchanged messages.

Briefly summarizing, an SBF can:

1. Mirror the PLC registers to deceive the intruder;
2. Recognize false logic events or sequence of events;
3. Alert the other closest SBFs and the eventual local IDS;
4. Increase its security level enforcing strict controls in accordance with a pre-set strategy.

In the following section the implementation of the proof of concept and some results are explained.

5 Proof of Concept

To implement the features described in the previous section, we need a platform that can:

- Receive commands from the field network
- Reconstruct the instructions received
- Filter through the rules' instructions
- Send the filtered commands to the connected PLC
- Send and receive alarm messages to / from the other SBFs
- React to cyber attacks increasing the security level

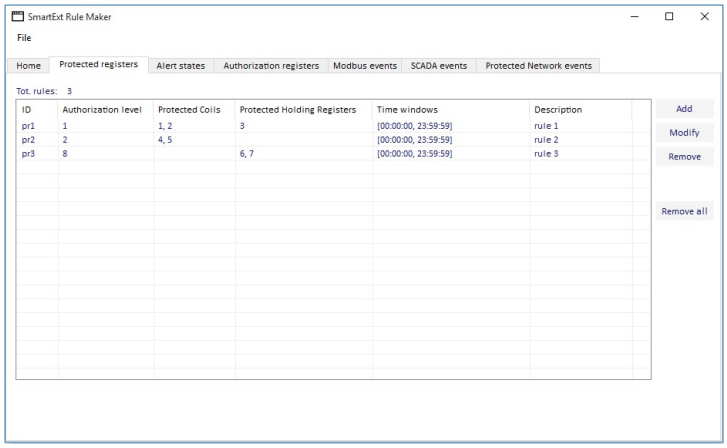

Fig. 3 rule maker interface with an example, where the rule has an identifier (ID), an authorization level, protected coils and registers, a time window and an optional description.

A standard RTU/PLC has a modular design, and usually consists of a Power Supply, a CPU, and an Input/output card. The actual and initial implementation of the SBF is realized on hardware using a microcomputer such as Raspberry PI.

The actual implementation of the SBF contains a rule maker, depicted in Fig. 3. Each rule is a row in a table, containing several columns:

1. Identifier: a unique identifier;
2. Authorization level: level 1 means the lowest level of authorization, level 2 means a higher level and so on; therefore, the SCADA command with authorization level 3 can bypass all the rules with authorization level 3 or less;
3. Protected coils or registers: the protected spaces of memory;
4. Time window: the period in which the rule is active;
5. Description: an optional description related to the rule.

To test the SBF, we consider as PLC a Schneider Electric Modicon M340 [1] with Modbus TCP/IP interface. The SBF receives packets and it is invisible to the downstream PLC and to the rest of the control network. The SBF is an advanced network card with additional processing capabilities.

The SBF has been integrated within the existing Roma TRE testbed [4]. The testbed is made of a SCADA server, a PLC and an IDS. Specifically, the IDS has been given the ability to communicate through the radio frequency (RF) protocol with the mesh network created by SBFs. This feature improves globally and locally the situational awareness. A soon as the IDS recognizes a potential threat it warns the control room and sends a broadcast alert message to the radio frequency network. Depending on the danger degree, the SBF can automatically reconfigure themselves to mitigate the threat.

The results are promising applied to the demo represented in Fig. 4. The example is a medium Voltage power grid with two substations (SUB in Fig. 4),

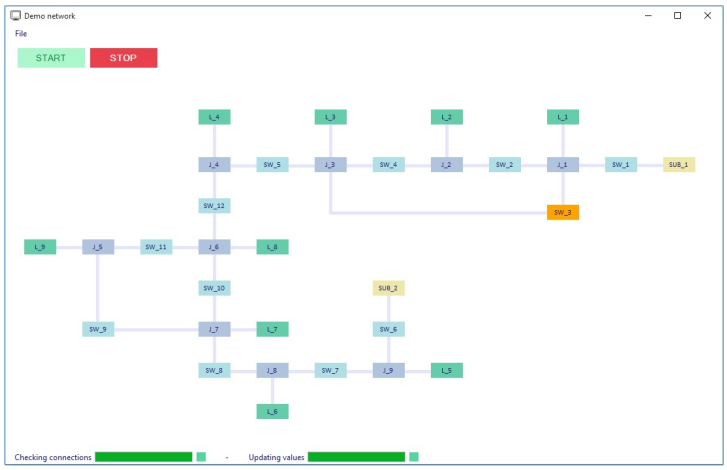

Fig. 4 example of a smart ecosystem: alert on SW_3.

which are feeding 9 loads (L in Fig. 4), and with 12 circuit breakers (SW), which are telecontrolled from the SCADA control centre in event of a permanent failure. Each circuit breaker has a PLC for exchanging messages with the control centre.

The Smart PLC (PLC and SBF, together) succeeds to recognize the dangerous instructions and sends an alert message to the control room. In Fig. 4, the circuit breaker 3 (SW_3) recognised an anomalous sequence of messages. In this example, the anomalous behaviour is a tentative to write on a never used set of registers that are not allowed. At the same time provides information on the incident to the other reachable Smart PLC (in the example in Fig. 5, SW_1 and also SUB_1) that are reconfigured in an appropriate way and, in case it is required, turn over the alert message to the control room. The IDS is able to communicate the details of an attack to the network of Smart PLC which reconfigures itself, thus obtaining an automatic response to the ongoing threat.

The SBF has been implemented and validated within the FP7 European CockpitCI project (www.cockpitci.eu) and it is still under development within H2020 European ATENA (www.atena-h2020.eu).

6 Conclusions and Ongoing Works

In this paper, we present a Smart Behavioural Filter (SBF) able to detect and block commands that are anomalous from a logic point of view. This anomalous behaviour can be interpreted as a very specific cyber attack performed by a high-skilled attacker.

The SBF is a passive firewall and is also a local reaction module for mitigating risk of cyber attacks. The SBF is the connection point between IDS, firewall and reaction strategies based on Software-Defined Network. To ex-

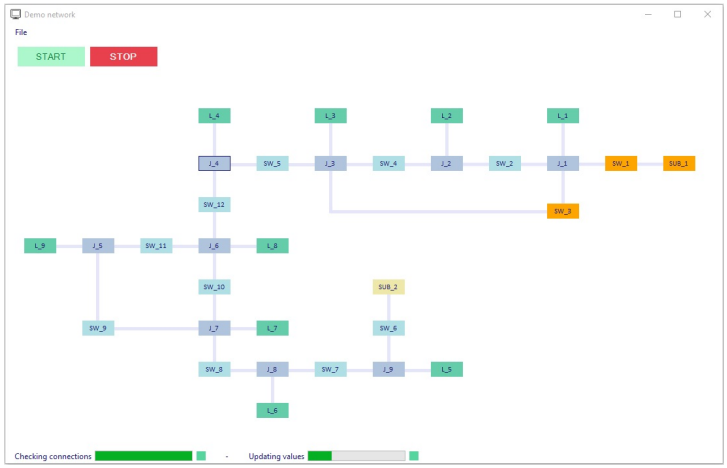

Fig. 5 example of a smart ecosystem: increasing the alert to the neighbourhood element of SW_3.

change securely information, the SBF has an additional and invisible radio frequency channel among SBFs and the IDS.

The actual implementation of the SBF is a proof-of-concept which demonstrates the feasibility of the proposed architecture. The SBF can be improved considering rules that can be modified or generated through an on-line training of the physical system. Another possible improvement is to change from a rule-based to an anomaly-based approach.

Actual works are more related to the Industrial Internet of Things (I2oTs), see Fig. 6. The SBF can also be applied in the modern industrial system. This is possible integrating a further module which is entrusted with the task of IoT Connector. This connector enables the outsourcing of the data coming from industrial sensors to collect and analyse them thanks to Industrial Cloud IoT. Therefore, the SCADA system transfers some functionalities to the Industrial Cloud IoT to improve performances, decrease start-up plant costs and enhance data mining.

References

1. Modicon M340 - Schneider Electric. URL `http://www.schneider-electric.com/en/product-range/1468-modicon-m340/`
2. The Bro Network Security Monitor. URL `https://www.bro.org/`
3. Abdul Aziz, M.Z., Ibrahim, M.Y., Omar, A.M., Ab Rahman, R., Md Zan, M.M., Yusof, M.I.: Performance analysis of application layer firewall. In: 2012 IEEE Symposium on Wireless Technology and Applications (ISWTA), pp. 182–186. IEEE (2012). DOI 10.1109/ISWTA.2012.6373838. URL `http://ieeexplore.ieee.org/document/6373838/`
4. Di Pietro, A., Foglietta, C., Palmieri, S., Panzieri, S.: Assessing the Impact of Cyber Attacks on Interdependent Physical Systems. pp. 215–227. Springer Berlin Heidelberg (2013). DOI 10.1007/978-3-642-45330-4_15. URL `http://link.springer.com/10.1007/978-3-642-45330-4{_}15`

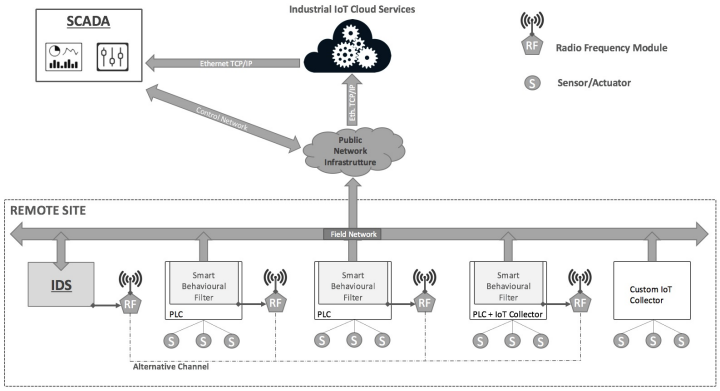

Fig. 6 Future development and possible integration with Internet of Things (IoTs)

5. Feng, Y., Foglietta, C., Baiocco, A., Panzieri, S., Wolthusen, S.D.: Malicious false data injection in hierarchical electric power grid state estimation systems. In: Proceedings of the the fourth international conference on Future energy systems - e-Energy '13, p. 183. ACM Press, New York, New York, USA (2013). DOI 10.1145/2487166.2487187. URL http://dl.acm.org/citation.cfm?doid=2487166.2487187
6. Fung, C.J., McCormick, B.: VGuard: A distributed denial of service attack mitigation method using network function virtualization. In: 2015 11th International Conference on Network and Service Management (CNSM), pp. 64–70. IEEE (2015). DOI 10.1109/CNSM.2015.7367340. URL http://ieeexplore.ieee.org/document/7367340/
7. Huitsing, P., Chandia, R., Papa, M., Shenoi, S.: Attack taxonomies for the Modbus protocols. International Journal of Critical Infrastructure Protection **1**, 37–44 (2008). DOI 10.1016/j.ijcip.2008.08.003
8. Kang, D.H., Kim, B.K., Na, J.C.: Cyber threats and defence approaches in SCADA systems. In: International Conference on Advanced Communication Technology, ICACT, pp. 324–327. Global IT Research Institute (GIRI) (2014). DOI 10.1109/ICACT.2014.6778974. URL http://ieeexplore.ieee.org/document/6778974/
9. Kushner, D.: The real story of stuxnet. IEEE Spectrum **50**(3), 48–53 (2013). DOI 10.1109/MSPEC.2013.6471059. URL http://ieeexplore.ieee.org/document/6471059/
10. Li, W., Xie, L., Deng, Z., Wang, Z.: False sequential logic attack on SCADA system and its physical impact analysis. Computers & Security **58**, 149–159 (2016). DOI 10.1016/j.cose.2016.01.001
11. Li, W., Xie, L., Liu, D., Wang, Z.: False Logic Attacks on SCADA Control System. In: 2014 Asia-Pacific Services Computing Conference, pp. 136–140. IEEE (2014). DOI 10.1109/APSCC.2014.27. URL http://ieeexplore.ieee.org/document/7175507/
12. Nivethan, J., Papa, M.: On the use of open-source firewalls in ICS/SCADA systems. Information Security Journal: A Global Perspective **25**(1-3), 83–93 (2016). DOI 10.1080/19393555.2016.1172283. URL http://www.tandfonline.com/doi/full/10.1080/19393555.2016.1172283
13. Piggin, R.: Development of industrial cyber security standards: IEC 62443 for scada and industrial control system security. In: IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp. 11–11. Institution of Engineering and Technology (2013). DOI 10.1049/cp.2013.0001. URL http://digital-library.theiet.org/content/conferences/10.1049/cp.2013.0001
14. Sheth, C., Thakker, R.: Performance Evaluation and Comparative Analysis of Network Firewalls. In: 2011 International Conference on Devices and Communications (ICDeCom), pp. 1–5. IEEE (2011). DOI 10.1109/ICDECOM.2011.5738566. URL http://ieeexplore.ieee.org/document/5738566/