OPANSec – Security Integrity Monitoring for Controllers

Mithil Parekh[1], Yuan Gao[2], Deeksha Gupta[3], Christian Luschmann [4]

Abstract: Industrial automation and control systems (IACS) are more and more a combination of standardized hardware and software components that are respectively linked. A continuous increase in digital Instrumentation and Control (I&C) in production lines and critical infrastructures lead to a remarkable increase in computer-based digital security risk [IE10]. The Internet of Things, services, data and people also opens up new avenues for data theft, industrial espionage and attacks by hackers [BM16]. Currently many solutions are available for industrial network and software but more focus is still required for controller programming integrity checks.

Keywords: Integrity monitoring, programming mode authentication, whitelisting, virus protection, intrusion detection, hardening of PLC.

1 Introduction

The standard IEC 62443 allows validating potential weaknesses of automation and control technology and developing effective protection measures [IE15b]. Though this standard focuses on IT security of IACS, which are necessary for reliable and secure operation of automated systems and infrastructures [IE15c], continuous integrity checks for program and hardware configurations of controllers is somewhere neglected [TS12][LR12].

The network-based cyber-attacks on IACS got worldwide attention after Stuxnet incident [LR12]. During the life cycle management, it has been emphasized that within the plant network, controllers must be isolated from the office network [IE13]. Therefore, till now, more efforts have been put on plant networks hardening. Even after adequately securing plant networks, there could be possible weaknesses, like Stuxnet, to breach security barriers in automated plants [DREP14]. Therefore, a new approach has already been developed by AREVA GmbH which protects integrity for controllers by monitoring.

[1] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätsplatz 2, 39106 Magdeburg, mithil.parekh@ovgu.de

[2] Otto-von-Guericke University Magdeburg, Research Group Multimedia and Security, Universitätsplatz 2, 39106 Magdeburg, yuan.gao@ovgu.de

[3] Areva GmbH, Henri-Dunant-str. 50, 91058 Erlangen, deeksha.gupta@areva.com

[4] Areva GmbH, Henri-Dunant-str. 50, 91058 Erlangen, christian.luschmann@areva.com

2 Literature review

There are various approaches which have been developed for security integrity monitoring for Programmable Logic Controllers (PLCs). A verification method has been developed to determine the safety and operability of PLC-based systems [MM94]. The method automatically checks sequential logic embedded in PLCs and provides counterexamples if errors are found. However, this modeling technique has been developed to verify only relay ladder logic. Another approach in [MS13] has a PLC backplane analysis system which connects directly to the PLC backplane to capture backplane communications between modules. WeaselBoard-backplane forwards inter-module traffic to an external analysis system that detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates [MS13]. This approach is based on real time monitoring but it is deployed on an additional workstation instead of on-device implementation. However, the approach is not practical but is recommended for understanding the properties of occurred vulnerabilities. PLC vendors normally do not guarantee for security if a backplane is used for capturing communication. But, OPANASec, as real-time and on-device security solution for PLC, takes just one cycle time for annunciation when the PLC integrity is being compromised.

3 Security integrity monitoring scope

With the advance of Industrial Ethernet solutions, increased networking with the office world and a large number of unprotected interfaces at the field level, security is of greatest importance. Therefore, knowledge of permitted communication relationships is a fundamental prerequisite for secure networks [IE10][SN13].

3.1 State-of the art for connecting office floors to automation facilities

In Fig. 1, a fundamental architecture is used for security solutions, especially to isolate industrial networks from office networks. The communication between two security zones (a concept introduced by IEC 62443) can be controlled by configuring a firewall and providing an additional zone which could be a Demilitarized Zone DMZ, as also described in IEC 62443. As indicated in Fig. 1, different security solutions like whitelisting, virus protection, and patch management are available for general IT application software. Some of these, like whitelisting, are also applicable for digital automation systems containing PLCs.

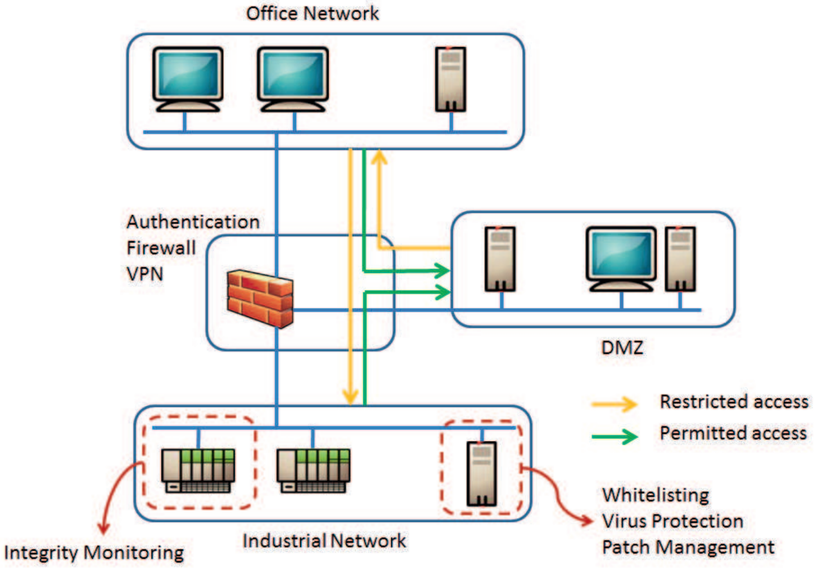


Fig. 1: Logically isolating plant controller by Firewall

3.2 Graded connections for high level Security Zones

Fig. 2 illustrates different graded security solutions for securely interconnecting industrial networks that are assigned to different logical security zones. Fig. 2(a) shows an elementary scenario without any type of control over the communication. This may be extremely dangerous and should usually be avoided for communication between different security zones. In the example in Fig. 2(b), the communication goes through a firewall, a scenario that was already elaborated in Fig.1. Particularly, SIEMENS recommends their own line of "Scalance S" security modules and "communication processor" for its platform. Difference between these modules and office-type devices is that these modules are hardened for use in industrial environments (IP30) and they are optimized for communication of process control information [SP12].

If two zones are physically separated without any hardwired interconnections or spanning networks, (non real-time) communication is still possible via an "air-gap connection". In this case, which is frequently encountered at legacy systems, a portable storage device (e.g. a USB key) can be used for information exchange. The portable storage device may feature support for authentication, see Fig. 2(c).

A further, often considered more expensive solution, is the deployment of physically unidirectional security gateways, also known as data diodes. These enforce the unidirectional communication at the hardware level.

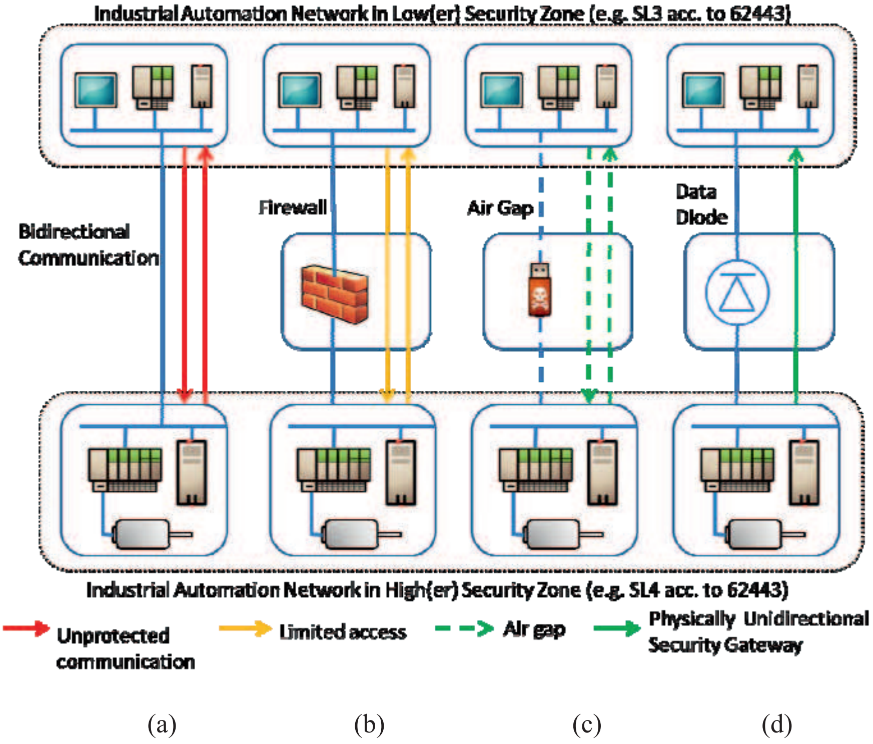

Industrial Automation Network in Low(er) Security Zone (e.g. SL3 acc. to 62443)
Bidirectional Communication
Firewall
Air Gap
Data Diode
Industrial Automation Network in High(er) Security Zone (e.g. SL4 acc. to 62443)
Unprotected communication
Limited access
Air gap
Physically Unidirectional Security Gateway
(a)
(b)
(c)
(d)

Fig. 2: Graded enforcement of communication restrictions between security zones

3.3 Secure connections originating from lower level Security Zones

Beyond the primary concern to isolate high security level zones, there are still many use cases where communication is required from site local intranets (lower security level) towards automation networks. Fig. 3 indicates a scenario in which a data diode is used to transfer set-points configuration files from a site-local intranet towards an automation network located in a higher security level zone.

This approach is resilient against many attack scenarios. While it provides a continuous communication, control and command loops that would allow a potential control from an outside location are not permitted.

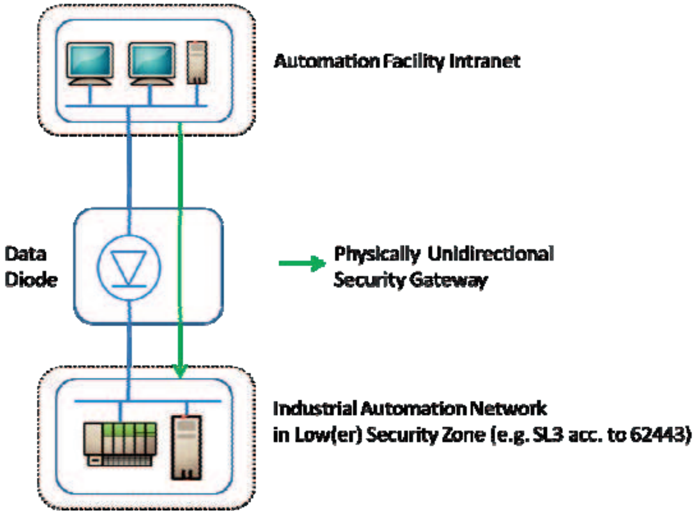

Automation Facility Intranet
Data Diode
Physically Unidirectional Security Gateway
Industrial Automation Network
in Low(er) Security Zone (e.g. SL3 acc. to 62443)

Fig. 3: Communication between Automation facility intranet to lower security zone

Additional verifications of the data received via the data diode can be performed based on the formal description of the content (e.g. simple syntax and semantics of a set-points file) using e.g. FPGA-based solutions, like SCOOP from seclab [SCO1].

3.4 Enforcing security integrity of automation systems

3.4.1 Motivation for the deployment of OPANASec

In an automated plant, the process control logic is mission- and, sometimes, life-critical, and is typically rigorously tested prior to deployment. It's remarkable that integrity checks are not performed on controller logic [WSGND]. Even if the PLC designers have not considered a malicious code threat, unintended changes to logic through memory manipulation and human error can have similar consequences.

OPANASec checks integrity of the application software and hardware configurations (including function block libraries) that run on PLCs. Therefore, it is suitable solution against types of attacks such as Stuxnet.

3.4.2 Existing security integrity monitoring solutions

Some security monitoring solutions already exist in current plant networks like whitelisting, anti-virus and patch management.

Application and file operations can also be considered by using whitelisting for controlling malicious activities. In this case, only specified, trusted applications can be run or only specified file operations can be performed. However, controlling a manipulation of the application programs and hardware configurations of PLCs is not implemented today as a standard. Therefore, this can be an ideal time to introduce OPANASec as a state-of-the-art security solution for PLCs.

Patch management is used as a security measure to protect applications of all security techniques described in this security concept. For example, a potential attacker must first overcome multiple security barriers before weak points from a lacking security update can be exploited [IE15].

However, unauthorized changes to PLC logic are not controlled here by assuming inherent trust in those possibly compromised systems.

4 The OPANASec approach

The OPANASec solution is the implementation of an access control and integrity monitoring solution for SIMATIC S7 Programmable Logic Controllers.

It consists of two function blocks. They are added to the existing PLC program and can be used in CFC (Continuous Function Chart), as well as FBD (Function Block Diagram), COP (Contact Plan) or STL (Statement List). The function blocks continuously monitor the user program of the PLC, the hardware configuration of the PLC and also the configuration of network connections for changes. The changes are detected by checksums over the relevant data. If a change is recognized, it is stored to the non-volatile diagnostics buffer and alerted at the output. The output can be used for alerting, signaling, shut down, etc. To avoid deletion of the integrity monitoring solution by an attacker (virus, malware, human), the two function blocks of the solution monitor each other, and if any block fails, it is recognized and an alert is created as presented in Tab. 1.

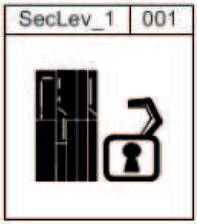
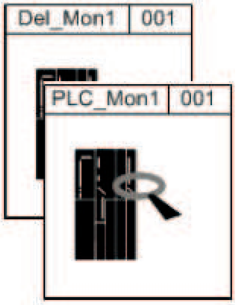
4.1 Key features

Some of the OPANAsec key features are:

- Easy integration into existing PLC programs in STL/FBD/COP [IE15a]
- Free usage of output signals (HMI/SCADA, Annunciation Lamps, SMS, etc.)
- Part of AREVA's NPLib (Nuclear Power Library) for S7, IEC62138 certified by TÜV Süd
- AREVA standard solution for S7-300/S7-400 including F/H-Systems.

4.2 Limitations

Currently this is only implemented for SIMATIC S7 PLCs.

Access control  	• Key-Switch for blocking of program changes • Effect on the whole program (operational & failsafe) • Two factor identification in combination with engineering environment
Integrity Monitoring  	• Online-Recognition of program changes on the PLC (including operational program code) • Online-Recognition of configuration changes (Parameterization of modules, network configuration) • Annunciation by SCADA and/or binary outputs • Logging of security events in diagnostic buffer and instance data block of PLC • Reciprocal self-monitoring of PLCMon and DelMon including annunciation of manipulation- and deletion attempts

Tab. 1: Two aspects of OPANASec

5 The OPANAsec implementation

The integrity monitoring is used together with another function block of the OPANASec solution, which implements a control of the programming mode (Access control). The “SecLev” function can lock the PLC, so programming is prohibited. If programming mode is needed, the PLC has to be unlocked. This task can be completed only by the “SecLev” function block itself. Thus, a signal that is given to the function block e.g. by a key-switch in the cabinet or remote signal from a control room is used. Only if this particular signal that allows programming is present, changes on the program, HW configuration or network connection configuration of the PLC can be performed. Together with a password in the engineering environment (engineering software), that means a two factor identification ensures secured implementation of programming.

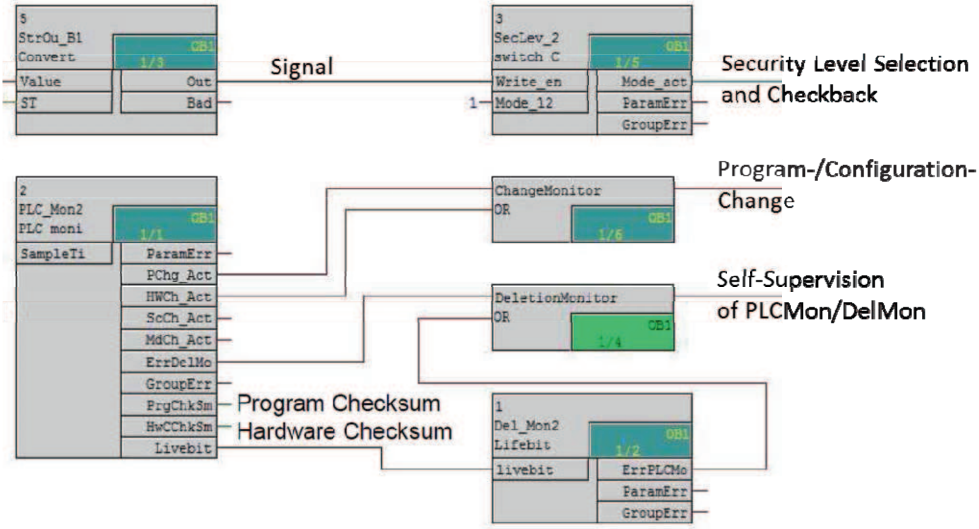


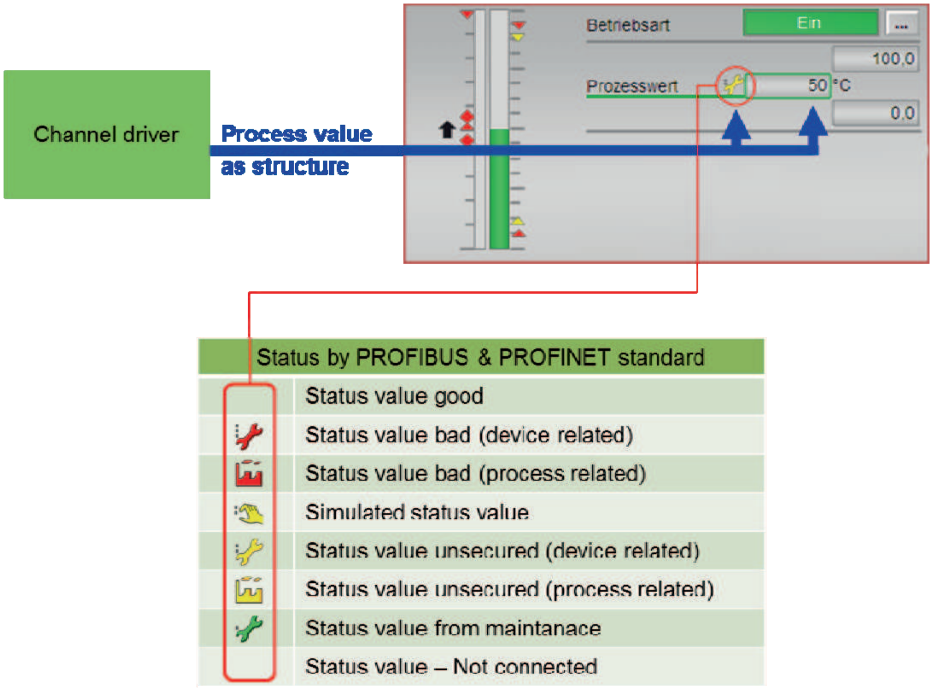
Fig. 3: Implementation of OPANASec

Only after access control through the “SecLev” function block is granted, a change/deletion in the PLC logic is possible. At each modification, an output signal from “ChangeMonitor” is generated and with this signal, it can be confirmed that an appropriate authentication is given to particular personnel, see in Fig. 3. Furthermore, using “Livebit”, both function blocks monitor each other against deletion. An annunciation is generated from “DeletionMonitor” if any of them is attempted for deletion.

6 Enforcing consistent security solutions for the process industry

The OPANASec approach described in the previous sections is effective in a framework of function diagrams and function blocks, as it is typically used in the process industry and for power plant automation. The difference, as compared to completely manual software development, is in the use of a comprehensive set of tools that generate most of the source code out of semi-formal graphical specifications.

The OPANASec function blocks make use of this framework to assure the software code integrity by a specific set of function blocks. Beyond this security integrity enforcement, further guidance on the design and interconnection of function blocks can be used similarly to security policies for secure code development. This guidance is at a higher level, as compared to source code level development details, like potential buffer overflows, handling of array indices or unsigned integer numbers arithmetic. An example of such guidance could be the recommendation (for lower security levels) or requirement (for higher security levels) to always accompany a signal value with a signal status. This obviously has a benefit for safety, as the signal status may be considered (as part of the “active status processing”) in decisions on whether to rely on the current signal value. Additionally, there are benefits for security, in case the status processing is performed at all stages starting at the smart signals that collect and distribute the initial values, over the network devices that receive and forward the values within application level data messages. Thus e.g. a denial of service attack at a network (between the smart sensor and a processing unit) would potentially result in obsolete data. However, the signal status can be used to indicate this (invalid / obsolete data), so that the obsolete signal value can be excluded from further computations that would result in the actuation of physical aggregates, see Fig. 4.



Status by PROFIBUS & PROFINET standard
Status value good
Status value bad (device related)
Status value bad (process related)
Simulated status value
Status value unsecured (device related)
Status value unsecured (process related)
Status value from maintanace
Status value – Not connected

Fig. 4: NPLIB Signal status

Such a library, called NPLIB (for Nuclear Power Library) is mandated by AREVA GmbH for selected applications, even if the implementation is performed by a subcontractor. This assures that, at a higher level of the data flow, appropriate security policies can still be implemented, based on assumptions that are reliably enforced. Otherwise, the different subcontractors may not intend or may not even be able to provide the needed security assurance. This is a supporting step for implementing the

IEC 62443-2-4 [IE15a] requirements for service providers and also in line with [II14].

7 Conclusion

Continuous Security Integrity Monitoring can be performed with efficient and effective technical security solutions like OPANAsec. In order to enforce security in line with the Security Levels (SL1 … SL4) of IEC 62443, additional solutions were addressed, like DMZ and Physically Unidirectional Security Gateways. While the use of physical data diodes may be more expensive than “air gap” connections, they may be mandatory for security conduits leading from high security level zones or in cases where real-time requirements cannot be met via manual “air gap” data exchange.

The function blocks that implement the OPANAsec solution are integrated into a certified function blocks library, called NPLIB. Enforcing the use of this library by internal engineering staff and by external engineering service providers assures a consistent level of error handling, e.g. signal status based, together with the provision of non-circumventable security controls.

References

[BM16] Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie - IT-Sicherheit für die Industrie 4.0 - Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, 2016.

[IE15] IEC 62443-2-3: Security for industrial automation and control systems – Patch management in the IACS environment, Edition 1.0, 2015.

[IE15a] IEC 62443-2-4: Security for industrial automation and control systems – Security program requirements for IACS service providers, Edition 1.0, 2015.

[IE10] IEC 62443-2-1: Security for industrial automation and control systems – Establishing an industrial automation and control system security program, Edition 1.0 2010.

[IE13] IEC 62443-3-3: Security for industrial automation and control systems – System security requirements and security levels, Edition 1.0, 2013.

[IE15b] IEC 62443-3-2: [Draft] Security for industrial automation and control systems – Security risk assessment and system design, 2015.

[IE15c] IEC 62443-4-2: [Draft] Security for industrial automation and control systems – Technical security requirements for IACS components, 2015.

[IE13] IEC 62443-1-3: Industrial communication networks - Network and system security - System security compliance metrics, 2013.

[WSG10] Wang, J; Stavrou, A; Ghosh, A.: HyperCheck: A Hardware-Assisted Integrity Monitor, 2010.

[ACM15] Sadeghi, A.; Wachsmann; C.; Waidner, M.: Security and Privacy Challenges in Industrial Internet of Things, 2015.

[DREP14] Hadžiosmanovic, D.; Sommer; R.; Zambon, E.; H.Hartel, P.: Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes, 2014.

[SN13] SIMATIC NET - DMZ with the SCALANCE S623, 2013.

[SCO1] SCOOP, http://www.seclab-solutions.com/use-cases/prevent-data-leakage, 2016.

[II14] ISO/IEC 27036-1: Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts, 2014.

[MM94] I.Moon: Modeling programmable logic controllers for logic verification, 1994

[MS13] Mulder, J.; Schwartz, M.; Berg, M.; Van Houten, J.; Urrea, J.; King, M.; Clements, A.; Jacob; J.: WeaselBoard: Zero-Day Exploit Detection for Programmable Logic Controllers, SANDIA REPORT, 2013

[SP12] SIMATIC, Process Control System PCS 7, Security concept PCS 7 & WinCC (Basic), Function Manual, 2012.

[TS12] Tyson, M; Singer, B; Cybersecurity for Industrial Control Systems SCADA, DCS, PLC, HMI, and SIS, CRC Press, USA, 2012.

[LR12] Langner, R; Robust Control System Networks: How to Achieve Reliable Control After Stuxnet, Momentum Press, 2012.