SECURITY MATTERS

Gartner 2014 Cool Vendor

How to Design and Maintain a Secure ICS Network

Support IEC 62443 Compliance with SilentDefense

Authors
Daniel Trivellato, PhD - Product Manager Industrial Line
Dennis Murphy, MSc - Senior ICS Security Engineer

16 June 2015

SECURITY MATTERS

Gartner 2014 CoolVendor

Contents

1 Preface 2

2 The IEC 62443 Standards 3

2.1 Standards Overview and Implementation Steps 3

2.2 Limitations of the IEC 62443 Standards 5

3 Building a more secure network with SilentDefense 6

3.1 Traffic flows and asset discovery 6

3.2 Network segmentation and threat detection 8

4 Conclusions 10

4.1 About SecurityMatters 10

4.2 About the Authors 10

1 Preface

Industrial network operators are subject to a constant demand from management to increase productivity and reduce costs. To achieve these goals and accommodate management demands, operators are shifting towards the use of standard communication technologies and commercial-off-the-shelf (COTS) equipment, and are opening up links between industrial and enterprise networks to enable sharing of process information in real time across multiple industrial and enterprise systems for analytical purposes. In spite of the clear business advantages, this paradigm shift has considerably reduced the resilience of industrial networks, opening the door to a new class of threats: cyberattacks directed against industrial control systems (ICS).

To limit the exposure of industrial networks to this new and actual threat, a group of network security and industrial automation domain experts have worked to establish the ANSI/ISA-99 family of standards, which is now known as IEC 62443 [1]. These standards provide a framework to help control system vendors, system integrators and operators deal with the security threats that arise from the "push for productivity" initiatives and the resulting openness towards enterprise and third-party systems, and also to ward off the specter of Stuxnet-like malware attacks.

This whitepaper briefly reviews the IEC 62443 standards, discusses their limitations, and illustrates how SilentDefense helps to overcome them, thereby supporting industrial network operators to comply with these standards and improve the security of industrial networks.

2 The IEC 62443 Standards

The IEC 62443 family of standards is a flexible framework designed to facilitate the mitigation of current and future vulnerabilities in industrial control systems and networks, by applying necessary security controls and best practices. The standards define requirements at different technical and organizational levels, in order for organizations to achieve an adequate cybersecurity posture. The figure below provides an overview of the IEC 62443 standards.

2.1 Standards Overview and Implementation Steps

In this whitepaper we focus exclusively on the technical standards of the IEC 62443 family, which are those targeting the network and its components (the lower levels of Figure 2.1, labeled as "System" and "Component"). The following is a short overview of the content of those standards:

- The **IEC 62443-3-1** standard provides an introductory description to all existing technologies for protecting industrial networks and systems (e.g., network- and host-based solutions, etc.), their advantages and limitations.
- The **IEC 62443-3-2** standard describes how organizations should segment their network into zones and conduits, grouping systems which are similar in functionality, purpose and/or location, and conduct risk analysis and definition of security requirements per zone. A target security level (in a 1-to-4 scale) is assigned to each zone. The focus of this standard is on zone-based risk management, and at this stage network segmentation is to be done only on paper; the actual segmentation of the network is discussed in the IEC 62443-4-2 standard.
- The **IEC 62443-3-3** standard describes general system security requirements in terms of identification and authentication, data confidentiality, and system integrity, specifying how these requirements differ for ICS networks with respect to IT networks. In particular, the standard stresses the fact that performance and availability should not be affected in the attempt to accommodate these requirements.
- The **IEC 62443-4-1** standard defines a development process that aims at reducing the number of security vulnerabilities in industrial control systems. The standard

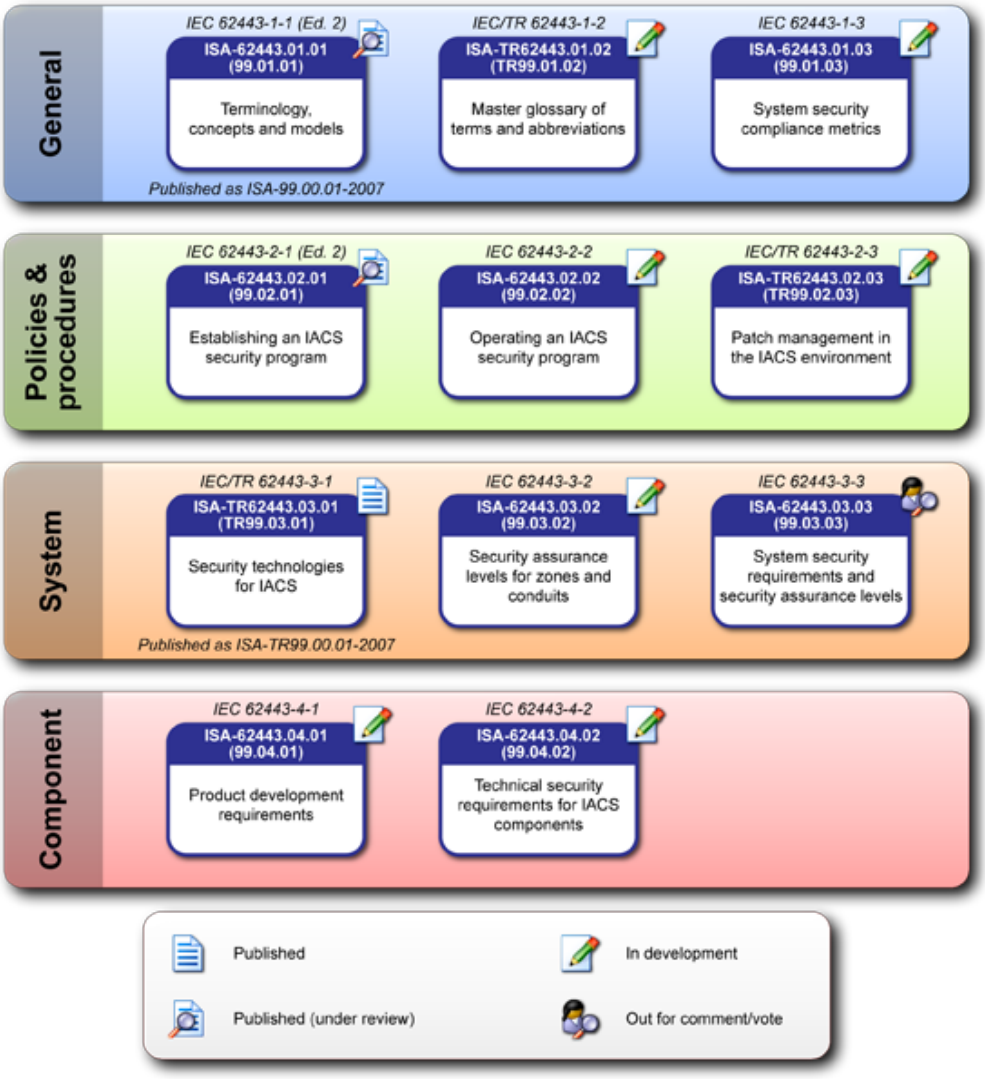

Figure 2.1: Overview of the IEC 62443 family of standards (www.isa99.org)

defines a number of techniques and processes based on best practices for secure design.

- The **IEC 62443-4-2** standard defines the technical requirements for securing the individual components of an industrial network. These requirements are based on the system level security requirements specified in IEC 62443-3-3; security goals focus on system availability, plant protection, plant operations, and time-critical system response. Furthermore, the standard discusses the enforcement of data flow restrictions to achieve proper network segmentation. In particular, it treats application partitioning, security function isolation, and boundary protection.

Based on the IEC 62443 framework, we can identify four incremental steps that operators should follow - with the support of qualified third parties - to design and maintain more secure and resilient industrial networks.

1. **Data gathering**: the first step consists of gathering all information required to understand how the network is built and the process operates;
2. **Security assessment**: the second step leverages the information gathered in step 1 to determine the current security posture of the industrial network, ascertain its exposure to cyberthreats, and identify appropriate countermeasures;

3. **Solution build**: based on the criticalities and priorities identified in step 2, operators apply the required changes to the network, and prepare it for the implementation of selected countermeasures;

4. **Solution deployment**: finally, selected countermeasures will be deployed and integrated into the day-to-day operations to preserve network and process security.

Figure 2.2 illustrates the four steps along with the main activities involved in each step.

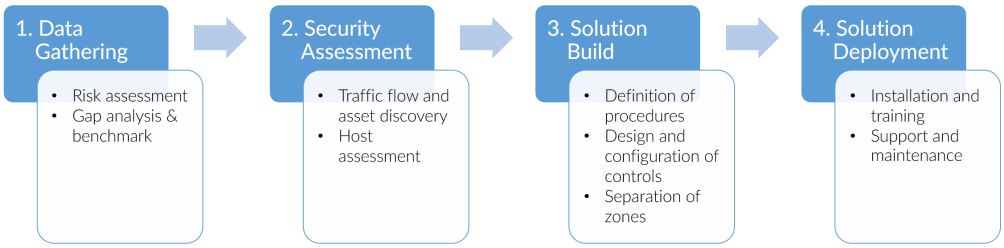

Figure 2.2: Four steps to implement the IEC 62443 standards

2.2 Limitations of the IEC 62443 Standards

The security and resiliency of the industrial network resulting from the implementation of the IEC 62443 standards are strictly dependent on the completeness and accuracy with which the activities within steps 1 and 2 in Figure 2.2 are carried out. In fact, only comprehensive and accurate data gathering and security assessment steps will result in the selection and successful implementation of adequate countermeasures.

Those activities, however, are typically carried out manually, or with the help of inadequate tools not designed for that specific purpose. As a consequence, the process is lengthy, error prone, and often incomplete, because it is difficult to characterize all relevant aspects without the support of an automated toolset.

In the next paragraphs we present how the network monitoring and intelligence platform SilentDefense can support operators to carry out some of those activities in a much more precise and complete way.

3 Building a more secure network with SilentDefense

SilentDefense is specifically designed to provide the missing visibility into industrial networks and processes. SilentDefense listens, analyzes, and automatically models the behavior of the network, presenting the operator with all the information needed to understand how the network is actually built and operates, and identify the weaknesses or possible trouble spots. It does all of this in a completely passive manner, to provide the most accurate picture possible of the network behavior with minimal effort, and without risk of introducing latency or affecting the performance of systems and process.

SilentDefense offers the ideal support in different steps of the implementation of the IEC 62443 standards. In particular, it:

- Enables an instant and accurate determination of the **traffic flows and active network devices**;
- Supports the enforcement of **network segmentation** into zones and conduits, guaranteeing that no undesired communication or information flow occurs;
- And provides the best possible day-to-day protection of the network; thanks to the most **advanced threat detection** engine currently available, you can detect new and yet unknown cyberattacks as easily as every day's threats to the network.

We will next illustrate the contributions of SilentDefense more in details.

3.1 Traffic flows and asset discovery

Operators can build an exhaustive asset and process inventory, determining information flows, protocols used and operations performed by each individual discreet network device by exploiting SilentDefense's powerful, self-configuring analysis engine and advanced visual analytics platform. The result is an instant, clear and accurate picture of the network, which facilitates the operator's understanding of the underlying process and identifies possible weaknesses and security breaches, from sources like using insecure protocols and services to the excessive use of the industrial network bandwidth. In addition, all of this

information is captured using a passive network mirror port without reconfiguring the ICS network or actively scanning the network.

The network picture is provided by a set of visual widgets, each of which is ideally designed to highlight certain aspects of the network's behavior. For example:

- Time series show the evolution of network/protocol communications over time;
- Pie charts put in proportion different aspects of the communications – like the most used protocols - to determine the structure of the network;
- Chord diagrams show in detail all the communication patterns observed in the network, and help identifying undesired information flows;
- Table elements list the network assets and their characteristics, or document undesired events in a given time interval.

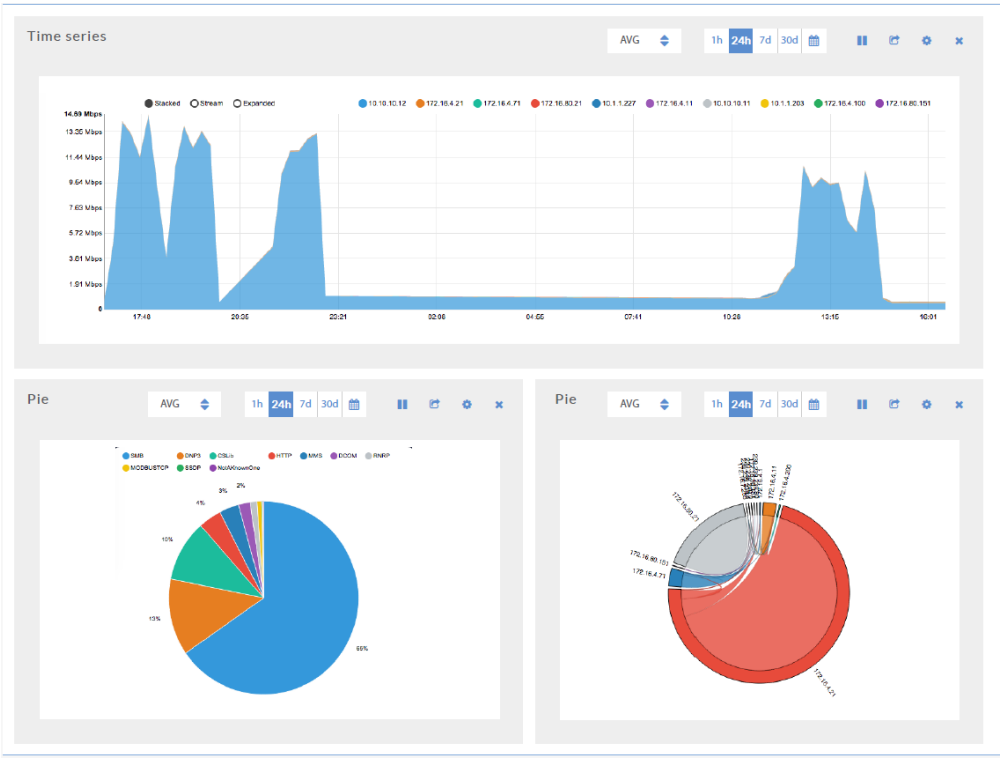

Figure 3.1: Some of the views enabled by the SilentDefense visual analytics platform

All graphs and analytics screens are fully customizable and may be used to represent multiple aspects of a communication flow, for instance the number of exchanged bytes or protocol messages. The information displayed can be filtered and cross-filtered with respect to different dimensions. The graphs provide a real-time view into the network, but can also be used to dig into the past and analyze network communications in relation to events. In fact, behind the visual analytics platform there is a full-featured data warehouse that allows operators to combine all their query preferences with historical data, giving them all the power they need to deeply analyze the behavior of the industrial network.

Besides the graphical representation provided by the visual analytics, SilentDefense also offers a detailed view of the information flows within the network in the form of "firewall-like" rules, which are automatically generated by a dedicated analysis engine. Each rule indicates which hosts have been observed communicating, over which port, using which protocols, and running which operations/commands over those protocols. This information is key to identify the presence of undesired information flows, insecure services run by the network devices, or undesired process operations.

The output of this analysis can be used to determine the security status of the network, clean up existing misconfigurations, and instruct firewalls to stop specific undesired

Source	Port	Dest	Port	Protocol	Operation
DCS	*	PLC_1	502	Modbus/TCP	Read Multiple Registers, Write Multiple Registers
DCS	*	PLC_2	502	Modbus/TCP	Read Multiple Registers
DCS	*	HMI	*	DCOM	SMB_COM_CREATE, SMB_COM_DELETE, ...
...	...	...	...	...	...

Figure 3.2: Network information flows, protocols and commands identified by SilentDefense

information flows. Furthermore, it includes all the required input to support the definition of network "zones" and "conduits", as recommended by IEC 62443. In other words, it is the big first step towards the design and implementation of a secure network.

3.2 Network segmentation and threat detection

But SilentDefense is not only a great platform to support network assessments; it can be also used to guarantee that the security posture is always preserved. In fact, the rules automatically generated by SilentDefense can be enforced to guarantee that whenever communications diverge from the intended network behavior, the operator is immediately alerted. For example, SilentDefense will alert in real-time in case a new, previously unseen host starts communicating in the network, or an undesired protocol or service is used (see Figure 3.3). In other words, SilentDefense will report any violation of the network segmentation determined in the "solution build" step (step 3 of the IEC 62443 framework implementation).

Summary

Alert ID	74
Timestamp	Oct 21, 2016 12:28:38
Sensor name	Demo sensor
Detection engine	LAN CP
Profile	7 Boiler network
Severity	Medium
Source MAC	08:00:27:9E:12:97 (CadmusCo)
Destination MAC	08:00:27:55:62:F7 (CadmusCo)
Source IP	192.168.56.102
Destination IP	192.168.56.10
Source port	49158
Destination port	502
L2 proto	Ethernet
L3 proto	IP
L4 proto	TCP
L7 proto	MODBUSTCP
TCP stream opened in hot start mode	false
Status	Not analyzed

Figure 3.3: Alert generated by SilentDefense when two unknown hosts appear in the network

Further to this fine-grained control over information flows, SilentDefense features the most advanced detection engine to analyze communications over industrial protocols. SilentDefense uses a learning mode to automatically generate a model of messages being actively used by the control network. Using Deep Protocol Behavioral Inspection, a tree-based model is generated and stored to allow for automatic real-time analysis of ICS communications. Figure 3.4 below is an example of a tree model that was auto-generated by SilentDefense while monitoring some Modbus/TCP communications.

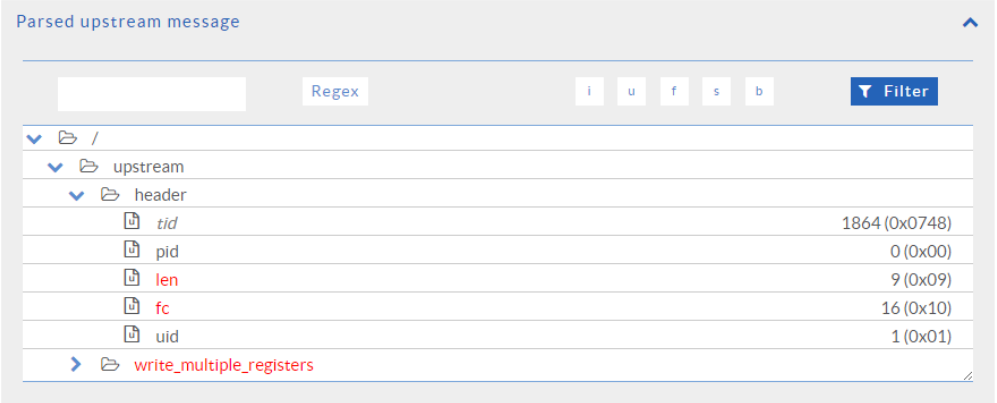

Figure 3.4: SilentDefense reports the use of unauthorized operations and suspicious values

The result is that SilentDefense is capable of analyzing every single field and value contained in an industrial protocol message, to ensure that the message is not only compliant with the protocol specifications, but also with the intended operations and value ranges specifically used in the monitored network. As soon as an outsider or disgruntled insider tries to exploit a vulnerability in network devices, SilentDefense will detect it and report it. This goes beyond the capabilities of other existing network monitoring systems, which stop their analysis at the protocol 11command" level. Therefore, SilentDefense offers protection from a more comprehensive set of cyberthreats, from the simplest to the most advanced ones.

4 Conclusions

SilentDefense is the ideal platform to gain and maintain all the required visibility of industrial network activities, at any time. It empowers operators to achieve the gain in productivity requested by the management without losing sight of the security of the network, as advocated by the IEC 62443 standards.

SilentDefense brings value that goes well beyond that of traditional cybersecurity solutions. It identifies and reports operations and networking issues that can have the same devastating effects of a cyberattack. All in all, it is the most comprehensive and powerful platform for monitoring industrial networks and industrial control systems.

4.1 About SecurityMatters

SecurityMatters is an international company with business in all major critical infrastructure and industrial automation sectors. Its network monitoring and intelligence platform SilentDefense has been deployed for years at customers across multiple continents, providing daily value to operations and protecting their networks from emerging cyberthreats.

4.2 About the Authors

Daniel Trivellato Daniel Trivellato received his PhD in computer security from the Eindhoven University of Technology in 2012. During his PhD, he worked in collaboration with Thales Netherlands on the design and implementation of an access control framework for protecting confidential data in dynamic distributed systems. In 2012, Daniel joined SecurityMatters as a project leader; his responsibilities encompassed marketing and sales, account management, and the organization and management of deployment projects at customers. Since 2014, Daniel is product manager for SecurityMatters' Industrial Products portfolio, and is responsible for the evolution and commercialization of the line of products targeting the industrial control systems domain.

Dennis Murphy Dennis Murphy is a Sr. Cybersecurity Engineer at Security Matters. He has 12 years of experience in SCADA and ICS design, development and implementation and 10 years of experience in computer security as it applies to critical infrastructure networks. Mr. Murphy directed multiple SCADA security tests at Idaho National Labs Critical Infrastructure Test Range while he was a program manager at BAE Systems in their cybersecurity division in Merrimack, NH. During his tenure at a Wonderware distributer in New England, he designed, installed and supported dozens of different SCADA systems in the Electric Power, Water, Biopharmaceutical, Oil & Gas, Chemical, Food & Beverage and Pulp & Paper industries. He has a masters degree in Systems Engineering from Johns Hopkins University. He is a member of the Boston, MA chapter of the FBI's infragard program and he is a member of the Control System Integrator Association's Cybersecurity Best Practices Working Group.

Bibliography

[1] International Society of Automation (ISA). Isa 99/iec 62443: Industrial automation and control systems security. https://www.isa.org/isa99/.