WHITE PAPER

Addressing the Implementation Conflicts of Cybersecurity Management Systems in IT/OT Environments

Adelina-Elena Voicu

Secura
A BUREAU VERITAS COMPANY

Table of Contents

1. Introduction **3**

2. Background **4**

2.1 ISA/IEC 624432 augments ISO/IEC 27001/2 4

2.2 Conflicts may arise when extending IT security implementations to OT 4

3. Conflicts explained **5**

3.1 Example 1: 7.7 Clear desk and clear screen 5

3.2 Example 2: 8.5 Secure authentication 5

3.3 Example 3: 5.17 Authentication information 6

4. The solution – OT Security Maturity Review Extended **7**

5. Conclusion **8**

6. References **8**

1. Introduction

With industrial environments becoming more connected and dependent on cloud-based solutions, real-time information sharing and constant monitoring, the threat landscape is constantly changing and evolving. As IT and OT solutions converge, IT implementations are extended to OT environments, IIoT solutions are used more and more, the boundaries between IT and OT are blurring. Therefore, it becomes more important that companies often have a good overview of the maturity of their information systems and the cyber resilience within their entire organization, both IT and OT.

The goal of this whitepaper is to provide some examples of conflicts which may arise when extending IT implementations to OT environments. The following standards are discussed because of their applicability to IT and OT environments:

- ISA/IEC 62443-2-1:2010 – Industrial communication networks – Network and system security –- Part 2-1: Establishing an industrial automation and control system security program [1]
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems – Requirements [2]
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls [3]

2. Background

2.1 ISA/IEC 624432 AUGMENTS ISO/IEC 27001/2

ISA/IEC 62443-2-1 belongs to the second part of the IEC 62443 family of standards, Policies and procedures and focuses on establishing an industrial automation and control system security program. This part of IEC 62443 series includes requirements addressing specific needs in the OT environment and complements the list of controls of ISO/IEC 27001/2 by adding critical details relevant to that environment [4]. It provide the requirements to implement a Cyber Security Management Systems (CSMS), which could be considered the OT equivalent of the ISMS.

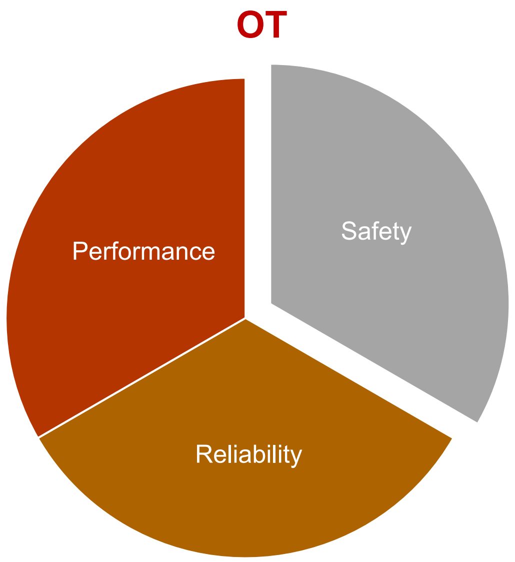
ISO/IEC 27001 provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) as well as a list of commonly accepted controls to be used as a reference for establishing security requirements. ISO/IEC 27002 serves as a starting point in determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001.

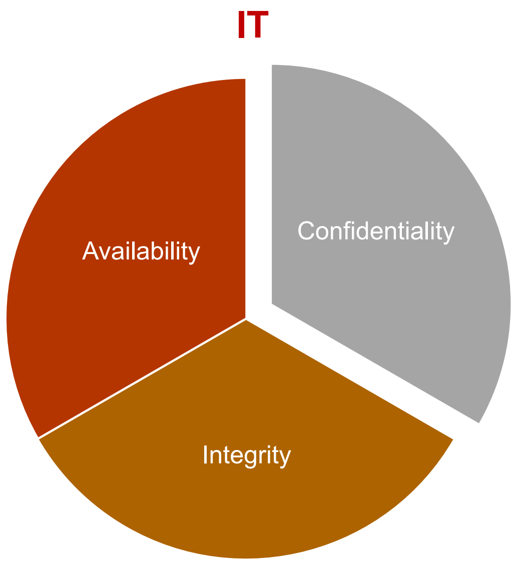
Both ISO/IEC 27001/2 provide controls, respectively guidance on how to implement the controls with a focus on IT, but can still be applicable to OT environments. Consequently, ISO/IEC 27001/2 contain IT-oriented controls that are not found in ISA/IEC 62443-2-1.

2.2 CONFLICTS MAY ARISE WHEN EXTENDING IT SECURITY IMPLEMENTATIONS TO OT

The focus in OT environments lies on safety, reliability and performance. Loss of operational continuity, environmental damage, may create unsafe conditions, such as an explosion, a fire, a chemical leak, a power outage or incorrect medication dosage. In IT, on the other hand, the focus lies on confidentiality, integrity and availability, as depicted below.

Attempting to ensure a robust approach to cyber security in an environment containing both IT and OT infrastructure entails considering controls in both ISA/IEC 62443-2-1 and ISO/IEC 27001/2. Consequently, extending IT security implementations to OT environments should take into account potential conflicts.





3. Conflicts explained

Conducting a coordinated approach to ensure cyber resilience in OT environments should be done with caution. When identifying controls in ISO/IEC 27001/2 which cannot be mapped to requirements in ISA/IEC 62443-2-1, areas of potential conflicts should be addressed, such that the extended implementation does not generate conflicts.

All three examples presented in this whitepaper were discovered while attempting to combine the controls in ISO/IEC 27001/2 and the requirements in ISA/IEC 62443-2-1, as referenced in the whitepaper “Combined approach to Information Security based on ISO/IEC 27001/2 and ISA/IEC 62443-2-1”.

3.1 EXAMPLE 1: 7.7 CLEAR DESK AND CLEAR SCREEN

The first example concerns the control **7.7 Clear desk and clear screen in ISO/IEC 27001**. The control states that “Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.” Additional guidance on how to implement the control is provided in ISO/IEC 27002.

Specifically, guidance points c) *(“leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature; “)* and f) *(“establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);”)* can introduce potential conflicts when extended to OT environments.

Screen savers with password protection may create unsafe conditions as they can potentially prevent operation or delay the response in an emergency situation. When addressing this conflict, Secura recommends prioritizing safety over security. A distinction shall, thus, be made between user screens and operator screens and controls should be applied on a case-by-case basis. User screens should be locked upon request or after a configured period, whereas operator screens should or may remain unlocked.

3.2 EXAMPLE 2: 8.5 SECURE AUTHENTICATION

A second example concerns the control **8.5 Secure authentication in ISO/IEC 27001**. The control reads: “Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.” Additional guidance on how to implement the control is provided in ISO/IEC 27002.

Guidance points e) *(“protecting against brute force log-on attempts on usernames and passwords [e.g. using completely automated public Turing test to tell computers and humans apart (CAPTCHA), requiring password reset after a predefined number of failed attempts or blocking the user after a maximum number of errors];“)*, *g) (“raising a security event if a potential attempted or successful breach of log-on controls is detected (e.g. sending an alert to the user and the organization’s system administrators when a certain number of wrong password attempts has been reached);“)*, *l) (“restricting connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.”)* can conflict with **section A.3.3.6.5.2 Authentication for local users** in ISA/IEC 62443-2-1.

Specifically, subpoints c) *(“Automatic access account lockout after some number of failed login attempts”)* and e) *(“Password changes after a specified number of days”)* introduce examples of situations when password protection practices may slow the response to situations when quick responses are needed. In these situations, safe operation of the IACS shall again be a priority. As such, instead of implementing the control for all accounts, Secura recommends conducting a risk assessment to identify any accounts that need to be exempted from the locking due to a failure to log in and password lifetime policies.

3.3 EXAMPLE 3: 5.17 AUTHENTICATION INFORMATION

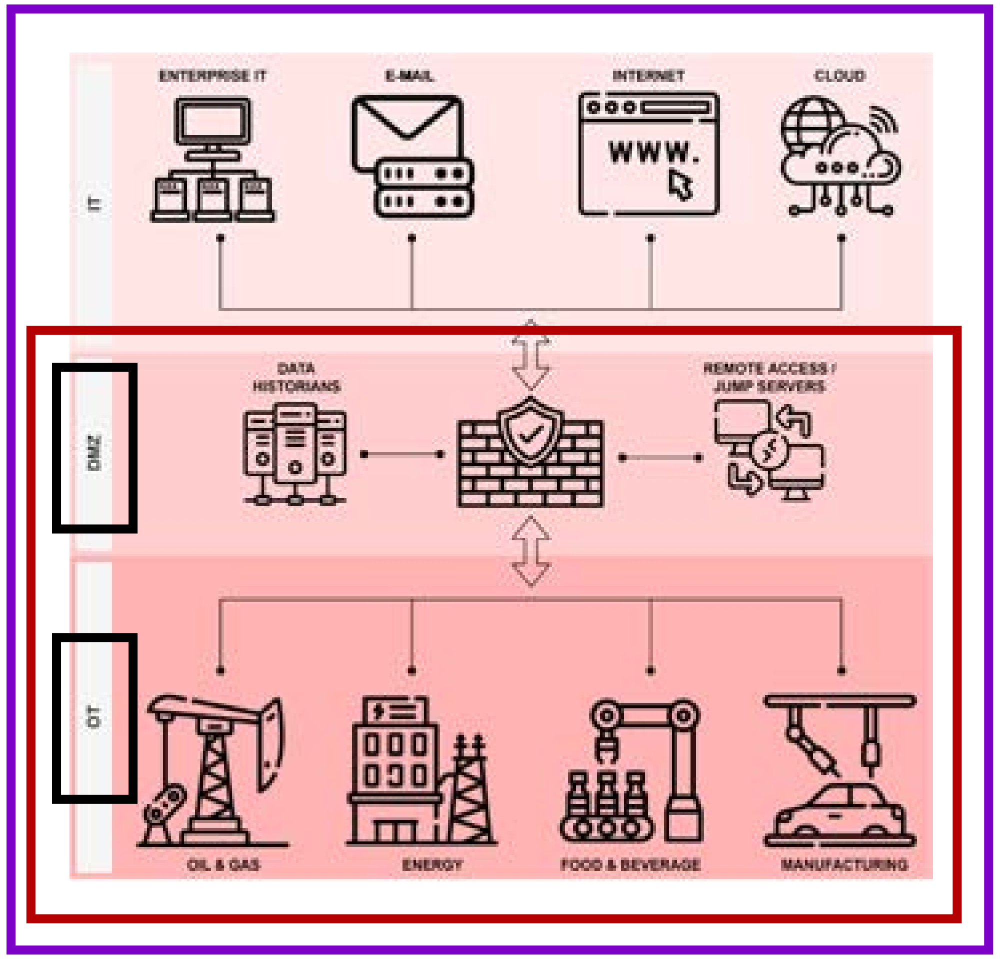
The last example is based on the control **5.17 Authentication information in ISO/IEC 27001**. The control requires that: “Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information. Additional guidance on how to implement the control is provided in ISO/IEC 27002.

Guidance points c) *(“when passwords are used as authentication information, strong passwords according to best practice recommendations are selected, for example: 1. passwords are not based on anything somebody else can easily guess or obtain using person-related information (e.g. names, telephone numbers and dates of birth); 2. passwords are not based on dictionary words or combinations thereof; 3. use easy to remember passphrases and try to include alphanumerical and special characters; 4. passwords have a minimum length;”)* and d) *(“the same passwords are not used across distinct services and systems;”)* can conflict with section **A.3.3.6.5.3 Authentication for local users** in ISA/IEC 62443-2-1.

Subpoint “a) Individual user IDs and passwords for each operator for work-team environments” illustrates an example of situation in which imposing individual user IDs and passwords may compromise quick response time. Once again, Secura recommend prioritizing safety over security. An assessment shall be conducted to determine when implementing individual user IDs and passwords is feasible. In situations when shared passwords are needed, for instance for maintenance and operator accounts, compensating countermeasures shall be implemented to allow for safe operation of the IACS.

4. The solution – OT Security Maturity Assessment

Secura defined two approaches to measure the OT cybersecurity maturity entitled Security Maturity Review & Assessment. The approaches are applicable for asset owners and cover the establishment and implementation of a management system. This could be based on either ISA/IEC 62443- 2-1 or ISO/IEC 27001/2. The third approach, is the focus of this whitepaper and is built on a combination of both standards.



-> ISO 27001/2

-> IEC 62443-2-1

The goal of the Security Maturity Reviews & Assessments is to provide insight into the maturity of the cybersecurity organization. Secura assesses the effectiveness of the (implemented) security policies and the security program and measures, identifies deviations and vulnerabilities and provides a clear report and advice for follow up. The outcome of this service is clear insight into the current maturity scoring and an indication of which control improvements help most raising the current maturity level to the desired level. These measures are formulated high level, with aim to report the most important to involved Senior Management. Recommendations are prioritized based on the risk profile and the maturity scoring.

5. Conclusion

It is expected that the prevailing trend towards IT/OT integration and convergence will continue in the coming years. This will be primarily driven by business and operational benefits. Since the end goal will remain the same, achieving **safe**, reliable, and cost-effective production, it will become imperative to reassess the way organizations approach the implementation of a cyber security management system in OT environments.

6. References

[1] IEC. 2010. IEC 62443-2-1. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. 1st ed. ISBN 978-2-88912-037-6. Accessed on [09.05.2022]

[2] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. 3rd ed. Accessed on [10.05.2022]

[3] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems – Requirements. 3rd ed. Accessed on [12.12.2022]

[4] ISA. Whitepaper. July 2021. Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments, p.6. Accessed on [14.04.2022]

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

About Secura

Secura has worked in information security and privacy for over two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organizations with up-to-date knowledge to work toward a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Follow us on:

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
1828
Shaping a World of Trust