Implementation of Zones and Conduits in Industrial Control and Automation Systems

Lars Halvdan Flå, Mary Ann Lundteigen, Fredrik Gratte, and Martin Gilje Jaatun

Abstract Despite being established concepts in standards we argue that zones and particularly conduits can benefit from more detailed discussions of their architecture and implementation. In this paper we make three contributions towards this. Firstly, we describe detailed principles for implementing conduits. Secondly, we outline a process for connecting zones with potentially different Security Levels (SLs), expressed in the form of a flow chart. Thirdly, we discuss a few highlighted challenges related to the application of zones and conduits in practice.

Key words: cybersecurity, industrial control systems, IEC 62443

1 Introduction

The IEC 62443 standards series describes cybersecurity of industrial automation and control systems (IACS), and based on our earlier survey [14], the IEC 62443 standard is the only quantifiable approach currently in use for determining and validating SLs in IACS.

Lars Halvdan Flå
SINTEF Digital, Trondheim, Norway e-mail: lars.flaa@sintef.no

Mary Ann Lundteigen
Department of Engineering Cybernetics, Norwegian University of Science and Technology, Trondheim, Norway
e-mail: mary.a.lundteigen@ntnu.no

Fredrik Gratte
Atina e-mail: fredrik.gratte@atina.no

Martin Gilje Jaatun
SINTEF Digital, Trondheim, Norway e-mail: martin.g.jaatun@sintef.no

Two key concepts introduced by IEC 62443 are zones and conduits. Establishing zones and conduits, i.e., grouping assets based on their security requirements, is a key activity when securing industrial control systems in accordance with IEC 62443. However, the details surrounding the architecture of these concepts seem to have received less attention than one could imagine, given how established these concepts are. This holds particularly true in the case of conduits.

Inspired by interactions with the industry, the overall objective of this paper is to highlight challenges in using the zones and conduits paradigm. Furthermore, we aim to sketch a practical approach to defining the architecture of zones and conduits. More specifically, in this article we:

1. suggest principles for zone and conduit architecture
2. suggest principles for connecting zones with different SLs
3. highlight challenges with using zones and conduits in practice

The remainder of this article is structured as follows: Section 2 presents related work. Section 3 presents relevant concepts from the IEC 62443 standard. Section 4 describes proposed architectural principles for implementing conduits. Section 5 presents a process for the secure connection of zones with different SLs. Section 6 discusses practical challenges of implementing zones and conduits in practice. Section 7 describes further work, while Section 8 concludes the paper.

2 Related Work

Arguably the contribution that has had the most influence on IACS architecture for cybersecurity is the Purdue model. This model originated from Purdue University in the 1990s, and despite not being created with cybersecurity in mind, it has seen wide adoption within cybersecurity for industrial control systems. The model assigns systems and components into vertical layers. In some cases, it also indicates how vertical layers can be further horizontally segmented, but this is often limited to instances where one enterprise has several factories or plants (see for instance figure 18 in IEC 62443-1-1:2009 [5]).

In addition to the Purdue model, there are also several whitepapers and product supplier reference guides for IACS cybersecurity design. An example of a product supplier reference guide is the Industrial Automation Security Design Guide 2.0 from Cisco, which has a chapter on segmenting the network into smaller trust zones [1]. This document (which refers to the IEC 62443 standard) defines a zone as "a collection of physical and functionally united assets that have similar security requirements". In addition to zone characteristics already known from IEC 62443, they additionally specify that the border is used to define access with another zone or outside system. A conduit is described as something that supports and defines allowed communication between two or more zones, with attributes that define which zones are interconnected by the conduit, type of data flow allowed, and security policies and procedures. With regards to the segmentation of OT networks, the document argues that area zones provide a good starting point. After visibility into plant operations has been obtained, the initial segmentation can later be extended by further segmentation within Virtual Local Area Network (VLAN) segments. Another interesting aspect of segmentation raised in the document is the potential complexity. While discussing a particular security measure, they give an example of a situation where one must consider 400 area zones. We discuss this further in section 6.

Combining zones and conduits within a Purdue reference architecture may be regarded as a defence in depth strategy. For example, DesRuisseaux [3] argues that proper defence in depth involves six steps. Step two involves separating networks by major function, and as example lists that a network can be divided into enterprise, plant, process, and field zones. Subsequently, all conduits between zones should be identified. In step three, named perimeter protection, these conduits should be protected. In step four, named network segmentation, existing zones can be divided into smaller zones. This division can be based on location or function.

Leander et al. [10] discuss the applicability of IEC 62443 in light of the expected transition to Industry 4.0 and increased use of Industrial Internet of Things (IIoT) devices. Specifically, regarding IEC 62443 zones, they argue that this concept may be challenged by IIoT devices relying on for instance cloud access and by the dynamic nature of Software Defined Networking.

Most requirements and discussions are made common for zones and conduits, without clarifying how the two types of segmentation are treated differently in practice. One exception is the European technical specification CLC/TS 50701 [2] that has an annex (A) dedicated to handling conduits. Here it is suggested that there are only three types of conduits:

1. Conduits implementing a transparent (i.e., logical) gateway connecting zones of the same SL.
2. Filtering conduits as firewall appliance, allowing a zone of lower or equal security to communicate with a zone of a higher SL.
3. Unidirectional conduit as a data diode or network tap, allowing output from a higher SL zone to others.

Here, the conduits may relate to logical functions implemented with the network devices and not necessarily the hardware involved. The technical specification comments that IEC 62443 does not clearly advice on whether network devices should be part of zones or conduits, and an interpretation is that a network device acting as a boundary protection of a zone can belong to the zone as well as the conduit.

Soderi et al. [12] have interpreted the practical application of CLC/TS 50701 when the conduit is a wireless communication within a train control system. Here, they assume that the connected zones have the same SL, meaning that a transparent gateway is the preferred type of conduit. In a wireless communication, additional measures are needed to achieve transparency when exposed to cyber attacks. Their solution is to use a host identify protocol (HIP) that provides transparency with end-to-end encryption, mutual authentication, and internet protocol security.

Kern et al. [11] have modelled and made an UML like visualization of an architecture of zones, data flows, and their related attributes and functions, following the basic requirements in IEC 62443. In their work, they consider conduits as the means of transporting data flows and they argue that the SL assigned to network components is determined by the highest SL assigned to the data flow that runs through them. The target SL of a zone is determined by the highest SL of the network components within that zone.

Schlehuber et al. [13] propose an application layer gateway (ALG) to tackle the challenge when conduits are connecting zones with different SL requirements. An ALG can be configured to allow the desired type of connection (or layer) to connect specific zones. The configuration may include whitelist filtering for each of the implemented layers. The ALG is also envisioned to be able to forward traffic to a Security Operations Centre for analysis. This solution of including an ALG implies that the same conduit can be used to provide different levels of security, depending on the direction of the data flow.

3 IEC 62443 and its Application

The IEC 62443 standard takes a holistic view on the cybersecurity of IACS, covering the technical, procedural and people aspects, for the different roles involved in the supply chain. These roles include the product supplier, service provider, and asset owner. The standard has been in development since 2009, and an overview of its different parts can be seen in Table 1. We now proceed to introduce a few selected concepts from the standard.

3.1 Application of Zones

IEC 62443 has introduced *zones* and *conduits* as means to group assets in a network architecture that share common security requirements. Unfortunately, IEC 62443 does not limit itself to only one definition of the term zone, and variants have been introduced with new parts of the standard being published, as shown in Table 2. A conduit is a special case of a zone, where the primary role is to group assets that play a role in connecting two or more zones.

Table 1 The IEC 62443 Series

Number	Name	Year	Status
62443-1-1	Terminology, concepts, and models	2009	Published (newer draft exists)
62443-1-3	System security compliance metrics	2021	Draft
62443-2-1	Establishing an industrial automation and control systems security program	2010	Published (newer draft exists)
62443-2-2	IACS security program ratings	2022	Draft
62443-2-3	Patch management in the IACS environment	2015	Published (newer draft exists)
62443-2-4	Security program requirements for IACS service providers	2019	Published
62443-3-1	Security technologies for industrial automation and control systems	2009	Published
62443-3-2	Security risk assessment for system design	2020	Published
62443-3-3	System security requirements and security levels	2019	Published
62443-4-1	Secure product development lifecycle requirements	2018	Published
62443-4-2	Technical security requirements for IACS components	2019	Published

Many industries apply a layered network architecture similar to the Purdue model, and IEC 62443 may have, for this reason, adopted this model as a reference architecture. The Purdue model splits a plant's network and systems hierarchically into 5-6 layers, with a clear separation of the operational technology (OT) side for plant operation, monitoring, data acquisition; and the IT side with the office networks and externally connected cloud solutions and applications. Each layer groups networks and assets that share common operational functions.

The cyber-risk assessment determines to what extent zones have similar boundaries as the Purdue model layers. For example, layer 2 with human machine interface may end up with the same security requirements, while layer 1 may decide on stricter security requirements for safety controllers compared to process controllers. Plants with a large outreach and many distributed systems, may group assets that belong to more than one layer into the same zone. A specific zone can therefore include some or all assets within a layer, or alternatively include assets in several layers.

Table 2 IEC 62443 definitions of a zone

Standard	Definition
62443-1-1 (2009)	Zone: grouping of logical or physical assets that share common security requirements. NOTE: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within a zone. Zones can be hierarchical in the sense that they can be comprised or a collection of sub-zones.
62443-3-2 (2020)	Zone: grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization. NOTE: Collection of logical or physical assets that represents partitioning of a system under consideration on the basis of their common security requirements, criticality (for example, high financial, health, safety, or environmental impact), functionality, logical or physical (including location) relationship.
62443-3-3 (2019) 62443-4-2 (2019)	Zone: grouping of logical or physical assets that share common security requirements. NOTE: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.
62443-4-1 (2018)	Zone: collection of entities that represents partitioning of a System under consideration on the basis [of] their functional, logical and physical (including location) relationship. NOTE: Zones are often created on the basis of common security requirements, criticality (e.g., high financial, health, safety, or environmental impact), functionality, logical or physical (including location) relationship.

3.2 Application of Conduits

A conduit is a ”particular type of security zone” introduced in IEC 62443-1-1:2009 [5]. The term is defined in several parts of the IEC 62443 standards, as listed in Table 3. In summary, we can say that a conduit is a grouping of communication assets or channels. The purpose of a conduit is to secure the communication exchange from one zone to another. However, apart from IEC 62443-1-1:2009 [5], the other parts of the standard do not to any large degree discuss the concept of conduits. Based on part 1-1, a conduit appears to include physical communication assets such as wires, routers, and network management devices. If we assume that the end points of the conduit are also a part of the conduit, the contents widen to also include the physical devices and applications using the channels in the conduit. This view can be supported by the example given of a conduit being the communication channels within a single computer.

Conduits do not appear to be as thoroughly discussed by the standard as is the case for zones. For zones IEC 62443-3-2:2020 [7] has clear requirements on what types of equipment and systems should be placed in separate zones, and IEC 62443-3-3:2019 [6] provides clear requirements for how a zone can achieve the different SLs. Adding to this, the established Purdue model provides a starting point for how the larger network can be segmented into different areas.

Given that a conduit is a special type of zone one can assume that many of the requirements applicable to zones are also applicable to conduits. However, since the standard does introduce the term conduit as a particular type of security zone, we believe more clarification of exactly what constitutes the ”particular” aspect of it could be useful.

Table 3 62443 definitions of a conduit

Standard	**Definition**
62443-1-1 (2009)	Conduit: logical grouping of communication assets that protects the security of the channels it contains. NOTE: This is analogous to the way a physical conduit protects cables from physical damage.
62443-3-2 (2020)	Conduit: a logical grouping of communication channels that share common security requirements connecting two or more zones. [the standard defines a channel as *”specific logical or physical communication link between assets”*, with the associated note *”A channel facilitates the establishment of a connection”*].
62443-3-3 (2019) 62443-4-2 (2019)	Conduit: logical grouping of communication channels, connecting two or more zones, that share common security requirements. NOTE: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

3.3 Application of SLs

In this paper we use the IEC 62443 definitions of SL, and specifically the definitions shown in Table 4. However, the definition of SLs can vary slightly between different sources, and we therefore start our discussion of SLs by referring to some of these definitions. The 62443-3-3:2013 [6] definition of SL is ”measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner”. The 62443-3-2:2020 [7] uses almost the exact same definition, but replaces ”IACS” with ”SuC”. The Global Cybersecurity Alliance [8] uses the same definition, but also include zones and conduits, in addition to SuC.

What further complicates the matter is that Annex A of part 3-2 defines the four SLs as protection against violations from increasingly sophisticated attackers, as shown in Table 4. These definitions, focusing on level of protection, are also in line with Gordon [4] and Kobes [9], who states that "security level values express the security capabilities of the automation solution".

Table 4 SLs as defined in 62443-3-2:2020 [7] Annex A

SL	Description
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple means with low resources, generic skills and low motivation.
3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
4	Protection against intentional violation using sophisticated memes with extended resources, IACS specific skills and high motivation

The IEC 62443 furthermore operates with three types of SL, as shown below. However, for the discussion in this paper, SL-T is the most relevant.

SL-C: Capability Security Level (in product or component)
SL-T: Target Security Level (defined by requirements and specifications)
SL-A: Achieved Security Level (the actual security level achieved "as built")

Determining SL-T is covered by zone and conduit requirement (ZCR) 5.6 [7]. This requirement states that an SL target shall be established for zones and conduits. A corporate risk matrix with tolerable risk is used as input for the requirement. The standard does not detail how the SL shall be established and instead states that there is no "prescribed method for establishing SL-T". It does however describe some potential approaches for determining SL-T, including basing it on the definition of SL, and basing it on unmitigated cyber risk and the organization's tolerable level of risk.

4 Allocation of Assets to Zones and Conduits

In this section, we present architectural principles for establishing conduits and associated zones. The process of creating zones and conduits is defined in ZCR 3 in 62443-3-2:2020 [7]. The overarching principle for dividing an IACS into zones and conduits is the risk assessment. However, we believe it could be beneficial with a more detailed discussion of how to best manage the connection between zones and conduits. As a contribution towards this, we suggest principles for the detailed architecture of determining the structure of zones and conduits. The guiding idea is that:

- A conduit does not implement any connections of its own, it merely transports connections implemented by others.
- All functionality for configuring the conduit is placed in one or more network device configuration zones. However, the conduit itself is not a zone, as it has no configuration interface.

Following this, we assume that a conduit and the associated network device configuration zone(s) have two main responsibilities:

- Protection and containment of zones from each other, by dropping all unintended connections between zones.
- Protection of the availability, integrity and confidentiality of allowed connections between zones.

Based on these principles, we believe that communication assets connecting zones should be split into a data plane, which we consider to be the conduit, and a control plane, which is managed through the different network device configuration zones. As an example, a firewall typically consists of a set of rules applied to incoming traffic, and an interface/application for managing and defining such rules. The rules will be applied to the communication in the data plane, while the changing, adding, and deleting rules will happen through the interface placed in the network device configuration zone.

Another example can be that of a Virtual Private Network (VPN) set up between two routers in different zones. In this example, we believe that the conduit should be the data pipe set up by routing rules along the way between the two zones, and the VPN endpoints providing encryption. The network device configuration zones will include the software used to establish and configure the VPN, along with the configuration interfaces for any network devices between the two zones. In the case of a physical level data diode this will not be part of any network device configuration zone, assuming that it cannot be configured in any way.

We illustrate these concepts in Fig. 1. Zone A and B are both connected to a router, and communicate through a conduit set up by this router (indicated by the green arrow). The router can for instance create this conduit by placing the connections to Zone A and Zone B on a dedicated Virtual Local Area Network (VLAN). The security of the conduit and the connected zones can further be enhanced by applying firewall rules or intrusion detection analysis to the data flowing through the conduit.

The router can implement or be part of several different conduits. For instance if Zone B requires a remote connection, another conduit (indicated by the orange arrow) can be established by creating a new VLAN to facilitate this connection. While the green conduit between zone A and B is primarily

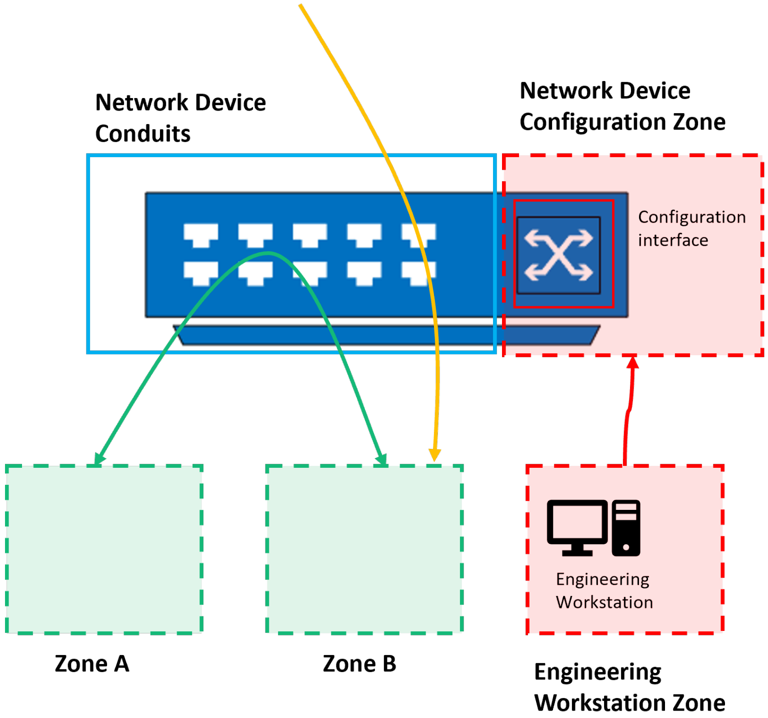

Fig. 1 In the case of a router, the data being transmitted is placed in the conduit, while configuration of the router is placed in the Network Device Configuration Zone.

managed from the router in Fig. 1, the orange conduit may pass through several routers and switches, each with a network device configuration zone.

In Fig. 1, we have placed the router configuration in its own zone, although it can also be part of a larger zone including other devices. The same applies to the engineering workstation used to configure the router. This can either be placed in its own zone or in a larger zone. Furthermore, we argue that two aspects related to this are of particular importance. The first is to harden the network device interface, so that only the minimum required number of engineering workstations can reach and configure it. The second is to ensure that the engineering workstation has minimum the same SL as the network device configuration zone.

Following our suggestion to place all configuration interfaces into network device configuration zones, we believe it only makes sense to assign an SL to these configuration zones. Using these principles the conduit will be reduced to a data pipe which does not have any interface or functionality to secure by itself, since this is moved to dedicated configuration zones.

5 Securing Conduits Connecting Zones with Different SLs

As stated in ZCR 5.6 in IEC 62443-3-2:2020 [7], an SL shall be allocated to zones and conduits. In this section we propose a process for securing a conduit, and the associated network device configuration zones, when the conduit is connecting zones with potentially different SLs. We express the process in the form of a flow chart, and the steps involved in the process are as follows:

1. In the first step, we evaluate if all zones connected by the conduit have the same SL.
2. If all involved zones have the same SL, we assign the same SL to the network device configuration zones, provided that the existing SL of the network device configuration zone is not higher. As many conduits may go through a network device, the SL of the network device configuration zone should be the highest of any zone connected by any of the conduits. Once this step is completed, the process terminates.
3. In the case that the involved zones have different SLs, we assign the highest SL to the network device configuration zones. Similarly as for step 2, we account for the scenario where a previously analysed conduit has resulted in a higher SL for the network device configuration zones.
4. In step 4, we enumerate all data flows or communication channels that are part of the conduit.
5. In step 5, we evaluate whether any of the data flows perform write operations from zones with lower levels of criticality or lower integrity requirement to zones with higher levels of criticality or integrity requirements.
6. If this is the case, one should assess the potential risk if this data flow is compromised by an attacker and, if necessary, implement suitable countermeasures. Examples may include proxy servers limiting what interfaces the zone exposes, or intrusion detection systems flagging suspicious traffic.
7. In the step 7, we check if there are remaining data flows to be evaluated, and if so return to step 5. Otherwise, the process terminates.

An interesting situation arises when a conduit connects zones with different SLs, particularly because we assign the responsibility of protecting access to a zone to the conduits (or more precisely to the zones configuring the conduits). We reason that these network device configuration zones will need to have an SL equal to the highest SL of the zones they are tasked with protecting.

This approach may in some ways be different from the IEC 62443 standard [5], which seemed to cater for scenarios where the conduit has a lower SL than the zone. In this case the conduit is labelled as untrusted, according to part 1-1 (2009) [5]. Following this scenario where the conduit is untrusted, the communication security becomes the responsibility of the individual channel. However, we questioned the usefulness of implementing a conduit in the

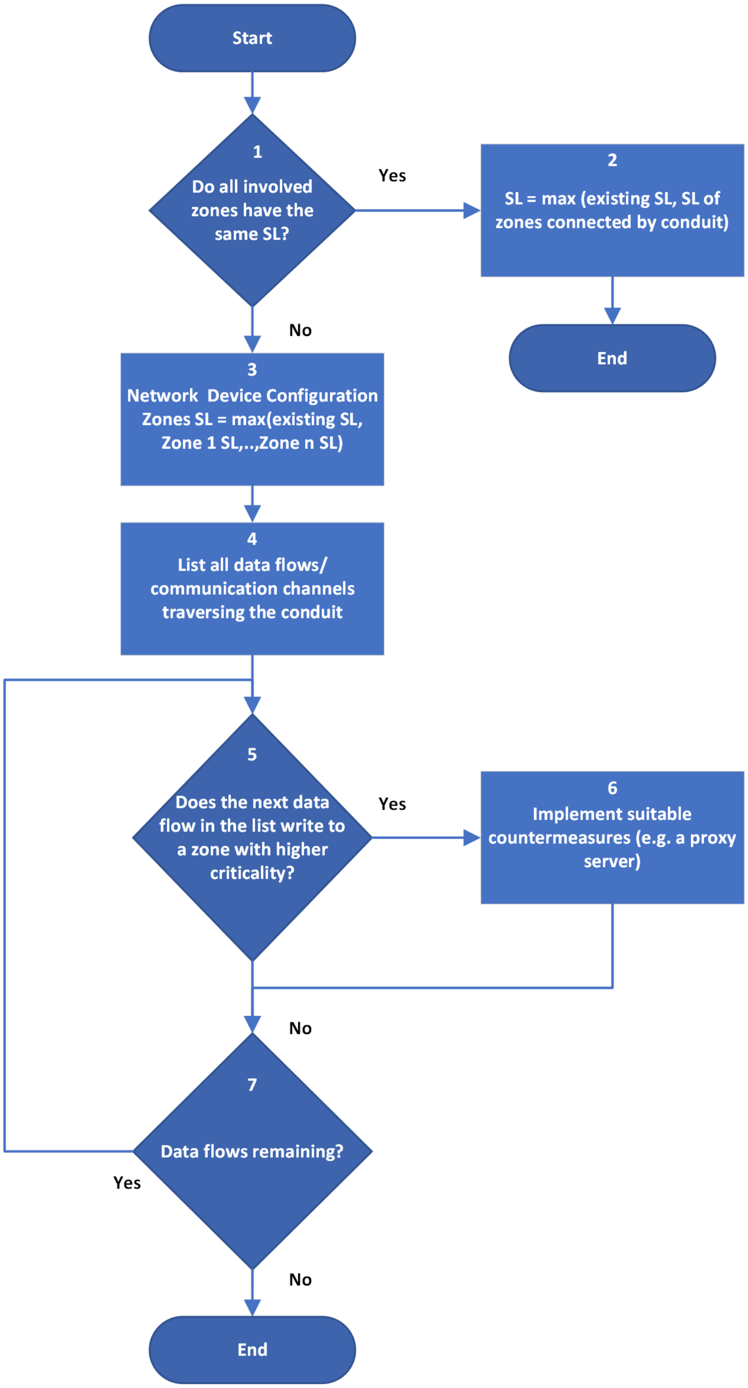
Start
1
Do all involved zones have the same SL?
Yes
2
SL = max (existing SL, SL of zones connected by conduit)
End
No
3
Network Device Configuration Zones SL = max(existing SL, Zone 1 SL,..,Zone n SL)
4
List all data flows/ communication channels traversing the conduit
5
Does the next data flow in the list write to a zone with higher criticality?
Yes
6
Implement suitable countermeasures (e.g. a proxy server)
No
7
Data flows remaining?
Yes
No
End

Fig. 2 The seven elements of the proposed process for securing conduits between zones with different SLs.

first place if the channels passing through it will have to provide their own security.

With our approach, and in line with the commonly accepted philosophy for ICS security where availability and integrity is regarded as more important than confidentiality, we believe that the network device configuration zones should ensure that the availability and integrity of higher SL zones cannot be compromised from lower SL zones. We note that this may imply further security controls in addition to segmentation and boundary protection. When discussing zones and conduits, much of the security discussion tends to revolve around such security controls. While segmentation and boundary protection are efficient security controls, a discussion of the security of zones and conduits must not overlook the aspect of what trust is placed in the data flowing through conduits and between zones. As an example, we can assume to have a server in an SL 1 zone, and a client in an SL 4 zone. While segmentation and boundary protection are suitable for protecting against unintended connections, it may not protect against misuse of legitimate connections.

Similarly, while a VPN connection will protect the confidentiality and integrity of data transmitted across the network, it will not protect against an attacker who has obtained a foothold on the host where the VPN connection originates.

To also defend against these scenarios where an attacker is able to exploit a legitimate connection, it may be necessary to set up intrusion detection functionality on the network devices implementing the conduits, or other methods for detecting or preventing malicious activity.

6 Practical Challenges of using Zones and Conduits

In this section we highlight what we perceive to be practical challenges with using zones and conduits in practice.

In addition to being a grouping of assets, a zone shall have a set of attributes, according to 62443-1-1 (2009) [5]. These attributes are: security policies, asset inventory, access requirements and controls, threats and vulnerabilities, consequences of a security breach, authorised technology (i.e., a dynamic list of technologies allowed and not allowed in the zone), and a change management process. An aspect of this which should not be overlooked is to what extent this is scalable. As an example, an oil and gas installation may implement 30 – 50 zones; for cases where a company has many installations, the number of zones quickly grows large. Another example is the Industrial Automation Security Design Guide 2.0 from Cisco, introduced in section 2, which speaks of scenarios with up to 400 area zones.

We would furthermore argue that the approach of listing threats and vulnerabilities for each zone is problematic for three reasons: it is economically infeasible, it has previously shown to offer limited value for the effort invested, and by the time an installation is in operation the list developed during the design phase may already be outdated.

Regarding the allocation of SLs to zones and conduits, we believe it would be beneficial with more guidance regarding how the overall architecture should influence the selection of the SL for a specific zone or conduit. If one fails to take advantage of the fact that zones in lower parts of the Purdue model are typically protected by zones higher up in the Purdue model, the result may be overly expensive and inefficient security. As an example, the most critical components are typically at the bottom of the Purdue model, and consist of embedded devices with limited features. In cases where these are of high criticality, there have been attempts in the industry to give these high SL values (SL-3 or SL-4), with the result of a lot of non-compliance due to missing features, or due to undesirable connectivity with other components. Provided that the Purdue model is properly implemented, the embedded devices on the bottom of the model are significantly protected by the surrounding networks and components, and should be left with limited responsibilities to protect themselves. Enforcing large numbers of requirements on embedded devices will push the suppliers to replace these devices with more standardized computer architectures and operating systems, to fulfil the requirements. This is not desirable as it leads to devices with increased need of anti-malware solutions, regular / frequent patching etc., which is undesirable for devices with high availability and high integrity demands.

A discussion of zones and particularly conduits should also include a discussion of communication channels, as a conduit is defined as a logical grouping of communication channels. The channel is in turn a specific communication link established between assets. We are of the opinion that concepts such as conduits, channels, communication links, sub-conduits, and sub-zones could benefit from clearer definitions, demarcation, and more examples of implementation. There should also be a clear justification in terms of added value for introducing additional concepts and definition.

Lastly, we believe that ensuring consistent definitions of such terms as zone, conduit and SL across the different part of the IEC 62443 standards would be beneficial for the users of the standard.

7 Further Work

The ideas and proposed principles in this paper are intended as a first proposal to the IACS community, and will have to be further tested and validated together with the industry in real world use cases. This paper should therefore be seen as a first contribution towards establishing detailed and commonly accepted practices for conduit and zone architecture, and subsequent SL allocation.

One particular aspect which we believe can benefit from further study is how to best secure connections between zones with different SLs. This can range from outlining specific recommendations for firewalls and intrusion detection deployment, to developing methods for detecting and preventing misuse of compromised legitimate connections, potentially by relating communication traffic to observed anomalies in the underlying process being controlled.

8 Conclusion

In this article we have investigated the details of conduit architecture and practical considerations of connecting zones with different SLs. Motivated by the widespread use of the zones and conduits paradigm, we propose principles for conduit and zone architecture and a pragmatic process for connecting zones with potentially different SLs. This process is expressed in the form of a flow chart. Lastly we highlight some key challenges with using the zones and conduit paradigm in practice.

Acknowledgements

The research in this paper was supported by the Research Council of Norway through the Cybersecurity Barrier Management project (grant no. 326717). We are grateful to the CBM advisory committee for their insightful comments and discussion.

References

1. Industrial Automation Security Design Guide 2.0 - Chapter: Segment the Network into Smaller Trust Zones (2023). URL https://www.cisco.com/c/en/us/td/docs/Technology/industrial-automation-security-design-guide/m-segment-the-network-into-smaller-trust-zones.html
2. CENELEC: Railway applications: Cybersecurity. ICLC TS 50701:2023 (2023)
3. DesRuisseaux, D.: Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications. Schneider Electric Whitepaper (2018). URL https://technology-signals.com/wp-content/uploads/download-manager-files/78151_PracticalOverviewofImplementingIEC62443SecurityLevelsWhitePaper.pdf
4. Gordon, J.: The Essential Guide to the IEC 62443 industrial cybersecurity standards (2021). URL https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/
5. IEC: IEC/TS 62443-1-1:2009 Security for industrial automation and control systems - Part 1-1: Terminology, concepts and models (2009)

6. IEC: IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (2013). URL https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf. ISBN 978-2-8322-1036-9
7. IEC: IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security Risk assessment for system design (2020). URL https://webstore.iec.ch/publication/30727
8. ISA-GCA: Security Lifecycles in the ISA/IEC 62443 Series - Security of Industrial Automation and Control Systems (2020). URL https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2022%20ISA%20Website%20Redesigns/ISASecure/PDFs/Miscellaneous%20PDFs/Documents-Articles-and-Technical-Papers/ISAGCA-Security-Lifecycles-whitepaper.pdf
9. Kobes, P.: Guideline Industrial Security - IEC 62443 is easy. VDE VERLAG GMBH (2023)
10. Leander, B., Čaušević, A., Hansson, H.: Applicability of the IEC 62443 standard in Industry 4.0 / IIoT. In: Proceedings of the 14th International Conference on Availability, Reliability and Security (2019)
11. Matthias Kern Emre Taspolatoglu, F.S.T.G.B.L.V.P.B.J.B., Sax, E.: An architecture-based modeling approach using data flows for zone concepts in industry 4.0. In: 2020 IEEE International Symposium on Systems Engineering (ISSE), pp. 1–8 (2020). DOI 10.1109/ISSE49799.2020.9272013
12. S. Soderi D. Masti, M.H., Iinatti, J.: Cybersecurity considerations for communication based train control. IEEE Access **1**, 92312–92321 (2023)
13. Schlehuber C., H.M.V.G.T.K.S.S.N.: A security architecture for railway signalling. In: Tonetta, S., Schoitsch, E., Bitsch, F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science (2017). DOI 10.1007/978-3-319-66266-4_21
14. Øien, K., Hauge, S., Jaatun, M.G., Flå, L., Bodsberg, L.: A Survey on Cybersecurity Barrier Management in Process Control Environments. In: Proceedings of 2022 IEEE International Conference on Cloud Computing Technology and Science. IEEE, Bangkok (2022)