HIRSCHMANN
A BELDEN BRAND

White Paper

WP00013HE

The "House of ICS Security" introduces a new and intuitive way to understand cybersecurity and enables users to explore and design effective solutions for a variety of threat scenarios

Dr. Oliver Kleineberg, Manager Advance Development, Hirschmann Automation and Control GmbH

Prof. Dr. Tobias Heer, Future Technologies, Hirschmann Automation and Control GmbH

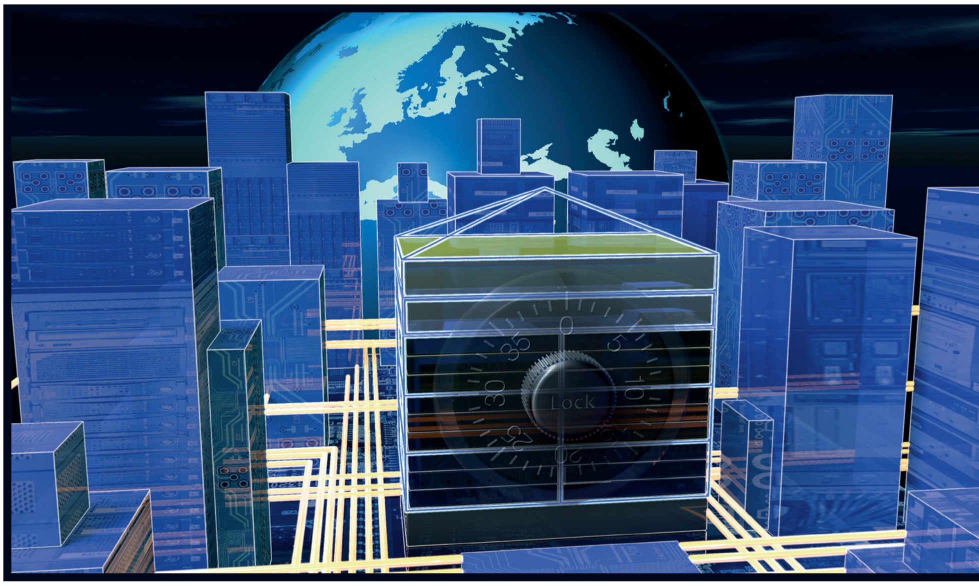


Table of Contents

Executive Summary

Creating connectivity across different networks, sites and companies is at the heart of the Industrial Internet of Things (IIoT). Naturally, cybersecurity is at the very core of these developments and thus, is more important than ever. Yet, it is challenging to discuss cybersecurity in Industrial Control Systems (ICS) because the topic is still very abstract, complex and intangible. While mechanisms to improve physical security, for example a fence or a locked door, can be easily seen and intuitively understood, means for cybersecurity, in contrast, are not visible to the naked eye and often hide behind difficult technical acronyms and concepts. Therefore, these measures are much more challenging to encompass through conventional senses.

The *House of ICS Security*[1] model is a simple but powerful structure to visualize this complex matter. It establishes a common ground for discussions about security threats, as well as an overview of available security features that counter those threats. The model itself is designed in a way that it can be used with two different approaches: a) to explore the different threats and security mechanisms and b) to guide a discussion between ICS experts and security experts based on concrete concerns and threats. When using the model, it provides insights on which security mechanisms are available and how these mechanisms will be effective against specific threats. In addition, it also supports users in determining other important influencing factors such as regulatory requirements and general best practices.

When exploring the model, the user can easily navigate through the different "rooms" and "floors" of the house to discover how threats, security features and best practices are interconnected. The house also shows how more abstract topics like secure product development and supply chain security connect to the overall concept of a secure ICS.

Introduction: Cybersecurity in the Age of the Industrial Internet of Things and Industrie 4.0

Efforts like the Industrial Internet of Things (IIoT) and Industrie 4.0 promise that companies will be able to leverage a vastly improved interconnectivity to create new business opportunities and to optimize many processes on all levels of an industrial plant – which will result in a quantum leap in profitability. While Industry 4.0 mainly deals with intelligent (discrete) manufacturing systems, the IIoT includes the entire world of production and control systems – far beyond the physical boundaries of the factory premises. Both of these concepts are based on the idea that all "things" – from servers, computers and control systems to single workpieces within the network and manufacturing planning and execution systems – will be made accessible from the IT world.

However, this accessibility bears many risks in regard to cybersecurity. Hence, without proper cybersecurity the benefits of the IIoT and Industrie 4.0 may turn into difficult-to-solve cybersecurity threats and dangerous attacks. But which mechanisms belong to a proper cybersecurity concept? Which mechanisms are available and which fit the threats that apply to specific applications? How do different cybersecurity mechanisms work and interact? Answering these questions is far from trivial since cybersecurity has evolved into a vast and complex field. Moreover, many cybersecurity mechanisms are difficult to comprehend because they do not directly relate to the everyday work if ICS experts.

The Challenge of Talking about Cybersecurity

Industrial plant operators are absolute experts in their fields. They usually have an excellent grasp of the control systems that are needed to operate their facility. However, they are often unaware of how they can integrate cybersecurity into their networks, or they are still at the beginning of a learning process in this regard. In the worst case, they might not even know how and where they should start. But this is what matters most: starting the thought process on cybersecurity. A comprehensive strategy cannot be realized in a single step – only in the course of a long-lasting improvement process that has to start at some point in time. This can be a start structured in small phases and small increments that will evolve and develop over time, but without an initial starting point, this process will often fail to set off at all.

Due to the complexity of cybersecurity and due to the fact that it is an abstract topic, a discussion between security experts and plant operators is often very difficult, especially in the beginning of implementing a continuous cybersecurity improvement process. But even if ICS experts already have a good grasp on cybersecurity, their terminology may not match the terminology of their security expert counterpart. Hence, they might understand certain terms to mean something entirely different than their conversation partner. In summary: only when the operators can define the requirements for the protection of their systems clearly and intelligibly can security experts address them and develop appropriate security concepts that are customized for the specific requirements and envisaged threat scenario. If this succeeds, the plant operators also gain valuable system information about the integration of cybersecurity into their own systems. Subsequently, they can use this knowledge to re-evaluate their cybersecurity concepts, taking these new insights into account. This will automatically result in new ideas to improve the existing cybersecurity concept and this is the start of a continuous improvement process. This process is indispensable in the changing world of the IIoT, where security threats are constantly evolving and security concepts must be adapted accordingly.

Creating a Common Knowledge Base

What is the best way to get security experts and plant operators to speak the same language to initiate this continuous improvement process and support it on the long term? What is the common ground to which both sides can relate? An excellent starting point is the physical world around us. This is common ground that we all understand very well since each of us has lived in it since birth. If the complex field of cybersecurity can be expressed in terms of our everyday life, this can create a strong foundation for further discussion.

Finding simple but accurate real life equivalents of cybersecurity mechanisms can boost the understanding of complex mechanisms and relations. Take a firewall as an example: A firewall in the network is a device that a user cannot see directly when using the network. It blocks specific traffic and permits other traffic to flow through. A real-life equivalent of the firewall would be a gate and a gatekeeper. A locked gate will only be opened for certain people who possess a key of the right size or shape or embedded with the right electronic coding. Similarly, the firewall only permits network traffic that follows predefined patterns. However, explaining network security concepts immediately allows users with diverse education and professional backgrounds to talk about cybersecurity with confidence. This basic concept of linking cybersecurity to the real world is the essence of the House of ICS Security.

To achieve this goal, Belden – which has longstanding experience in the area of industrial data security with its brands Hirschmann, Garrettcom and Tofino Security – has created the House of ICS Security. It is a model to relate the complex field of ICS security and its many aspects and facets to a real-world representation of a house with floors, rooms, an attic and a basement. This model enables plant operators to determine countermeasures for concrete threat scenarios that they perceive for their installation. The House of ICS Security can also be used as a reference tool to reduce the knowledge gap between plant operators and experts to create a consistent basis for meaningful discussions.

The following section will introduce the construction principles of the house and – to keep the image consistent – which rooms and other elements it contains and how the foundation and roof are formed. However, the primary focus is not a full, exhaustive overview of the numerous functions, norms and regulations that are contained in the house. Instead, this is about how users can profit from this model to ensure their systems fulfill the three basic goals of cybersecurity: the availability of the network and its services, the integrity of information and the confidentiality of data.

The House of ICS Security

All security mechanisms can be categorized based on their nature. However, such categorization is not simple because many different characterizations exist. Depending on a) the threat that a mechanism defends against or b) the type of attacker or c) the time and nature of its protection, different mechanisms fall into different categories. Understanding and looking at different mechanisms in these categories helps us understand the vast field of mechanisms better and helps us explore new options for defending an ICS. Yet, the result of such categorization is a multidimensional model which is difficult to understand. The House of ICS Security translates this multidimensional model to a real-life example: a house with rooms and floors. The following sections explain the different parts of the house and show how this house can guide a discussion.

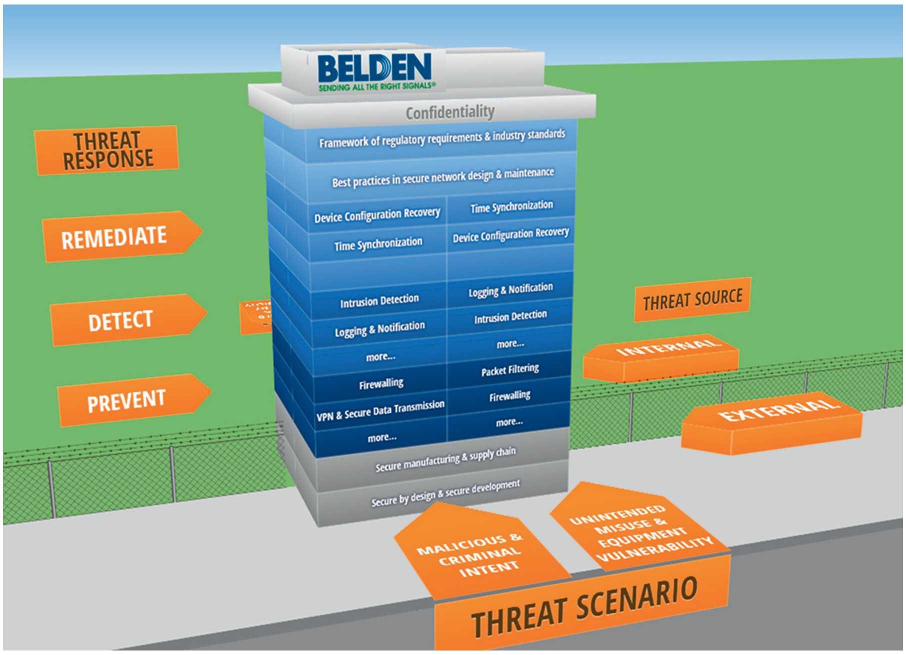

BELDEN
SENDING ALL THE RIGHT SIGNALS
Confidentiality
Framework of regulatory requirements & industry standards
Best practices in secure network design & maintenance
Device Configuration Recovery
Time Synchronization
Time Synchronization
Device Configuration Recovery
Intrusion Detection
Logging & Notification
Logging & Notification
Intrusion Detection
more...
more...
Firewalling
Packet Filtering
VPN & Secure Data Transmission
Firewalling
more...
more...
Secure manufacturing & supply chain
Secure by design & secure development
THREAT RESPONSE
REMEDIATE
DETECT
PREVENT
THREAT SOURCE
INTERNAL
EXTERNAL
MALICIOUS & CRIMINAL INTENT
UNINTENDED MISUSE & EQUIPMENT VULNERABILITY
THREAT SCENARIO

Figure 1 – the architecture of the House of ICS Security

Categorization of Threats and Countermeasures

One option for considering threats to cybersecurity in more detail is to divide them into different defining aspects. The three defining aspects that are chosen for the House of ICS Security are:

- Threat Source
- Threat Scenario
- Threat Response

When these three aspects are set up in the form of a grid, this creates a cube that resembles a house with different rooms, as visible in **Figure 1**. These aspects have characteristics assigned to them so that they can be refined further.

There are generally only two possible characteristics for the threat source – either it is inside the network that has to be protected ("internal") or the threat is located outside of the network ("external"). This differentiation constitutes the first dimension of the House of ICS Security.

The threat scenario can also be expanded into two different characteristics. For one, an attacker can act with "malicious and criminal intent," for example to hack a system in order to sabotage it or gain information. However, only about 20 percent of all documented cybersecurity problems have this characteristic. In nearly 80 percent of the cases, there is no malicious intention at *all*[2].

In those cases, the root causes are mistakes made by users, such as incorrectly configured devices or the cause might be weaknesses in the software. Therefore, this threat scenario can be named "unintended misuse and equipment vulnerability," which might lead to the failure of a network or an unintentional dispersal of sensitive information. The classification into security issues based on the presence or absence of malicious intent form the second dimension of the House of ICS Security.

Once the threat has been narrowed down on the basis of the source and the scenario, the best response to it still has to be determined.

Three threat responses are possible: First, one can try to avert an attack before it starts ("prevent"). If this can't be realized – for whatever reason – an alternative is to recognize the attack ("detect") and then act. Additionally, the damage that occurs in a system can also be removed afterwards ("remediate"). To effectively counter a particular threat, all three threat responses can be used independently or combined. These three responses provide the third dimension of the house.

When the values of all three aspects have been determined, the three aspects will point to exactly one room of the house. This room contains precisely those security mechanisms and countermeasures that are effective against the threat that has been described via the three aspects that led to this particular room.

Using the House to Discover Relevant Security Technology

Even during the initial phase of cybersecurity implementation in a plant, an operator can describe possible concerns or threats in some way. This verbal description of the threat can then be analyzed and categorized on the basis of the three described aspects. Typically, the described threat scenario can be directly mapped onto the three aspects – and by association directly mapped onto the House of ICS Security – with the aid of simple keywords. Here are three examples to illustrate this method:

1. If a plant operator is worried that an attacker might penetrate a network via the Internet and spy on important production knowledge, this is an external threat that can be classified under the key concept "malicious and criminal intent." In this case, the keyword "Internet" indicates the external threat source while "spying on the know-how" in the threat scenario points to the criminal intent. Subsequently, it just has to be determined whether such an attack should be prevented, if it is sufficient to detect it or if the damage needs to be remediated at a later time. In the course of developing a comprehensive security strategy or expanding an existing concept, it is also possible to combine different responses to achieve greater effect. This example points at specific rooms in the house in which relevant technologies and measures are listed and explained.

2. A plant operator wants to be protected against possible software errors in the control applications, which may result in security gaps in the network at some point in the future or against the network or a specific application becoming unavailable. In this case, the threat source is "internal" due to a possible malfunction of the machines that are located on the internal network. The keyword "software error" indicates a security problem that arises unintentionally – namely through the hidden error in the device software. Therefore, the threat scenario is "unintended misuse and equipment vulnerability." Since the occasional occurrence of software errors – so-called bugs – is impossible to prevent, the first step in developing a countermeasure is usually the detection and remediation of the threat and not preventive protection. However, this approach is often combined with preventive responses, although the preventive measures will not always be effective – after all, it is not possible to precisely predict in advance what flaws may occur in the software. Again, this description allows the user to identify a specific room in the house.

3. An external attacker has penetrated the network of a company and has disabled a production system (similar to the scenario in the first example). The "prevent" and "detect" responses are therefore not applicable, as the attack has taken place in the past. But to make sure that the attacker has not left a back door open for further attacks, the subsequent analysis and remediation of the damage are effective means to prevent further damage. The corresponding room in the house contains exactly the mechanisms that are available for remediation.

After determining the corresponding room, the user can discover the related technologies and mechanisms. By looking at neighboring rooms, the user can expand his knowledge by looking at similar technologies that address different threat sources, scenarios and responses.

Navigating the Rooms of the House of ICS Security

With two threat sources, two threat scenarios and three different reactions to the threat, as shown in **Figure 1**, the house contains twelve rooms in total. The rooms are arranged in the "coordinate system" that is spanned by these three independent axes: threat source, scenario and response. This is visualized by the arrows in **Figure 1**. The rooms can be selected by the user, and this will expand the view of a particular room to show the included security features. Determining which room needs to be selected depends on which characteristics of the aspects were selected or which key concepts can be recognized in the description of the threat. With regard to the three examples in the previous section, this means:

1. To make sure that important production know-how is not spied on during an attack from the internet, external threat source, malicious and criminal intent and prevent are identified as being the relevant characteristics. Following these three characteristics and narrowing down the possible rooms each time a selection is made, the user arrives at precisely one room in the house. This room contains functional groups such as firewalling, packet filtering, VPN (Virtual Private Network) and secure data transmission or deep packet inspection, which are effective against this particular threat. This example is shown in **Figure 2**.

2. To prevent the creation of new attack surfaces in the network due to potential bugs in the control software, internal threat, unintended misuse and equipment vulnerability and "detect" are selected. Among other features, the corresponding room offers information on network segmentation, device access control, DoS (Denial of Service) prevention and deep packet inspection.

3. To ensure that no backdoor was implemented for further attacks after an act of sabotage of a production facility, external threat source, malicious and criminal intent and remediate are selected. This will lead to a room where functional groups like device configuration recovery or time synchronization are explained to help in the remediation of the security incident.

The information in each of the twelve rooms may be partially identical. After all, a highly effective protective mechanism that has a broad field of application can be applied to more than just one combination of aspects. Here is an example:

- The combination external threat source, malicious and criminal intent and prevent, and the combination external threat source, unintended misuse and equipment vulnerability and prevent both lead to rooms that include the firewalling security feature. Although both of these scenarios lead to different rooms and the exact configurations of their threats are different, protection of the network with a stateful packet inspection firewall is possible and effective in both cases.

The rooms give users a comprehensive overview of the security functions that guarantee optimal protection for their respective threat scenarios. If, at this point, a user wants to delve deeper into this matter, this is certainly possible. To this end, the rooms contain "drawers" in which the functions are described in detail. The House of ICS Security can therefore also be used simultaneously as a knowledge database.

Drawers in the Rooms

In the standard view of the house as shown in **Figure 1**, three drawers per room are visible. The first two drawers show the security function groups that are most effective to defend against the threat that is assigned to the respective room.

The room identified via example no. 1 in the left lower corner, just above the two foundation levels (see **Figure 2**) has "Firewalling" and "VPN and Secure Data Transmission" as its most important function groups, so these are visible in the drawers.

The third drawer contains additional effective function groups. Upon entering a particular room, the house itself moves to the background and the security functions that were previously hidden in the third drawer are unfolded, as shown in **Figure 3**.

Describing the variety of security functions in each of the function groups in detail would go beyond the scope of this white paper. This is why only a short introduction will be provided here, followed by an example that shows how multifaceted the information is. The interactive model that contains all the information can be accessed through the House of ICS Security website (http://houseofsecurity.belden.com) or through the House of ICS Security App in the Apple App store.

The detailed security features are summarized as function groups. The function groups include, for example, "Firewalling," "VPN and Secure Data Transmission," "Packet Filtering," "Intrusion Detection," "Logging and Notification," "Device Configuration Recovery" and "Time Synchronization." Anyone who would like to know more can select the "Firewalling" function group, for example, and then receive more detailed information, such as an overview of the basic functionality of a Stateful Packet Inspection (SPI) firewall. Among other things, it explains how this firewall differs from a pure "stateless" packet filter and how it is used in additional security concepts such as Defense in Depth or Zones and Conduits.

In **Figure 3**, the *Firewalling* function group was selected for a more detailed view. Through the selection of individual topics, the user has the option to obtain in-depth information about this function group or directly access information about products and services by Belden that contain this security feature. The text also contains additional information that associates the security functions with best practices in industrial network security that this feature will support or enable.

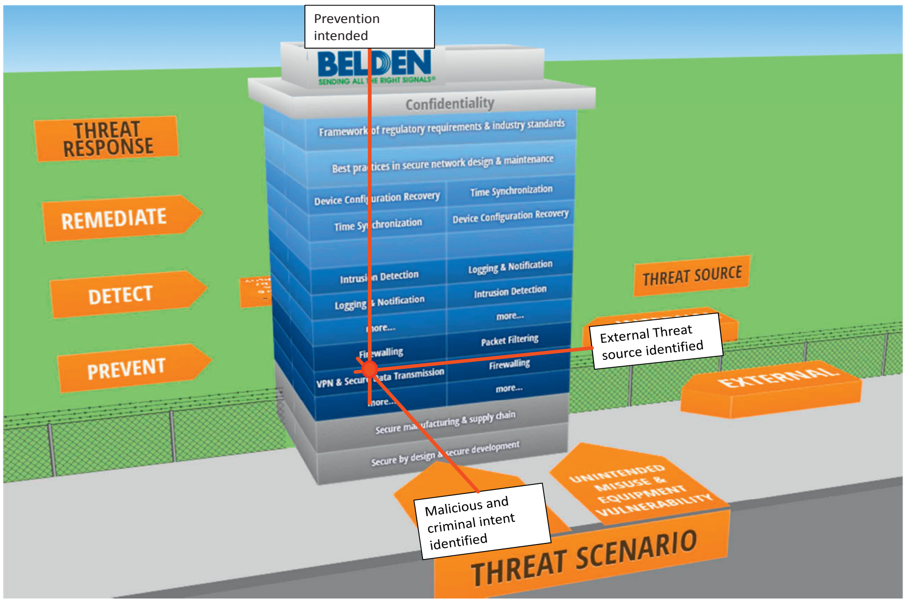
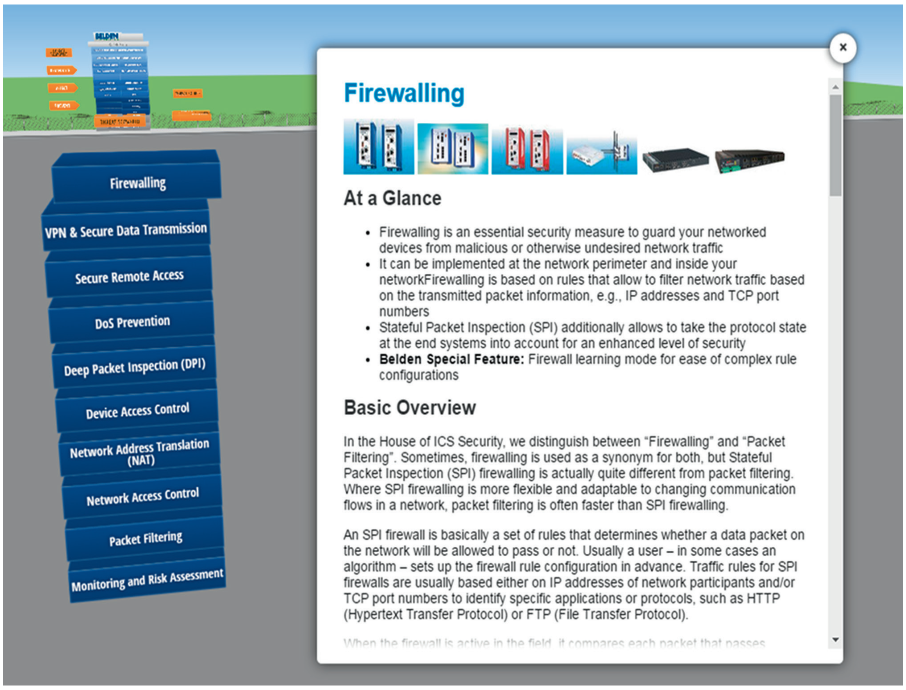

Prevention intended
BELDEN
SENDING ALL THE RIGHT SIGNALS®
Confidentiality
Framework of regulatory requirements & industry standards
Best practices in secure network design & maintenance
Device Configuration Recovery
Time Synchronization
Time Synchronization
Device Configuration Recovery
Intrusion Detection
Logging & Notification
Logging & Notification
Intrusion Detection
more...
more...
Firewalling
Packet Filtering
VPN & Secure Data Transmission
Firewalling
more...
more...
Secure manufacturing & supply chain
Secure by design & secure development
THREAT RESPONSE
REMEDIATE
DETECT
PREVENT
THREAT SOURCE
External Threat source identified
EXTERNAL
Malicious and criminal intent identified
UNINTENDED MISUSE & EQUIPMENT VULNERABILITY
THREAT SCENARIO

Figure 2 – Selecting the room that fits to the threat


Firewalling
VPN & Secure Data Transmission
Secure Remote Access
DoS Prevention
Deep Packet Inspection (DPI)
Device Access Control
Network Address Translation (NAT)
Network Access Control
Packet Filtering
Monitoring and Risk Assessment
×

Firewalling

At a Glance

- Firewalling is an essential security measure to guard your networked devices from malicious or otherwise undesired network traffic
- It can be implemented at the network perimeter and inside your networkFirewalling is based on rules that allow to filter network traffic based on the transmitted packet information, e.g., IP addresses and TCP port numbers
- Stateful Packet Inspection (SPI) additionally allows to take the protocol state at the end systems into account for an enhanced level of security
- **Belden Special Feature:** Firewall learning mode for ease of complex rule configurations

Basic Overview

In the House of ICS Security, we distinguish between "Firewalling" and "Packet Filtering". Sometimes, firewalling is used as a synonym for both, but Stateful Packet Inspection (SPI) firewalling is actually quite different from packet filtering. Where SPI firewalling is more flexible and adaptable to changing communication flows in a network, packet filtering is often faster than SPI firewalling.

An SPI firewall is basically a set of rules that determines whether a data packet on the network will be allowed to pass or not. Usually a user – in some cases an algorithm – sets up the firewall rule configuration in advance. Traffic rules for SPI firewalls are usually based either on IP addresses of network participants and/or TCP port numbers to identify specific applications or protocols, such as HTTP (Hypertext Transfer Protocol) or FTP (File Transfer Protocol).

When the firewall is active in the field, it compares each packet that passes

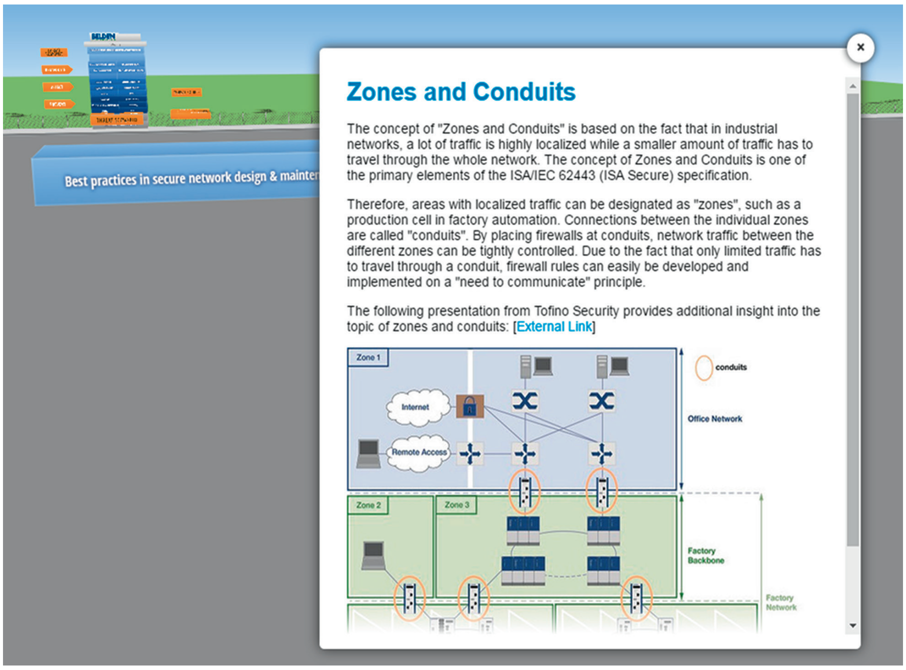
Figure 3 – detailed view of a room with all drawers visible

This helps the user to build knowledge bridges between security functions, such as firewalling and overarching security best practices, such as Zones and Conduits. To support the understanding of the connections between security features and best practices, the interactive model supports direct links to allow a smooth transition between the different parts of the house by the user.

An example of a best practice with firewalls is Zones and Conduits, as defined in the international standard *IEC 62443*[3]. This process identifies zones in the network in which devices communicate primarily with each other and where data exchanges with other zones are rare occurrences. These zones are separated from each other with several firewalls, as shown in **Figure 4**. Only certain devices may communicate via the transitions between these firewalls, i.e. the “conduits.” Different network areas can be effectively sealed off from each other and a need-to-communicate approach can be realized.

In this way, the various rooms of the House of ICS Security can also serve as a basis and guideline for discussions between security experts and, for example, plant operators. Based on the shared information that the house provides, a target-oriented dialog can be developed, resulting in a customized security concept.

This dialog can be very dynamic and can jump from topic to topic, and the House of ICS Security matches this by providing an easy to use dynamic access to the information it provides, as shown in **Figure 3**. Users will be able to quickly jump from topic to topic in the model as the discussion evolves. If a deep dive into a specific topic is necessary, the house will also provide information for this within the individual drawers.



Zones and Conduits

The concept of "Zones and Conduits" is based on the fact that in industrial networks, a lot of traffic is highly localized while a smaller amount of traffic has to travel through the whole network. The concept of Zones and Conduits is one of the primary elements of the ISA/IEC 62443 (ISA Secure) specification.

Therefore, areas with localized traffic can be designated as "zones", such as a production cell in factory automation. Connections between the individual zones are called "conduits". By placing firewalls at conduits, network traffic between the different zones can be tightly controlled. Due to the fact that only limited traffic has to travel through a conduit, firewall rules can easily be developed and implemented on a "need to communicate" principle.

The following presentation from Tofino Security provides additional insight into the topic of zones and conduits: [External Link]

Figure 4 – Best practice Zones and Conduits

For most security concepts, it makes sense to combine more than one security function. The reasoning behind this is that if an attacker is able to overcome one security function, there is still another line of defense that (ideally) will operate with a different security technology. This proven approach is part of a diverse defense-in-depth concept, a strategy for a multi-layered defense.

By selecting several functional areas within the same room in the House of ICS Security, a user – possibly together with a security expert – can create a defense-in-depth concept that is customized specifically for the identified threat. Furthermore, the threat source and threat scenarios can be kept constant and only the threat responses varied in order to round off the concept. Security functions that are used at different times can be combined with each other, for example to create a strategy for prevention, subsequent detection and possible remediation. The user can switch between the various rooms of the house and assemble the necessary information to create defense-in-depth strategies that also encompass variety in prevention, detection and remediation. To support this, solutions and services by Belden are also visible in the room that includes a particular security feature.

Foundation and Roof of the House of ICS Security – Essential for Stability

Just as with any house, the House of ICS Security needs a solid foundation and roof. These two areas do not contain specific security features but are still significant for the development of a holistic security concept. The foundation of any effective security strategy is the use of products in which security is considered as an integral component, starting at the early stages of product development (“secure by design and secure development”). Cybersecurity is an essential component of industrial communication technology, such as Ethernet switches or IP routers, and should preferably be implemented from the start – because it is very difficult to achieve a comparable level of protection with security that is bolted on as an afterthought.

Furthermore, integrating cybersecurity into every process is becoming increasingly important, both for industrial network communication solution providers as well as plant operators. In other words: From purchasing to development and on into manufacturing of a product (“secure manufacturing and supply chain”), security is a constant companion. This is particularly important for the manufacturers of industrial network devices that are a potential target for attacks: For example, hackers might

try to smuggle firmware images into manufacturing that are faulty or infected with harmful software. If such a firmware image was to be installed on a product, for example an Industrial Ethernet Switch, at manufacturing time, the device may shut down systems or open back doors for data theft somewhere else later, after it has been installed in the field. This is why there are already international standards and provisions for security in supply chain and manufacturing in place. Examples include the North American C-TPAT (Customs-Trade Partnership Against Terrorism) or the European AEO *(Authorized Economic Operator)*[4]. A company that is certified according to AEO-S (Security) or AEO-F (Full) thereby includes supply chain and production components in its overall security concept and acknowledges, that product manufacturing is a sensitive process that needs to be protected.

The roof of the House of ICS Security also consists of two layers: the best practices for secure design and a secure operation of networks, along with framework of regulatory requirements and industry standards. Together, they form a reference work in which essential aspects of cybersecurity are presented in an easily comprehensible way.

Users can take advantage of this reference work to obtain information independent from a concrete threat. The best-practices are interlinked with the security features in the rooms to support the building of systemic knowledge: How to connect the dots between overarching security concepts, best practices and individual security features.

The framework of regulatory requirements and industry standards provides users with information that is important for their own plants or for participating in proposals for projects – for example if they are providers in a critical infrastructure area. In Germany, operators of critical infrastructures – from energy supply to rail transportation to telecommunications – are legally required to prove that their IT systems are protected against cyberattacks. This requirement is mandated by the IT Security Act that was passed by the German parliament in *June 2015*[5]. Within a period of two years, the respective infrastructural areas have to create and implement guidelines for cybersecurity. There are similar regulations in other countries, such as NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) for power grids in the United States.

The House of ICS Security and a Secure Product Lifecycle

Based on the central significance of cybersecurity, plant operators should check whether the processes and products by manufacturers of industrial communication technology correspond to the required standards. But this is only one side of the coin, since threat scenarios are constantly changing: A product or a security protocol that was absolutely secure at a certain point in time will not necessarily be secure in the future. Long-term security can thus only be achieved through a constant inspection and re-evaluation of one's own security concepts. This results in a continuous improvement cycle and collaboration between manufacturers and plant operators – they are connected to each other through the secure lifecycle of the products. It is essential that plant operators take not only the total cost of ownership into account when selecting an equipment manufacturer's products – they must also consider the total risk of ownership.

The manufacturers are obliged to immediately notify the plant operators of any issues that have arisen and to provide timely updates for their products that can be used to close potential security gaps. The operators, in turn, must install a continuous improvement process in their companies to provide lasting protection for the networks and ensure that they can implement product updates in a timely manner. The House of ICS Security is helpful in this regard as well, the website/app will be updated regularly to include new products, concepts and features and also to reflect changes to the existing cybersecurity landscape. Through this, the House can be used as a tool to develop security concepts further and to prepare for future threats.

Conclusion

The IIoT and Industry 4.0 lead to much more interconnected ICS. This enables companies to increase their productivity and efficiency, but it also makes them more susceptible to threats from the virtual world, the so-called cyberspace. With the interactive model "House of ICS Security," the threats as well as the corresponding countermeasures can be categorized on the basis of consistent criteria.

Just like a real house, the interactive model has a foundation, a roof and several rooms. The rooms contain security features that are effective against a particular threat that is defined by three categories:

- Threat Source
- Threat Scenario
- Threat Response

The rooms offer a comprehensive overview of the security functions that guarantee optimal protection for their respective threat scenarios. They contain "drawers" in which these security functions are described in detail. The House of ICS Security thus represents a knowledge database that is updated continuously to match the constant changes of the security landscape.

The foundation and the roof of the security house each consist of two layers in which overarching aspects are considered that are essential to an effective cybersecurity strategy. The spectrum ranges from the consideration of cybersecurity during the planning (secure by design) to the integration of security into the entire manufacturing and supply chain processes up to cybersecurity best practices, accompanied by the regulatory requirements and industry standards.

The interactive model, offered through a website and a smartphone app, offers plant operators and security experts a shared foundation to develop customized security solutions. These solutions do not always need to start off as complete master plans. A comprehensive security strategy can only be achieved through small steps and gradual improvements – and this process actually never ends. But as it is well known, the first step is always the hardest. With the help of the House of ICS Security, this essential first step can be facilitated to great extent.

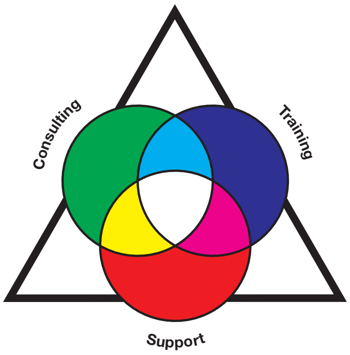
HIRSCHMANN

A BELDEN BRAND

5. References

1. The House of ICS Security interactive Website - https://houseofsecurity.belden.com
2. The repository of Industrial Security Incidents – http://www.risidata.com/
3. Notes by the German Commission for Electrical Engineering (Deutsche Kommission für Elekt rotechnik, DKE) about the standard series IEC 62443 - https://www.dke.de/de/std/Industrie40/Seiten/IEC62443.aspx
4. Notes on the Authorized Economic Operator (AEO) at zoll.de - http://www.zoll.de/DE/Fachthemen/Zoelle/Zugelassener-Wirtschaftsbeteiligter-AEO/zugelassener-wirtschaftsbeteiligter-aeo_node.html
5. Website of the Federal Office of Security in Information Technology on the IT Security Act - http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html

Belden Competence Center



As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge play a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world's first certification program for industrial networks. Up-to-date manufacturer's expertise, an international service network and access to external specialists guarantee you the best possible support for products from Belden, GarrettCom, Hirschmann, Lumberg Automation and Tofino Security.

Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at **www.beldensolutions.com** and follow us on Twitter **@BeldenInc.**