HIRSCHMANN
A BELDEN BRAND

White Paper

Advanced Security for Industrial Networks

Redefining visibility, authentication and access to protect mission-critical networks

Gilad Walden – Vice President Technology Strategy, ForeScout

Prof. Dr. Tobias Heer – Senior Architect CTO Office, Hirschmann Automation and Control GmbH

Dr. Oliver Kleineberg – Global CTO Industrial Networking, Hirschmann Automation and Control GmbH

Executive Summary

The threat landscape for industrial networks is rapidly changing. As new attack vectors and attacks surface, operators of these operational technology (OT) networks struggle to maintain visibility into the network's security posture. Moreover, formal requirements stemming from new standards and regulations are putting an additional stress on the operators of OT networks. Network access control plays an important role in solving these two very different and difficult challenges.

This paper presents a powerful integration between the ForeScout® platform as a network visibility, assessment and access control solution, and Hirschmann Industrial Ethernet switches as points of enforcement. The solution paves the way for a holistic approach to network access control in OT networks and succeeds in applying next-generation network access control to the access links in industrial applications: bringing it down to the factory floor.

Table of Contents

Chapter 1 – New Challenges for Cybersecurity in Mission-Critical Networks

Significant changes are happening in the world of industrial operational technology networks: Formerly closed and relatively inaccessible networks and installations are being forced away from isolated existence as they become increasingly interconnected with the rest of the world. The drivers behind this change are novel applications that provide real, measurable added value, such as secure remote access over the Internet directly to manufacturing machines for remote maintenance operations.

Another key reason for increased connectivity is the need for advanced data processing which requires the aggregation of sensor data from the field level to on-premise. This aggregation is essential to enable the use of powerful cloud services and valuable big data analysis.

The increasing interconnection with the world of IT (Information Technology) and the IoT (Internet of Things), however, exposes new attack surfaces in the OT networks and forces OT network operators to rethink established but outdated security best practices to adjust to the new threats. Moreover, simple and formerly effective security methods like perimeter security and the proverbial "air gap" – the complete disconnect of the OT network from any other networked resource – have become impractical or ineffective.

Targeted attacks against industrial sites like Stuxnet, BlackEnergy and Industroyer malware can "jump" the air gap by means of infected devices or USB media. What makes the situation even worse is that Conficker, Wannacry and other ordinary IT malware continue to wreak havoc in vulnerable OT networks all over the world on a regular basis.

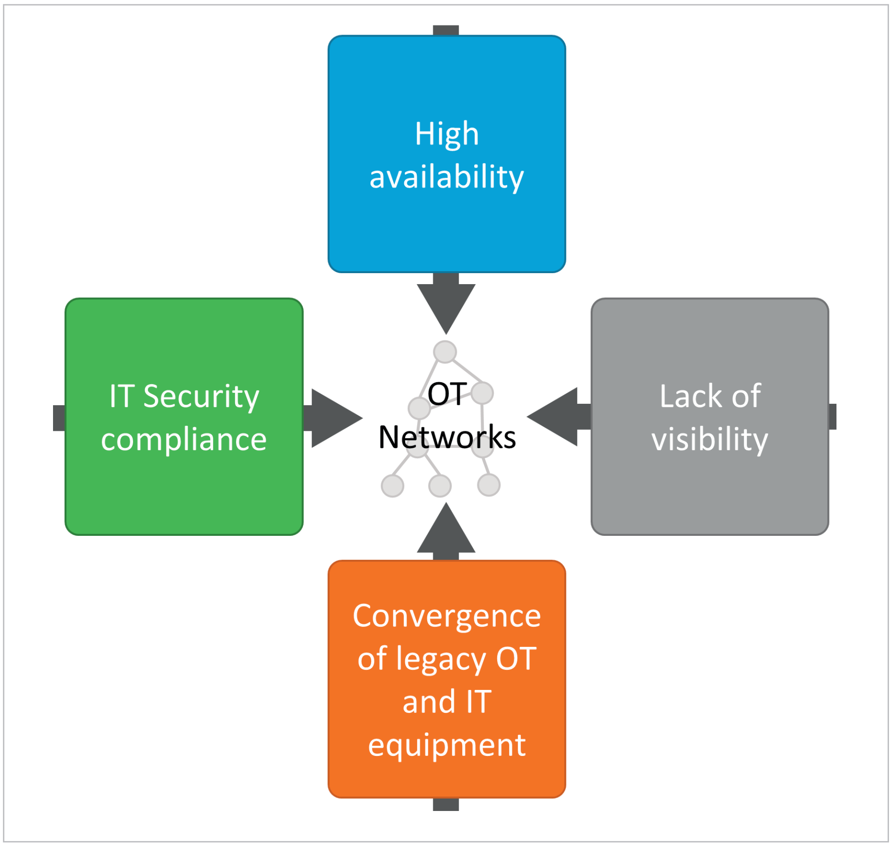

Figure 1: Current pain points for OT networks

When implementing new security measures to address the new threat landscape and expanding attack surfaces, OT network operators are faced with four severe challenges:

- lack of visibility into their networks,
- a vast installed base of legacy equipment,
- additional pressure from new regulations and compliance requirements and
- the requirement to still deliver high reliability and uptime for all mission-critical systems of the OT networks.

In the following pages, we briefly address these four core challenges for implementing new IT Security measures in OT networks.

Challenge 1: Lack of visibility into network activity and connected devices

OT network operators often suffer from a lack of visibility in their networks. The devices and functions that are allowed and should be present on OT networks are often strictly regulated but difficult to enforce. Equipment, be it OT, IT or IoT, is constantly connected to and disconnected from the network. For example, many maintenance processes are still performed manually or performed as part of a maintenance agreement through their equipment vendors. Moreover, "creative" solutions and quick fixes may lead to a considerable number of hidden or unknown devices. This so-called "shadow IT" often has poor security settings and runs outdated software. With hidden or temporarily connected devices, such as service laptops, and externally generated network activity taking place, a constant potential threat level is present in the network that needs to be controlled.

Challenge 2: Convergence of legacy operational equipment and IT technologies

While newer OT equipment is constantly and increasingly adopting newer network security protocols and features, many organizations have a huge installed base of devices that predates the time when network security was deemed a necessity for OT networks. While consumer electronics are regularly replaced with the most recent and fashionable devices, industrial equipment is expected to operate for decades to achieve a solid return on investment. Thus, sub-standard security due to outdated devices becomes a long-term problem that cannot be solved by simply waiting for the old devices to be replaced with newer, more secure models.

At the same time, more and more IT software or devices with appropriate security capabilities enter the industrial space. However, despite their more modern interfaces and more up-to-date security protocols, devices that were primarily developed for IT environments lack important industrial features, such as special purpose protocols and essential reliability and redundancy mechanisms that are of paramount importance for operating mission-critical networks.

Combining OT and IT devices and software solutions in the same application networks can actually lead to reduced security and insufficient reliability and availability. To make the situation even worse, many IT vendors only offer a product lifecycle with guarantees for product availability and software updates that is too short for the long lifetimes of industrial plants and applications. Hence, IT equipment may fail earlier than long-life OT equipment and replacements become increasingly difficult to get the longer the application runs.

This mixed mode of operation between modern and outdated systems as well as between IT and OT systems causes the OT network solutions to constantly rise in complexity. High complexity then causes network administration – especially security designs – to become significantly more complex and thus, increasingly prone to error. Therefore, seamless integration between IT and OT equipment is essential to improve security of these networks and minimize friction between components.

Challenge 3: Constant pressure caused by audits and compliance obligations

Safety and security for employees and customers have always been top priorities in industrial and utility companies, which is partly why they are so highly regulated. Security mandates that result in fines for noncompliance exist across most industries. Agreed-upon standards must be met to help institutionalize best practices. New regulations for critical infrastructure (transportation, power generation and distribution, food and beverage, water, etc.) have increased the pressure to introduce new security processes and follow additional standards. These standards require both organizational and technical changes to be made. The increasing regulatory requirements put additional pressure on the operators because they need to consider compliance aspects in their technical security concepts at all times. Staying up to date with the most recent requirements and the ever-changing state of the art has become a major challenge for OT operators across many industrial sectors.

Challenge 4: Necessity for continual uptime

Failure of a mission-critical OT network typically results in downtime of the most important aspects of a company's business. Hence, any downtime can turn into millions of dollars in lost productivity, highly vocal, disappointed customers, emergency repair costs and regulatory fines. This is the prime reason why the value of availability is placed significantly above integrity and confidentiality in mission-critical networks. Machines must reach a high OEE (overall equipment effectiveness) metric. There is no time to allow IT-style updates and patches that take down and reboot equipment due to tight interconnections between the different parts of the mission-critical network. For example, on a manufacturing line, taking only certain parts of the network or even individual machinery offline is difficult.

The necessary adoption of new defensive strategies creates significant challenges for OT network operators. One major concern of OT operators is that additional security can compromise the robustness and availability of the network – albeit only under certain circumstances. The prevalent fear is that new security measures could lead to unexpected side effects like disruptions in the operation and too-difficult-to-understand communication limitations that might make operating a network with extreme reliability requirements a daily nightmare. With this in mind, OT network operators must implement new state-of-the-art security measures in a way that the availability of the network continues to be a top priority.

The focus of this white paper is to illustrate how modern security principles can be combined and utilized to enable network security in mission-critical installations without compromising security or availability. Through an efficient combination of technical features on different levels, such as the integration of Hirschmann-branded Industrial Ethernet switches and IP routers with the industry-leading ForeScout visibility and control platform, advanced security mechanisms are enabled throughout the entire network infrastructure. This is valid from the industrial factory floor on the field level up to the industrial backbone network in an on-premise industrial data center.

The combination of highly reliable industrial network access switches, together with the state-of-the-art software solution, enables tailor-made effective security postures for the different areas of the mission-critical network, taking into account the requirements and constraints of each application area.

Chapter 2 – The Role of Network Access Control in IT and OT Security

The high-level definition for network access control is a set of technologies that enable implementation of policies for controlling access to corporate infrastructure by both user-oriented devices and 'headless' devices (IoT). Policies that regulate access to the network may be based on authentication, endpoint configuration and posture, endpoint function, location of the connectivity and/or a user's role/identity.

Network access control solutions should implement both pre-connected as well as post-connected network admission. Pre-connected admission checks the identity of a device before it can connect to the network. Pre-connected network admission enables the policies and actions to be set up prior to the connection attempt of a device to the network. It regulates if a device can access the network and what its clearances and capabilities on the network may be. This has historically been based on the IEEE 802.1X [1] network authentication standard in combination with authentication servers, such as RADIUS [2]. Post-connect policies are usually based on the integration with other security products. Such a protocol monitors devices and their behavior constantly after the connection to the network has been established. Post-connection admission can remove a device from the network or can isolate it, if it is found that the device is not conforming to the security standards required.

The network access control market has evolved from primarily pre-connection solutions that were limited to a binary network access decision (i.e., grant access or not), based on a limited exchange with the connecting device, to a new paradigm that takes post-connected network admission into account. In this case, devices are continually assessed and more granular access enforcements and other remediation controls are applied to elevate the overall level of hygiene of the devices connected to the corporate network.

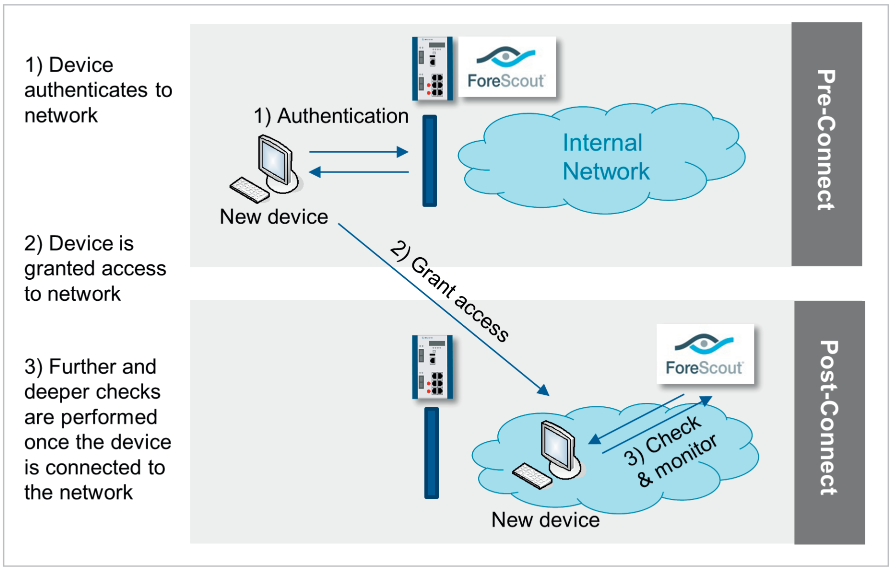
1) Device authenticates to network
2) Device is granted access to network
3) Further and deeper checks are performed once the device is connected to the network
1) Authentication
ForeScout
Internal Network
New device
Pre-Connect
2) Grant access
ForeScout
3) Check & monitor
New device
Post-Connect

Figure 2: Process of device admission to the network

Moreover, network access control software solutions are shifting to become network access orchestration engines. Information is exchanged in near real time with other security and IT solutions such as firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS), configuration management database (CMDB) asset repositories, and identity and access management (IAM) solutions in a bi-directional fashion.

Another important trend is the application of some level of network access orchestration for network segments to mission-critical operational technology networks. This is a new application use case that goes beyond the traditional campus networks and requires the network access control solution to observe new requirements and constraints. This is true for the OT networks just as it is true for other novel application use cases, such as virtualized networks (desktops and servers) or cloud infrastructures, each with its own unique operational characteristics.

In addition to traditional use cases such as enterprise-wide device visibility, guest/non-corporate access management and endpoint compliance, there are emerging use cases gaining traction, such as IoT device discovery and asset management in the context of IT and OT convergence.

Chapter 3 – How Can Network Access Control Facilitate IT-OT Convergence?

One of the key elements for network security is efficient and effective network access control. Controlling which devices can access the network under which circumstances – including which parts of the network specific endpoints can access – drives successful implementation of each network security strategy. An effective network access control solution can address the four major challenges that we discussed above:

Lack of visibility

In addition to restricting network access, network access control can also provide a detailed overview of which devices are actively connected to the network and which devices have been connected to the network in the past. Depending on the solution, assessing the identity of a device can be based on strong credentials and certificates. Moreover, additional constraints can be applied. One example of an additional constraint is the presence of up-to-date antivirus definition files on end-devices. Such information provides much deeper insight into the network's security status. Combining these capabilities with industrial-grade OT switches and routers provides critical visibility – even down to the factory floor where potential attackers may otherwise connect unauthorized devices. Hence, using a network access control solution ensures that operators know exactly which devices are on the network without any guesswork or scanning to determine this critical information.

Convergence of legacy operational equipment and IT technologies

A major challenge in network access control is the heterogeneity of different devices regarding their options for authenticating to the network. Modern devices might support authentication protocols such as IEEE 802.1X, while legacy end-devices may only be identifiable by their MAC address or by logging into them. Hence, without an effective network access control solution that already integrates diverse authentication options, OT administrators are confronted with the task of implementing different kinds of network access control mechanisms for each device. A powerful network access control solution can provide a wide range of authentication options for modern devices as well as for different kinds of legacy devices. This empowers administrators to design more general network access policies and focus on availability instead of spending their time addressing a diverse set of authentication methods for a heterogeneous array of OT end-devices. However, authenticating modern and legacy devices is not sufficient to achieve security for the network because the access decision that is made after the authentication process must also be enforced. Such enforcement must happen as close to the industrial end-systems as possible – at the field level or the factory floor. Hence, powerful industrial switches that support a rich set of endpoint authentication and access restriction options are required to perform this task.

Constant pressure caused by audits and compliance obligations

Asset management and limiting what assets (devices on the networks) can do is a very important aspect of all security standards and regulations related to operating a network. Moreover, assessing the state of all communicating devices (for example, patch level, security configuration, installed software) is an important aspect of documenting the compliance of a network. Effective network access orchestration solutions can support this task by not only limiting the access before a device enters the network but also by continuously assessing the security of a device and by enabling follow-up steps should a device become noncompliant. Such follow-up steps can range from a quick notification to the administrator to completely isolating the suspicious device from the network. In industrial networks, the choice of action always depends on the required availability of the specific device and should be made on a case-by-case basis.

Another important security concept is the zones and conduits concept. It is one of the central aspects of the widely accepted ISO/IEC 62443 [3] standards family as well as other key industrial security standards. The zones and conduits concept mandates the division of an industrial network into separated functional zones. These security zones isolate different independent areas of a plant from each other. Conduits are connections between these zones that facilitate traffic moving from one zone to another. The conduits serve as gatekeepers that tightly restrict which traffic can traverse the boundaries of a zone based on information about the communicating devices or the employed protocols. Typically, zones are implemented as physically separate networks or logically separate virtual local area networks (VLANs [4]). Conduits are typically implemented by firewalls or switches with very restrictive rules and access control lists.

Network access control plays an important role in implementing an efficient zones and conduits concept because fine-grained definition of zones and the assignments to zones can be error-prone and time-consuming. An effective network access orchestration solution can automate many aspects of the zoning and assignment tasks, thereby making the whole process less time-consuming and less error-prone. Enforcing zones and conduits in the network requires industrial-grade firewalls and powerful industrial-grade switches with access control lists and modern endpoint authentication capabilities, such as IEEE 802.1X. However, since this enforcement must happen at the very edge of the network at the factory floor, switches, access points and firewalls must offer industrial redundancy protocols such as the Parallel Redundancy Protocol (PRP) and the Media Redundancy Protocol (MRP), as well as provide IT-grade firewall and switching capabilities. Smoothly integrating industrial-grade communication hardware with an efficient network access orchestration solution provides the necessary components to fulfill the important industrial standards requirements of zones and conduits without losing the capability to use industrial reliability and redundancy features that mission-critical networks require, thereby making complying to the essential industrial standards feasible and manageable.

Necessity for continual uptime

Over the last decades, industrial Ethernet networks have managed to take availability and robustness to an impressively high level. With the advent of redundant ring structures and redundant point-to-point links in combination with the redundant transmission of frames with protocols such as the Parallel Redundancy Protocol, failover times of zero milliseconds are practically achievable. Ring protocols like the Media Redundancy Protocol allow even for a physical failure of a ring node (a switch) and can still maintain connectivity. However, the switches and infrastructure components for building such highly reliable components have been purpose-built with the primary goal of availability in mind. While many of these devices perform their single job of keeping the network up and stable at an impressive level, additional security requirements have often not been the focus of development. Hence, to upgrade an existing high-availability network or to design a mission-critical network to meet today's security requirements requires networking hardware that can both cater to the needs of reliability as well as the needs of security. Moreover, these switches must be integrated in state-of-the-art network access control solutions and must support the collection of security-related networking information so that network connectivity can be managed adequately.

Chapter 4 – Hirschmann and ForeScout Solution in Detail

Today, no single vendor, product or methodology can fully secure plant-wide networks. With the accelerated rate of innovations and the demand to adopt new technologies that contribute to business success without compromising security, agility is becoming a key factor. In order to address the challenges outlined earlier, security practitioners need a solution that can proactively assess, mitigate and reduce risk with as little heavy lifting as possible, and without disrupting manufacturing on the factory floor or any other enterprise operational infrastructure.

ForeScout and Hirschmann teamed up to introduce a best-of-breed solution where the ForeScout platform serves as an overarching network access engine, assessing in real-time multiple variables such as the device identity, ownership/user, integrity and security posture. Network access decisions are translated to fine-grained access and authorization instructions enforced by Hirschmann devices on the factory floor and the network ingress points. Hirschmann, with its proven experience in industrial networks, is uniquely positioned to effectively enforce security within the unique constraints of an industrial environment while maintaining system availability.

The solution consists of the ForeScout visibility and control platform that works in close integration with Hirschmann routers, switches and access points to provide full network access control and network access orchestration. New devices that attempt to access the network can be treated with the full spectrum of market-leading network access control and orchestration features. For example, end-devices can be identified based on certificates and strong per-device credentials before they are granted access to the network. All devices can be automatically assigned to their respective security zones (e.g., a machine-wide security zone or a plant-wide zone), which makes fulfilling the requirement for a fine-grained zones-and-conduits concept, as required by all major industrial security standards, much easier. Moreover, the state and security of the end-devices can be checked and enforced based on a powerful policy engine. This means that properties like up-to-date virus definition files or specific logged-in users can be used as network access criteria. Suspicious or non-conforming devices can automatically be isolated or transferred into a lockdown mode in which the device can fulfill its basic purpose in the plant but cannot be accessed by an attacker.

Network access orchestration can only work effectively if it is enforced at the proper locations in the network. In most cases, this means that enforcement (the lockout of an unauthorized device or the limitation of a non-conforming device's communication capabilities) must be performed directly where the first switch or access point connects to the end-devices. In industrial environments, these need to be high-quality industrial-grade switches, since environmental conditions such as temperature, vibrations and electromagnetic interference can be very harsh. In addition, special industrial protocols are often mandatory. A prime example for such protocols is a set of redundancy protocols that can seamlessly keep the essential processes in the plant running even if parts of the network infrastructure are no longer operational due to physical disruptions or loss of power.

On top of these two requirements, the industrial communication hardware must support up-to-date security mechanisms like IEEE 802.1X for network access control and state-of-the-art packet filtering to enable access control and essential security concepts like zones and conduits. Hirschmann routers, switches and access points excel in all of these three areas, making them a perfect match for a close integration with the ForeScout platform. The combination of both solutions enables effective network orchestration down to the factory floor where network access control has historically entailed a patchwork of different mechanisms, vendors and solutions, at best. Figure 3 shows the components and some of the benefits the integrated solutions provides.

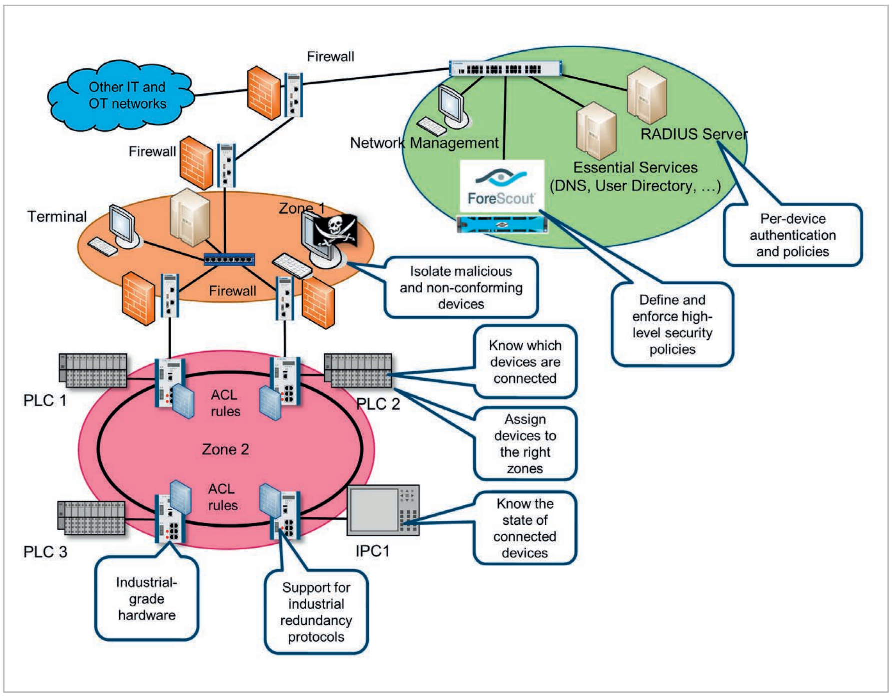
Firewall
Other IT and OT networks
Firewall
Network Management
RADIUS Server
Essential Services (DNS, User Directory, ...)
ForeScout
Terminal
Zone 1
Firewall
Per-device authentication and policies
Isolate malicious and non-conforming devices
Define and enforce high-level security policies
Know which devices are connected
PLC 1
ACL rules
PLC 2
Zone 2
Assign devices to the right zones
ACL rules
Know the state of connected devices
PLC 3
IPC1
Industrial-grade hardware
Support for industrial redundancy protocols

Figure 3: Elements and benefits of the combined ForeScout and Hirschmann solution

Several characteristics make the ForeScout and Hirschmann solution superior to other NAC offerings. These characteristics provide significant benefits to industrial customers:

Continuous device visibility – The platform continuously discovers and monitors device behavior and compliance status as devices come and go from the network. It offers agentless discovery and passive monitoring techniques to avoid disruption of operation. Devices are classified and profiled using multiple feeds and by seamlessly interoperating with the network infrastructure. This allows for a continuous assessment of the security and conformity of the devices in the plant to lessen the stresses of compliance requirements and to provide a tractable benefit to the security of the plant.

No reliance on network-level prerequisites – IEEE 802.1X ensures a strong preconnect network authentication using Layer 2 exchange between the device and the network switch. Hence, IEEE 802.1X is the best solution for network access control in IT as well as OT environments. While Hirschmann devices fully support IEEE 802.1X, ForeScout also works in network architectures without 802.1X. This is a very important property for industrial networks since these networks are often operational for very long time spans and, hence, contain a wide variety of devices with mixed capabilities. Especially in the industrial space, many corporations are facing challenges in ensuring full compatibility with the requirements that an 802.1X implementation necessitates, such as software agents (supplicants) on each device, certificates and a PKI infrastructure for strong authentication and network devices that are fully compatible and properly configured for 802.1X.

ForeScout can also effectively work in a hybrid mode, allowing legacy wired network segments to be controlled without 802.1X in order to reduce disruption in this area, while applying 802.1X authentication in wireless and newer 'greenfield' segments of the network. Hirschmann is also committed to the use of open and established standards and its products can easily be integrated in existing industrial networks based on other vendors' devices. In other words, the combination of ForeScout and Hirschmann is perfectly suited to extend and improve existing networks regarding performance, security and manageability.

Support for networks with heterogeneous end-systems – In the industrial space, it is rare to have networks with end-devices that are entirely based on components of single vendors. Typically manufacturing equipment, sensors and other components are provided by many highly-specialized vendors or are even purpose-built for the plant. The ForeScout platform policy engine can adequately use various network access means such as VLAN assignments and ACLs that are provided by the network infrastructure to securely integrate diverse end-systems. Access decisions are based on rich device context, such as device location, role and ownership, as well as its security posture. ForeScout covers wired, wireless and virtualized networks with a single pane of glass that ensures consistent and complete coverage across any network access point.

In order to best support industrial customers, ForeScout integrated, tested and certified Hirschmann Layer 2 and Layer 3 switch models. This particularly includes, but is not limited to, products that are designed for use in harsh environmental conditions, such as the OCTOPUS switch series or the MACH family of ruggedized switches and routers. Testing and integration have been completed for both the latest HiOS operating system and the Classic Switch Software OS to ensure full compatibility throughout the entire Hirschmann device portfolio, starting from the Classic Basic Rail Switch RSB to the HiOS Industrial Backbone Switch/Router DRAGON MACH 4000.

ForeScout discovers devices that are reported by Hirschmann switches and routers and augments this capability with additional device context that is used to allow, deny or limit network access based on your security policies and applied by switches located at the relevant network zones and ingress points.
This architecture ensures that
conceptual Policy Decision Point (PDP) components are fully integrated with the Policy Enforcement Point (PEP) components, as they are referred to in some of the InfoSec literature.

The combined solution of Hirschmann industrial communication equipment and the ForeScout platform is perfectly suited to address the critical pain points in industrial network security. It is ideal for integrating visibility into existing plants and networks through the use of open standards. It alleviates the pressures of regulatory compliance by allowing enforcement of high-level security policies at the field level. And it ensures the availability of industrial network products and industrial-grade hardware to enforce security at the factory floor without compromising availability.

Chapter 5 – Summary

Today's OT network operators face numerous challenges for planning and implementing a comprehensive network security strategy in industrial settings. These challenges put industrial plants and applications at risk because they lead to degraded visibility into the activities throughout the network and threaten compliance with mandatory standards and regulations.

A powerful network access control and network access orchestration system in combination with industrial-grade, factory-floor-capable network equipment addresses these challenges. In particular, the integration of the ForeScout platform as a security orchestration solution and Hirschmann switches, routers and access points brings next-generation access control down to the very edge of the industrial network.

This solution provides cutting-edge security while retaining proven industrial features such as exemplary robustness and high availability through the use of redundant protocols. The tested integration of both companies' products ensures that network access orchestration can be performed in industrial networks where it matters most: at the factory floor.

References

[1] IEEE 802.1X-2010 – IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control

[2] IETF RFC2865 – Remote Authentication Dial In User Service (RADIUS)

[3] IEC 62443 – Security for Industrial Automation and Control Systems (IACS)

[4] IEEE 802.1Q-2014 – IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks

About ForeScout

For more than 2,900 enterprises in over 80 countries, ForeScout network access control solutions provide intelligent, cost-effective network access control that meet the highest standards for security and regulatory compliance as well as ease of use and deployment.

The ForeScout platform is sold as either a virtual or physical appliance that deploys within your existing infrastructure and typically requires no changes to your network configuration. It installs out-of-band, avoiding latency or issues related to the potential for network failure, and can be centrally administered to dynamically manage up to two million endpoints from one Enterprise Manager console.

Always Stay Ahead with Belden

In a highly competitive environment, it is crucial to have reliable partners who add value to your business. When it comes to signal transmissions, Belden is the No. 1 solutions provider. We know your business and want to understand your specific challenges and goals to show how effective signal transmission solutions can push you ahead of the competition. By combining the strengths of our five leading brands, Belden, GarrettCom, Hirschmann, Lumberg Automation and Tofino Security, we are able to offer the integrated solution you need. Today, it may be a single cable, switch or connector, to solve a specific issue; tomorrow, it can be a complex range of integrated applications, systems and solutions. With the rise in smart, connected devices brought on by the Industrial Internet of Things (IIoT), together, we can make sure your infrastructure is ready to handle and make sense of the influx of data. Transform your business now with instant access to information, and make your vision a reality. Visit info.belden.com/iiot to learn more.

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.belden.com and follow us on Twitter @BeldenIND.