Anybus® BY HMS NETWORKS

Industrial Network Security Solutions

Solutions designed to protect industrial and operational critical infrastructures

HMS

Industrial Network Security Challenges

OT is not just another version of IT

According to the World Economic Forum (WEF), the manufacturing sector stands out as the primary target for cyber attacks, leading to significant downtime and operational disruptions. It's imperative to develop more effective solutions to safeguard against breaches and minimize their impact across all operational environments and critical infrastructures.

With the emergence of new regulations such as NIS2 and standardization initiatives like ISA/IEC 62443, operational organizations are under increasing pressure to enhance their network security measures and protect critical devices.
Operational environments (OT) are different than IT in the way that the quality of the networks is more critical while at the same time networks are traditionally designed to be very open. Machines can be attacked from all sides as thread can enter via IT through Supervisory Control systems, but also via Remote access to the shop-floor or from a site-vistit of a 3rd party connecting to the network. With flat designed networks it's common that a single small thread can spread quickly infecting a whole plant can resulting in significant downtime.

The Purdue model – commonly referred to as a reference architecture of a Defense in Depth strategy designing an architecture to keep IT systems far away from OT – is not only often badly implemented, it's also guiding for open levels. This results in a vulnerable architecture allowing infected machines to quickly spread their threads to other machines and systems in the plant. This increases the impact by resulting in more downtime and often significantly longer recovery time as well.

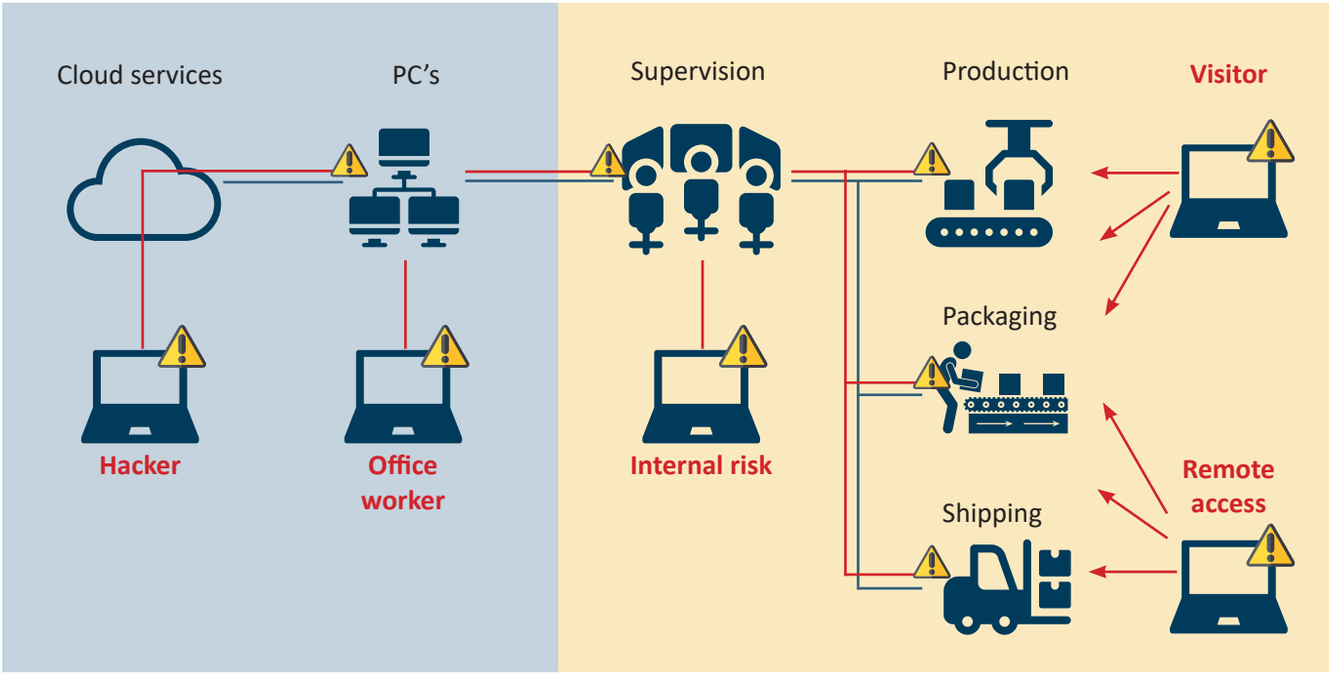
NIS 2

IEC International Electrotechnical Commission

ISA GLOBAL CYBERSECURITY ALLIANCE

Navigating network vulnerability zones

In industrial networks, vulnerabilities exist at every junction. These critical zones demand our attention as we protect against cyber threats. Beyond the fortress walls, cybercriminals probe firewalls and exploit exposed services. The DMZ acts as a buffer between external and internal networks, hosting public-facing services but also posing risks. Within the internal network, employees and visitors impact security. Safeguarding these zones requires vigilance and education.



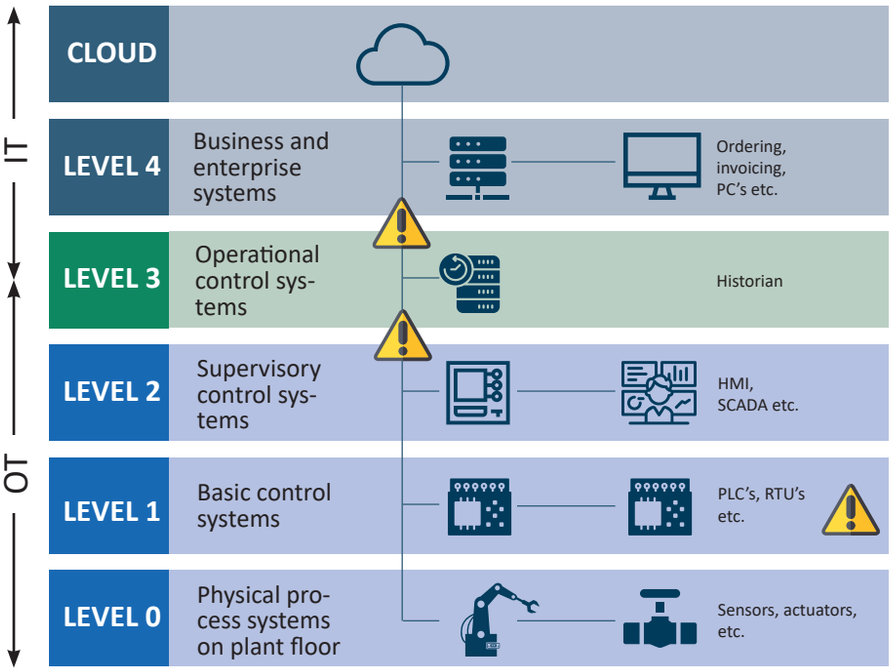
Common architecture - Purdue Model

Defense in depth

- Layered model to keep access to "OT" as far away as possible
- 'Easy' to enforce access controls between without hindering business

Good theory but in reality:

- # of layers depends on maturity
- Poor border control creates flat network in reality
- Not considering size and complexity of "OT" side



Industrial Network Security Solutions

Anybus is the world's most widely used product family for industrial network connectivity. Anybus devices enable communication between machines and segment networks, thereby offering enhanced control and ensuring that industrial networks remain safeguarded and optimized for uninterrupted operation.

Network Security Use-Cases

1. OT/IT segregation: Enforce strict policies for domain separation, with a defence in depth strategy and up to 10 Gig Ethernet connectivity.

2. Address conflict avoidance: Manage IP addresses efficiently thorough implementation of Network Address Translation (NAT) and routing scenarios. Add filtering to control what traffic can pass through and what should be blocked.

3. Deep packet inspection: Ensure security of industrial protocols with deep inspection and gatekeeping, enabling capabilities to allow certain transition but not others. E.g. Allow PLC reprogramming only between 06:00 and 08:00, but not during operations.

4. IEC62443 compliance: Implement security zones and conduits according to industry standards for precise machine isolation and reduce impact on breach by stopping bi-lateral movement.

5. Secure plant-to-plant OT connections: Establish encrypted links between facilities using WireGuard®, OpenSSL, and IPsec Virtual Private Network (VPN) protocols. Use redundant WAN and enhanced routing functions and control centrally on a Cybersecurity Console.

Solution Essentials

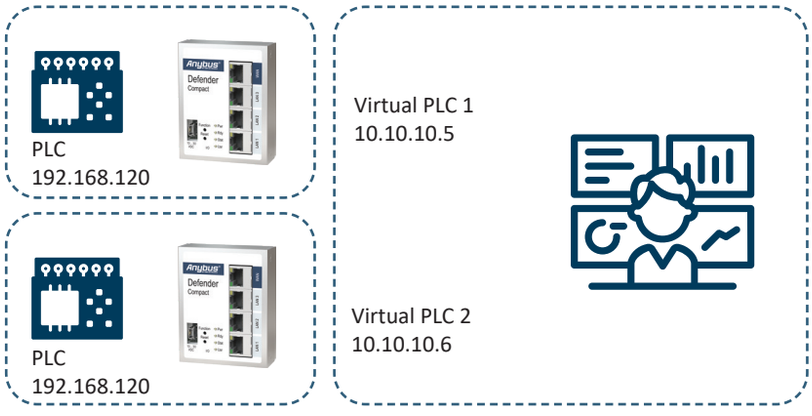
1. Central management: Anybus network security soluton is available with a central management console providing access to manage the security posture as well as view intelligence centrally

2. Network and asset insights: Asset detection and inventory features built into the Defenders enables deeper visibility of what's connected to your network and design security policies accordingly.

3. Diagnostics & threat detection: Detect all anomalies causing downtime, security and faults. Enable a pro-active scan of the security configurations of your assets.

Case Study 1: Simple NAT and protection

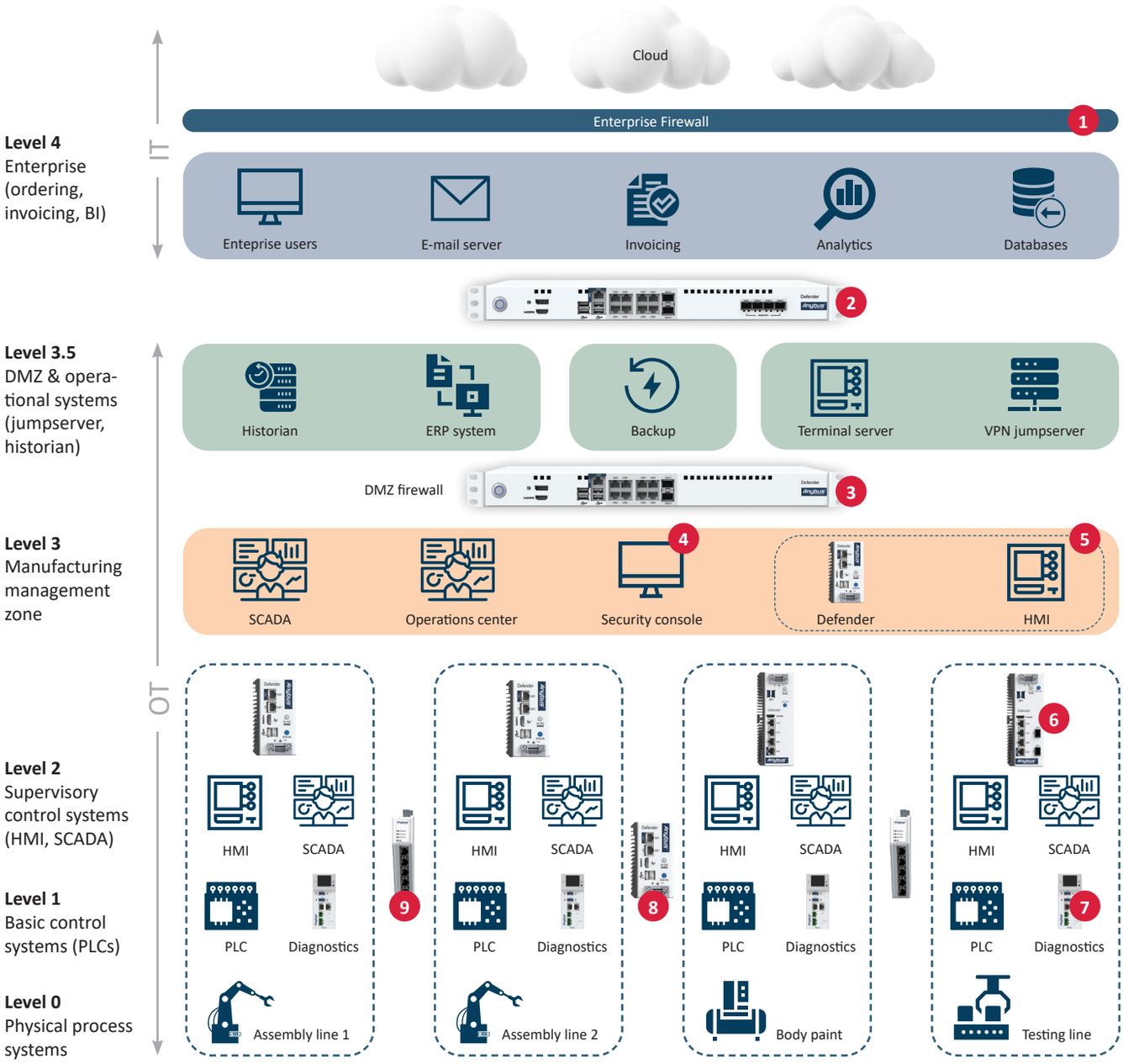
A common problem is overlapping IP address space usage between machines or production lines. Network Address Translation can be applied for shop-floor assets that need connectivity to higher level control systems. At the same time as traffic filtering can be applied to apply a secure-by-default architecture.



PLC with same IP address can not be on the same network. Anybus Defender Compact preforms a Network Address Translation to virtually represent each PLC on a common network, so that it's accessible from other systems like a SCADA or HMI.

Case Study 2: Segmentation in Manufacturing

A large factory with extended industrial automation is advised to separate their machines and lines in separate zones, implementing firewalls and gateways between them as conduits. This follows the ISA/IEC 62443 model and lowers the threat surface resulting in lower risk and reduced impact. North/South is controlled by Industrial Firewalls inspecting and controlling all traffic. East/West by Coupler Gateways allowing only industrial protocol content to be transferred, blocking all other IP communication between zones.



1. *Enterprise Internet Firewall*

2. *OT/IT Separation Firewall with high speed up to 10 Gbit/s interfaces. Different brand as Enterprise FW for best practice Defense in Depth strategy.*

3. *Demilitarized Zone firewall securing OT supervisory zone while ensuring data transfer capabilities to IT*

4. *Central Cybersecurity Console enabling central supervision of all Defenders, manage configuration backups and control policies in groups.*

5. *Vulnerable system protection with virtual patching strategy and DPI.*

6. *Industrial Firewall as Conduits separating assets in Zones according to 62443 best practice model.*

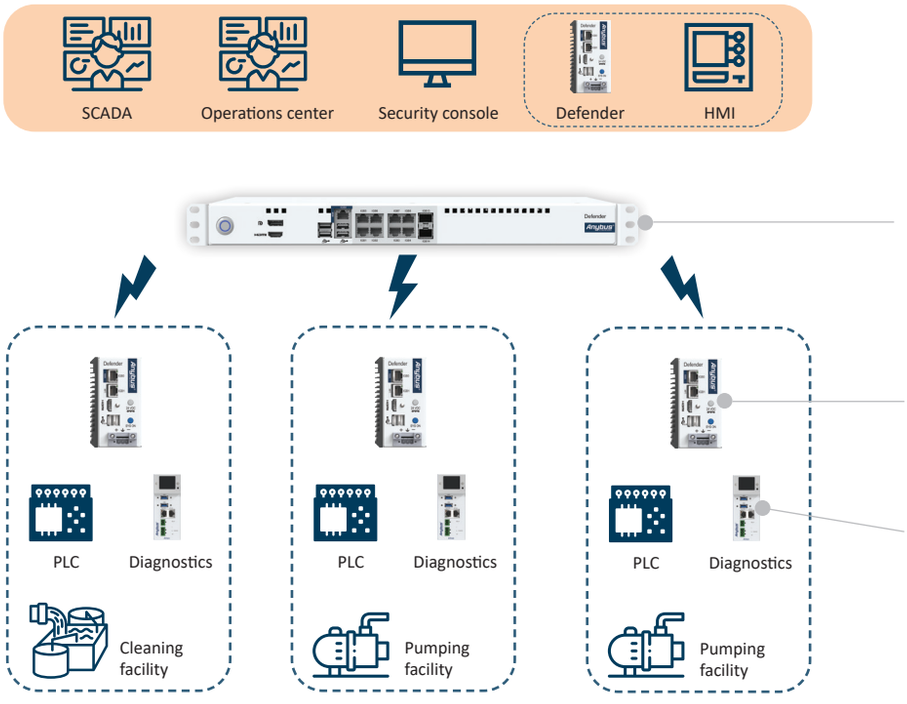
7. *Diagnostics and security monitoring enabling pro-active action on threads and faults.*

8. *Industrial Firewalls as DPI gateway enabling screening inside industrial protocol transactions*

9. *Gateways as Couplers connecting Zones securely without any risk of other traffic transferring.*

Case Study 3: Water treatment

In distributed environments such as water treatment facilities, individual sites need protection from external intruders. Additionally, secure connectivity must be maintained with the central control center. An OT-SDWAN integrated into Anybus Defender can easily facilitate this using modern VPN technologies like WireGuard©, all centrally managed from the Anybus Cybersecurity Console.



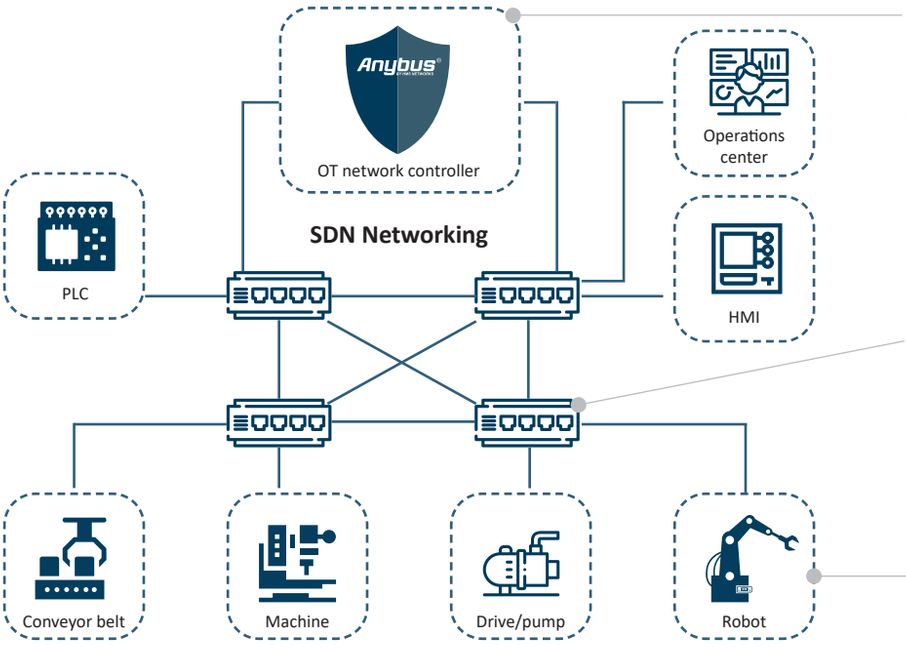
OT Firewall with VPN Concentrator, IPsec, OpenVPN or WireGuard© compatible. Enable remote user access too, if desired.

Industrial Firewalls as VPN spokes and Network Address Translators. Access control lists and Deep Packet Inspection guarding what traffic can pass through.

Diagnostics and security monitoring enabling pro-active action on threads and faults.

Case Study 4: Small/Medium Manufacturing

A small factory using Software Defined Networking technology to isolate each asset individually on a layer 2 level. The centralized OT Network Controller manages the access lists for each port on the Open-Flow compatible switches and receives continues updated on flows present in the network.



The OT Network Controller keeps central control of all the policies on who can allow to talk to whom with what protocol.

Any OpenFlow Ethernet switch is compatible, implementing policies on every port for micro segmentation.

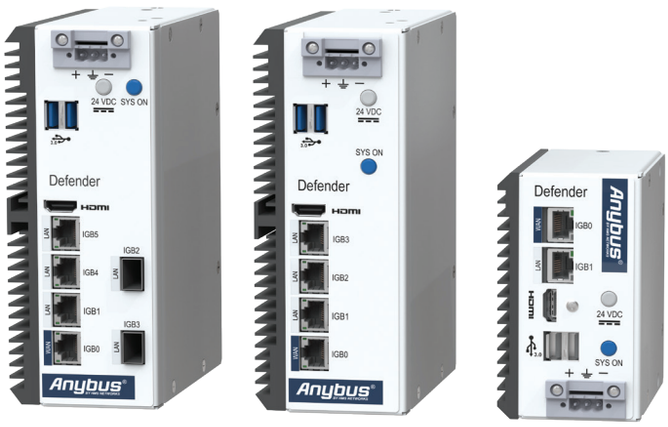
Each asset is isolated and traffic to and from is managed on a protocol level. Moving assets around is easy as the policy is instantly transferred to the new port.

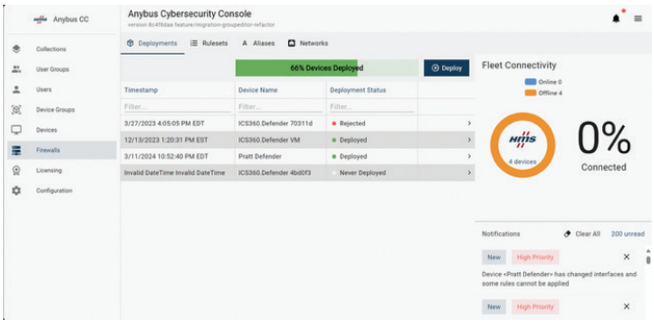
Anybus Network Security Portfolio

Anybus Defender

The Anybus Defender is a range of industrial network security appliances enabling:

- Optimized segmentation, follows NIS2 guidelines for robust network segmentation
- IEC62443 Compliance: Establishes zones and conduits for precise machine isolation
- Access Control: Utilizes Deep Packet Inspection for granular control of industrial protocols
- Secure Plant-to-Plant Connectivity: Ensures secure OT connections with simplified VPN technology
- Range of DIN rail and 19” Rack mount models with connectivity up to 10 Gig Ethernet





Anybus Cybersecurity Console

- Centralized system management app for Anybus Defenders
- Easy-to-Use modern web UI interface
- Monitor operational and protective states of a network
- Adopt existing configurations and handle backups centrally
- Firmware and extension package depository and centralized license information

Anybus Defender Compact

Highly compact industrial firewall that offers protection against attacks by segmenting the production network into manageable and logically separated sections. Both bridge and Network Address Translation (NAT) mode are supported providing key use cases. PLC Like configuration GUI, ideal for machine builders hard configured border gateway.

Enhancing security with micro-segmentation

The Anybus OT Network Controller revolutionizes Zero-Trust network management through its tailored Software Defined Networking (SDN) technology, meticulously crafted for Operational and Critical environments. By seamlessly integrating with any Layer 2 OpenFlow switch, the central controller assumes complete command, offering unparalleled visibility and control over network traffic. This ensures stringent regulation of permitted devices and traffic, fortifying the network against potential threats.

Secure Conduits with Communicators

Anybus Communicators establish highly secure connections between machines through streamlined conduits. They ensure utmost security by exclusively transferring industrial protocol data, without allowing any IP packets to pass through. These devices are fortified with physical lockdown features, offering peace of mind and facilitating uninterrupted east-west communication across security zones

Security Insight and Proactive Intelligence with Diagnostics

Anybus Diagnostics offers comprehensive visibility into industrial devices, their behaviors, and network quality. It conducts security health checks to ensure devices lack unnecessary open ports and access points. Instant notifications are triggered for device alterations or abnormal traffic patterns, while predictive analysis foresees potential quality impairments, preempting costly unplanned downtime.

Work with HMS.
The number one choice for Industrial ICT - Information and Communication Technology.

HMS Networks - Contact

HMS is represented all over the world.
Find your nearest contact here:

www.hms-networks.com/contact