BELDEN

12 Reasons for NAC in OT

I Can Only Protect What I Am Aware Of

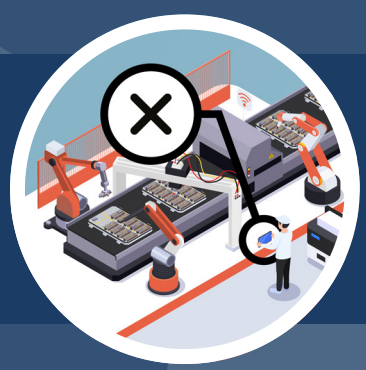
The overview and segmentation of the entire network and all connected assets supports the concept of security zones.

The Plant Availability is the Top Priority

A NAC system should not specify fixed implementation strategies, but must allow sufficient freedom to maximize the radius of action of a NAC. At the same time, a NAC must not conflict with consistently high plant availability to ensure business continuity.

Sustainable Implementation of the Safety Strategy

Heterogeneous IT/OT networks require flexible and future-proof software solutions. A NAC system does not require extensive hardware upgrades in the network in order to achieve a high level of sustainability.



Unwanted Devices Stay Out

In a hardened OT environment consisting of various OT specific end devices (e.g. robots, PLC), cybersecurity solutions have to prevent unknown end devices from obtaining a connection that could negatively influence the production plant.

Detection of Unwanted Network Events

By monitoring a wide range of network events, undesired behavior will be identified immediately, whether caused deliberately or unconsciously. Possible critical network events (e.g. duplicate IP addresses) are detected in order to take proper countermeasures automatically or manually.

Legal Requirements

Regulatory requirements, such as ISO62443/ISO27001/ISO9001, demand reliable enforcement of corporate policies for all areas of the network. Information from third-party sources, such as OT Visibility or DPI Solutions can be used to automatically isolate detected threats.

Automatic Transfer of Access Authorizations

In the event of an authorized exchange of terminal devices, access authorizations should be transferred securely and dynamically to new devices that need to be integrated.

Compliance Requirements

Most OT assets cannot be protected by conventional technologies such as endpoint security, but even Non-IT assets must meet certain compliance requirements. In the event of a compromise, immediate and targeted alerts and responses must be initiated.

Time-Limited Access to Specific Network Areas

An external company (e.g. technical service provider) requires time-bounded access to very specific network areas for defined end devices (e.g., notebooks, control devices).
Any access beyond this should be automatically prevented.

Granular Access Control or Automatic Exclusion

Unauthorized network devices or end devices (such as private routers brought into the enterprise, unmanaged switches, or private tablets) have to be excluded automatically from the network communication or given limited access.

Device Localization

A handheld scanner or programming device has been lost. It must be possible to have a quick and easy view of the communication history of this device in order to be able to initiate correct and targeted measures in the shortest time possible.

Reduction of Administrative Effort

In addition to their core function and despite the massive increase in threats to networks, security solutions need to keep the associated administrative expenses down in order to maintain a high level of acceptance within the company.

macmon nac

Overview Control and Security in the Network