SIEMENS

Technical article

Industrial Network 4.0

Software solutions make a significant contribution towards saving costs

Digitalization generates a multitude of customer benefits, but also poses challenges for industrial communication networks. Security-relevant standardizations – such as IEC 62443 or IEC 61850 – also play an increasingly important role and must be taken into account for a sustainable industrial network. Software solutions make a significant contribution towards that – reducing commissioning times and maintenance phases.

An industrial network for different applications

To achieve the goal of making industrial companies future-proof, new ways and possibilities have to be created. These begin with the expansion of the networking of sensors that are to transmit production data for further processing to central databases (e.g., cloud) or can also increase flexibility (e.g., provide data for different applications). These are just two examples that have developed due to digitalization. In this context, the topic of virtualization should not be ignored, either. Virtualization offers the key advantage for industrial facilities, and generally the applications of the future, to gain greater flexibility and scalability. For example, new applications can easily be created via additional virtual instances and exchange data with the industrial facilities. An industrial communication network will also have to deal with all of these issues in the future. Furthermore, industrial communication networks must offer a high degree of flexibility and adaptability in order to meet the challenges of the future.

Collaboration between IT and OT worlds – lowering investment costs for industrial facilities.

Compliance with IEC standards

Especially in industrial communication networks, though, there are additional requirements. There are additional standards existing in various industries that must be adhered to (such as IEC 61158 / IEC 62443 in the field of machine construction and manufacturing and process industries, or IEC 61850 in electrical switchgear). These standards also include specifications that in particular affect the definition of the network architecture. Take for instance the IEC 62443 standard, where the topic of strict network separation between the corporate network (IT network) and the production network (Operational Technology – OT network) is described. Another example is the IEC 61850 specification, which defines corresponding communication protocols (such as MMS for data communication and GOOSE telegrams).

All of these aspects need to be considered when creating a network infrastructure for an industrial communication network. In addition, the topic of "security" – i.e., network security – must of course not be disregarded. In many cases, however, it is neglected as it is considered to be too cumbersome and too complicated. But there are reasons why such security-related approaches exist – including user management, encrypted data protocols, and secure authentication. Paramount to all of these security requirements is primarily the protection of industrial networks against unauthorized access and manipulation.

Collaboration between IT and OT worlds

Another point that must be taken into account in industrial communication networks pertains to the central "company policies". Company policies are rules and specifications (e.g., certain ports have to be blocked, passwords must meet certain security features) that are set for the company by the central network administrators and that must also be taken into account in the industrial communication network. Coordination with the company's network administrators is necessary for this to jointly determine the responsibility for the network transitions between the IT and OT networks. Security is a success factor for digitalization not to be underestimated.

Once the network concept has been devised, it is time to think about what software and hardware products to use. There are many manufacturers on the market whose product range extends from hardware components (e.g., switches, routers, modems, firewalls, wireless LAN access points) all the way to software products (e.g., network management systems – such as SINEC NMS for managing the hardware, RADIUS servers for device authentication in the network, or syslog servers for transparency of events occurring in the network).

Regarding the hardware, it bears mentioning that in the meantime all manufacturers are offering a comprehensive portfolio with very extensive feature sets. This means that the hardware products hardly differ functionally from one another. Rather, the software solutions will make the difference in the future.

Network management for industrial networks

The simplicity of operation (reduction of network complexity) and the lowering of operating costs (operational expenditures) play roles that should not be underestimated, especially when it comes to managing networks. Not only is the network itself of importance for industrial communication networks, but especially the end devices are very important. Only in concert with the end devices can a complete overview of the industrial facilities be obtained, and a premature failure be recognized and prevented thanks to correlated information. This is achieved by correlating the network information together with the end device information in the analysis.

Especially in industrial applications, however, there are many other aspects that are very important in this interaction. For one thing, industrial facilities grow again and again due to the installation of new machines. Consequently, these new machines must also be integrated and tested: Has the machine been configured in accordance with the specifications (e.g., IP address, device name, correct firmware version)?

The time and effort involved in testing is sometimes very complex and involves a lot of manual labor. There is an increasing desire here for such machines or facilities to be automatically tested and documented utilizing an acceptance protocol. In addition, there is the need for scalability in the software products: So that additional machines can be integrated into ongoing operations without great effort.

Another important point is the ability to obtain a complete inventory list of all devices at the push of a button, i.e., a central overview of which components (e.g., network components and end devices) are installed including their respective firmware version. This not only applies to a single manufacturer, but to all components in the industrial network across manufacturers.

The topic of central firmware management must also be taken into account. With an overview of which components run which firmware version, unauthorized firmware versions used in industrial facilities can be quickly identified as well as devices that need to be upgraded to the current firmware version.

SINEC NMS is flexibly scalable and can depict industrial networks of all sizes, manage them centrally, and configure them based on rules – including security-related aspects.

With SINEC NMS – increasing productivity of industrial facilities.

But already a phase earlier, i.e., before the ongoing operation of an industrial network, the requirements are changing as networks become increasingly complex due to the advancing digitalization. For instance, the basic initialization of devices in industrial facilities is becoming more and more of a challenge because the initially required basic settings are made individually for each new device – which is cumbersome. This includes, e.g., the assignment of IP address and device name as well as activation and deactivation of SNMP or services (such as DHCP client, NTP client). Here, one desires small, compact helper tools that are intuitive to use and with which one can quickly and simultaneously commission several devices in parallel.

The SINEC PNI (Primary Network Initialization) tool simplifies and reduces the time required for the initial commissioning of network components in industrial networks.

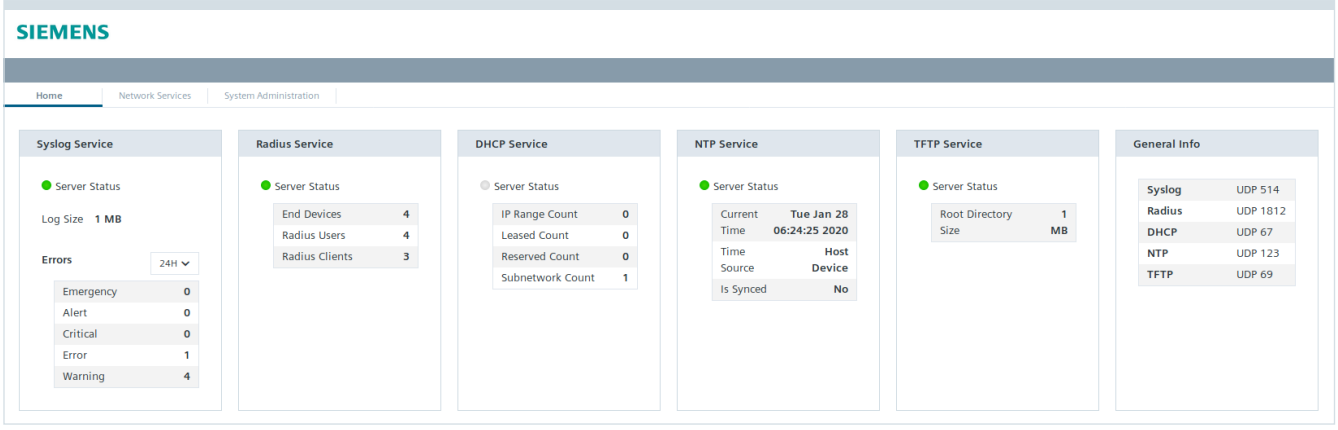
Quick and simple installation of all necessary services

In today's security concepts, a secure network access plays an increasingly important role. When it comes to access to the industrial network, it should be made sure which applications and devices are to be given access at the industrial network. Access by applications and devices can be protected via firewalls between the network segments, or the specifications from the IEEE 802.1X standard can be used to regulate access by devices directly in the industrial networks.

An equally valuable point from a security perspective is to track the events in industrial facilities in order to identify possible irregularities in the industrial networks. For this, "syslog messages" are primarily used. Each component sends its events (e.g., User A has logged in to Device B at dd.mm.yyyy hh:mm:ss) to a central syslog server. All events are saved there and can be used for further analysis.

In addition, certain network services are consistently required for a holistic network approach throughout the entire life cycle for the maintenance and upkeep of the network. A central infrastructure server that combines different services in one instance would be ideal here.

SINEC INS (Infrastructure Network Services) simplifies the installation and management of all services necessary in an industrial network in a single tool.



SINEC INS includes all services necessary in a single user interface – reducing the effort for installation and management.

Conclusion

With the new SINEC software family, Siemens has the right answer to all of these topics in the different phases centered around the industrial network. From initial commissioning of new devices to monitoring and management of an increasingly complex network – including all software services necessary for an efficient network operation. Here, it is particularly convenient that the products are scalable and interact with each other. This makes a significant contribution towards reducing OPEX (e.g., reduced maintenance costs) and readies industrial companies for the digital future.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. For additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Technical article
DI-PA-1920-14
PDF 0420 5 En
Produced in Germany

siemens.com/sinec