## Upcoming technologies

There are a number of technologies that will shape the future industrial communication landscape. Perhaps the strongest trend is that IP (Internet Protocol) will emerge as the main information carrier in tomorrow’s smart and interconnected industry. Furthermore, several new communication protocols will be used in parallel with existing networks. Here are some of the communication technologies that will shape the communication landscape of the future, and how HMS will support them.

### OPC UA
OPC Unified Architecture (UA) is a service-oriented industrial communication standard for secure and reliable data exchange. OPC UA is platform-independent and ensures a seamless flow of information among devices from multiple vendors. It defines services for data exchange between Clients and Servers including access to real-time data, monitoring of alarms and events, access to historical data and other applications. The standard is managed by the OPC Foundation.

OPC UA is today applied in a wide range of applications and solutions stretching from straight-forward M2M communication to new upcoming solutions like IIoT bridging and cloud connectivity. As any other IP based communication protocol, OPC UA can co-exist with other industrial protocols on the same network, complementing real-time control with a secure and service-oriented data channel.

HMS has recognized OPC UA as one of the most important protocols for data and information exchange within the smart industrial solutions of the future. As a result, OPC UA will be supported by industrial Ethernet modules within the CompactCom series, starting with EtherNet/IP and PROFINET.

### MQTT
MQTT (Message Queue Telemetry Transport) is a publish/subscribe messaging protocol ideal for IIoT bridging and IIoT solutions. Based on its light-weight and straight forward approach, it has become one of the most popular protocols enabling industrial data and information exchange.

MQTT is based around a message broker to which industrial devices (clients) connect. The clients exchange information via the broker based on topics with a flexible syntax. The broker uses the topics to decide which clients to receive a message.

Compared to OPC UA, MQTT is more flexible and easier to implement. On the other hand, it lacks the data, service models and security schemes provided by OPC UA.

HMS has recognized MQTT as one of the most important protocols for data and information exchange within tomorrow’s smart industrial solutions. MQTT will be supported by industrial Ethernet modules within the CompactCom series, starting with EtherNet/IP and PROFINET.

### Time-Sensitive Networking (TSN)
TSN (Time-Sensitive Networking) is a set of IEEE 802 Ethernet standards that enable deterministic real-time communication over standard Ethernet infrastructure.

TSN extends Ethernet with functions like time synchronization, network scheduling and time-based queues which provide guaranteed latency and delivery of scheduled real-time traffic in a network.

TSN addresses important topics like redundancy, bandwidth reservation, preemption and network topology/path functions. A major driving force behind the development of these new TSN standards is the automotive Ethernet market.

HMS R&D is evaluating and testing different solutions for TSN.

### Security technologies
Security is one of the main challenges within IIoT as connecting “things” to the Internet also means that they are subject to increased security risks. Many of the major industrial network organizations are currently underway with developing security standards. HMS follows and takes active parts in many of these developments.

### Different initiatives for smart manufacturing
Today, there are several major ongoing initiatives around the world about how to bring IIoT into factories and how to connect operational technology on the factory floor with enterprise systems. Examples of these include Industry 4.0 (Germany), The Industrial Internet Consortium IIC (North America), Industrial Value Initiative IVI (Japan) and Made in China 2025 (China).

These initiatives focus on improving quality and reliability as well as increasing flexibility in manufacturing, and this will also enable new, innovative business models in the future.

### What is the basis for this?
A data pipeline is established to harvest data from the factory floors so that it can be analyzed in the outside world. The data is transferred via the existing standard industrial network cabling, but bypasses the traditional control system, using new IIoT protocols like OPC UA and MQTT to syphon the data up. This means that the existing industrial networks do not only provide normal day-to-day control but also serve as a backbone for the data and the IIoT functionality.

For example, we are currently developing and evaluating support for technologies such as:

- **TLS** (Transport Layer Security)
- **HTTPS** (Secure version of HTTP)
- **FTPS** (Secure version of FTP)
- **CIP Security™** (An initiative from ODVA defining security-related requirements and capabilities for CIP devices, specifically EtherNet/IP devices. CIP Security is currently under development and HMS is working with ODVA to develop support.)

### Safety networks
Safety networks have been a hot topic on the industrial network market for some time and is now becoming increasingly adopted on factory floors around the world. Anybus CompactCom is equipped with a Black Channel which enables transfer of safe signals over PROFINET (PROFIsafe), EtherNet/IP (CIP safety) and Functional Safety over EtherCAT, FsoE.

HMS offers a specific safety module, the IXXAT Safe T100, which substantially speeds up the integration of safety into an industrial product. Also, HMS has safety stacks for CIP-Safety and FsoE.

This means that HMS offers several ways to implement integrated safety depending on how much customization you want.
A changing view of security

Traditionally, security in industrial control systems has been based on the fact that these systems are isolated and not connected to other systems (including the Internet). Therefore, there has not been a great need to add security to the control network itself. Until now.

The control networks are undoubtedly getting increasingly connected to the outside world — and thereby also a target for hackers, espionage, sabotage and data manipulation. Hence, it becomes increasingly important also for the devices and machines on the factory floor to defend themselves. This is why several industrial networks now are developing security standards.

These standards enable machines to:

- Reject data that has been altered (Integrity)
- Reject messages sent by untrusted people or devices (Authenticity)
- Reject messages that request actions that are not allowed (Authorization)
- Protect sensitive data (Confidentiality)
- Be robust against high traffic loads and malformed packets (Availability)

Methods HMS uses to keep data safe

Security is a key integral part of product development and maintenance at HMS. We continually test our products using industry standard test suites to check resistance against packet storms (to prevent, for example, denial-of-service attacks), known security holes and malformed packets (fuzzing attacks).

In this process, we use tools like Achilles, Netload and Nessus for our Ethernet-based products.

Also, all Anybus CompactCom 40-series firmware files are validated with signed firmware certificates, ensuring that the firmware is authentic and unmodified.

Access control is another important security feature, giving only selected users access to Anybus CompactCom features such as web servers, FTP, firmware updates, etc. Access can also be shut down completely.

Unused protocols and functionality can be disabled as necessary by the host application.

In full technology control

Using our own technology, we are in full control of the design, allowing us to optimize performance and fix possible vulnerabilities easily.

Furthermore, HMS participates in the network user organizations and work together with leading customers on cyber security.

Security in product development

HMS has a well-established development process that is ISO9001 certified. HMS internal security guidelines make sure the security aspect is included from start.

All source code is reviewed by programmers trained in secure coding technologies.

SECURITY IS AN ONGOING PROCESS

“Everybody who works with security knows that the work is never completed — it is an ongoing activity. HMS works continually with keeping our products secure and up to date with the latest standards, trends and technologies.”

Magnus Hansson
Global Systems and Security Manager, HMS Industrial Networks

How we keep data safe

As more and more machines go online, security is perhaps the biggest challenge of industrial networking. That’s exactly why it is important to work with solid and secure communication solutions like Anybus. Here is how HMS works with security in Anybus CompactCom. Now and in the future.