
STATE OF INDUSTRIAL NETWORKS *2026*

Market overview, trends
and recommendations



Hardware
Meets
Software™

CONTENTS

NETWORK MARKET SHARES 4-5

Annual estimated distribution of newly installed nodes

THE BEST NETWORK? 6-7

The network debate nobody wins
[and that's okay]

SURVEY CONCLUSIONS..... 8-11

The next industrial network will not
be one network

VOICES AROUND THE GLOBE. 12-13

Industrial networking, region by region

TOTAL COST OF OWNERSHIP..... 14-17

The hidden cost of in-house connectivity

ELOTECH CASE STUDY 18-19

PROFINET in six weeks, EtherNet/IP in two days

CYBERSECURITY..... 20-22

From awareness to execution!

The market is talking. Are we listening?

For more than a decade, the conversation about industrial networks has been a numbers game. Which protocol is up? Which is down? Which standard will win? Those questions still matter, and you will find the latest answers in the annual market shares on page 4. But anyone working in industrial automation today knows the real questions have moved on. This year's survey makes that shift impossible to miss. When industrial designers and users are asked what keeps them up at night, the top answers are not

bandwidth or latency. They are vendor compatibility and cybersecurity. When asked about the future, they do not point to a single winning protocol. They describe a layered stack where deterministic Ethernet, OPC UA, MQTT, wireless and security all need to coexist. And when asked about new technologies, they separate practical value from hype with a discipline that should humble anyone selling a revolution. That is why this report exists. The numbers tell us what is happening. The market tells us what matters.

Both are needed. The chapters that follow draw on the second edition of our Future of Industrial Networks survey, regional voices from four continents, an industry leader interview, and a hard look at the total cost of ownership behind every connectivity decision. We do not have all the answers. But the people building, specifying and operating tomorrow's factories do, between them. Our job is to ask the right questions, listen carefully, and pass on what we hear.

Turn the page.

ABOUT THE AUTHORS



Thierry Bieber
Business Developer

Thierry Bieber is a Business Developer at HMS Networks, specializing in industrial communication interfaces and IIoT solutions. With over 25 years of experience, he drives business development and market expansion within the industrial automation sector.



Magnus Jansson
Director of Product Marketing

Magnus Jansson is Director of Product Marketing at HMS Networks, with over 18 years of experience in industrial communication and automation. He leads strategic marketing initiatives, driving innovation and growth in the industrial sector.



Dr. Jens Jakobsen
Product Security Manager

Dr. Jens Jakobsen is Product Security Manager at HMS Networks, leading work to strengthen the cybersecurity of industrial communication products. He brings experience from Schneider Electric and Motorola, and holds seven patents in industrial communication.

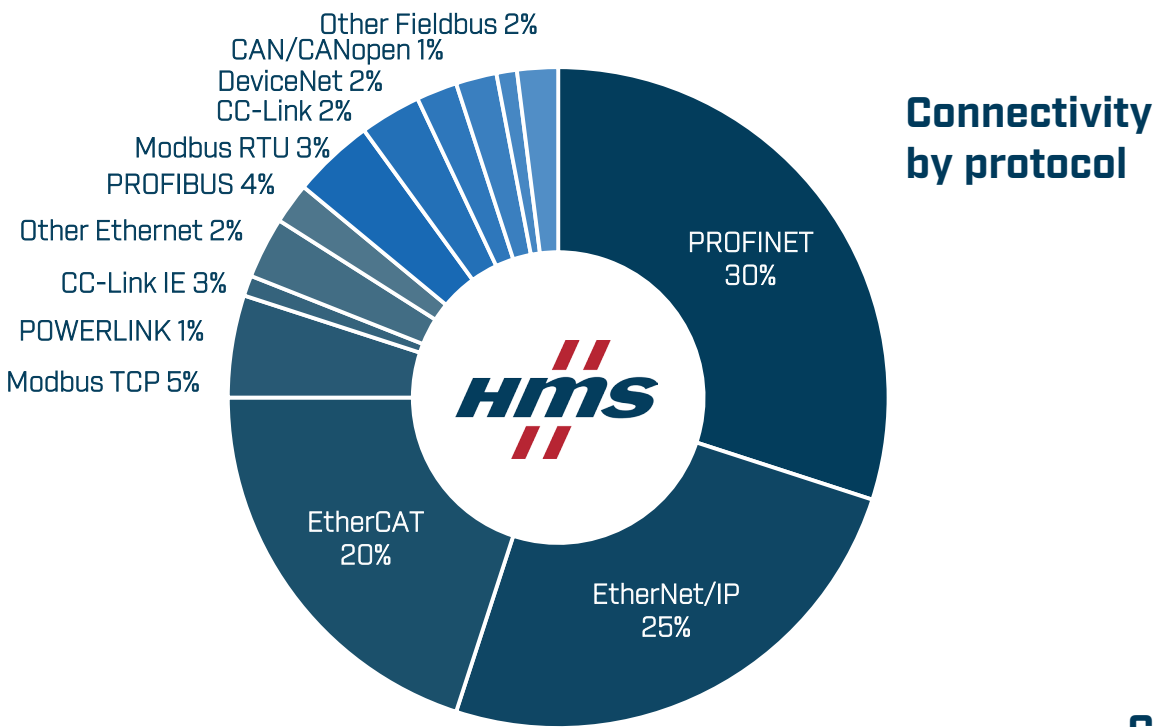


Mark Crossley
Marketing Content Specialist

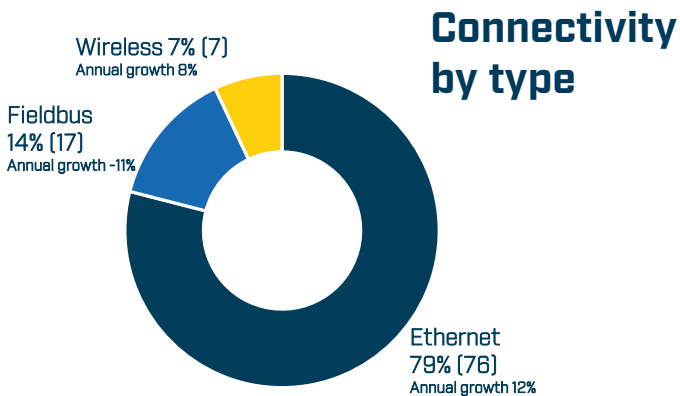
Mark Crossley is Marketing Content Specialist at HMS Networks, where he has worked across technical documentation and product content. He brings a background in technical writing for Ericsson's packet core products and holds a degree in IT forensics and information security.

Industrial Ethernet in Eight of Ten New Nodes as Fieldbus Decline Accelerates

HMS Networks has released its annual analysis of the industrial network market, marking twelve consecutive years of tracking how factories and machine builders connect their automation systems. The 2026 study shows that the long-running shift from traditional fieldbus technologies to Industrial Ethernet has continued through another full year, with Industrial Ethernet now accounting for 79% of newly installed nodes worldwide, up from 76% in 2025 and just 34% when HMS first began publishing these figures in 2015.



The HMS Networks analysis is based on a combination of market insights, internal data, and input from key stakeholders in the industrial automation industry. The study focuses on newly installed nodes in factory automation worldwide, each node being a device or machine connected to an industrial control network. This is the twelfth consecutive year HMS Networks has published this annual analysis.



After the slowdown of 2024, the market stabilised in 2025. Component availability has returned to normal levels and inventory cycles in highly automated sectors have largely been worked through. While Europe's automotive sector continued to face headwinds, broader manufacturing activity recovered modestly, and capital spending on new automation projects resumed in most regions. The 2026 study confirms HMS Networks' expectation of approximately +7.7% average annual growth in newly installed nodes over the next five years, with continued migration of the remaining fieldbus install base to Industrial Ethernet driving much of that expansion.

INDUSTRIAL ETHERNET REACHES 79% OF NEW INSTALLATIONS

The 2026 analysis shows that Industrial Ethernet now accounts for 79% of new nodes, up from 76% in 2025. The three leading Ethernet protocols continued to consolidate their position, together representing roughly three-quarters of the wired protocol market.

FIELDBUS DROPS TO 14% AS PROFIBUS DECLINE

Fieldbus technologies now represent 14% of new nodes, down from 17% in 2025. PROFIBUS & PROFINET International's own published figures showed PROFIBUS new-node installations dropping from 1.1 million in 2024 to 1.0 million in 2025, a 9% decline corroborated by HMS Networks' internal data and by HMS's industry survey.

WIRELESS REMAINS STEADY AT 7%

Wireless technologies continue to connect 7% of new node installations, unchanged from 2025. Wireless retains its established role as a complement to wired industrial networks, particularly

valuable for mobile equipment such as AGVs (automated guided vehicles) and AMRs (autonomous mobile robots), retrofitted machinery, and IIoT sensors in hard-to-reach locations.

5G remains an area of significant interest but slow industrial deployment. The complexity of private 5G infrastructure is the most commonly cited barrier. Early industrial 5G deployments continue to grow, particularly in Asia, but the technology has yet to deliver the breakthrough adoption many in the industry expected.

REGIONAL INSIGHTS

Europe: PROFINET and EtherCAT continue to lead, with strong activity around APL (Advanced Physical Layer) for process automation and SPE (Single Pair Ethernet) for sensor-level connectivity. PROFIBUS decline is most visible in Europe, where the install base is largest and the migration to PROFINET most advanced.

North America: EtherNet/IP remains the dominant protocol, particularly in automotive and discrete manufacturing. Adoption of IO-Link, APL and SPE is gaining clear momentum, supported by interest in OT cybersecurity ahead of the regulatory landscape taking shape around CRA and IEC 62443.

Asia: PROFINET and EtherCAT both continue to grow in the Chinese market. CC-Link IE, the first industrial protocol with TSN mechanism, maintains a strong regional foothold.

HMS NETWORKS' PERSPECTIVE

"Twelve years of data tell a remarkably consistent story. The migration from fieldbus to Industrial Ethernet is now in its later stages, but the more interesting question is what happens next. When nearly everything is Ethernet, the conversation shifts from 'which

protocol?' to 'what is running on top of it?', functional safety, cybersecurity, TSN, OPC UA, Single Pair Ethernet, IT/OT convergence. That is where the complexity, and the differentiation, will increasingly sit," says Magnus Jansson, Director of Product Marketing, at HMS Networks.

"The 2026 numbers also reinforce something we have been seeing in our industry survey: cybersecurity is now cited by nearly half of respondents as a top integration challenge, and 93% expect OT cybersecurity to change substantially over the next five years. The protocols matter, but the layers above them increasingly define how factories actually operate." Magnus continues.

BEYOND THE PROTOCOLS: A WIDER LENS ON INDUSTRIAL NETWORKING

To complement the long-running annual market shares analysis, HMS Networks publishes the State of Industrial Networking, an extended companion report that examines the broader dimensions shaping industrial communication: cybersecurity, leading industry voices from across the world, regional or industry-specific dynamics and much more.

The extended report draws on the Future of Industrial Networks survey, an externally panelled study now in its second annual edition. The 2026 cycle captured responses from industrial designers and users across all major regions and industries, with the 2027 edition opening for participation in June this year. As individual protocol-level shifts grow smaller year on year, the broader picture captured in the extended report will increasingly carry the conversation about where industrial networking is heading.

What is the best industrial network?

The network debate nobody wins (and that's okay)

In the world of industrial automation, asking “What is the best industrial network?” is a bit like asking a room full of Italians what the best pasta is. You’ll get heated arguments, passionate defenses, maybe even a fight, but you won’t get a single answer.

Yet it's a central question that product

managers, automation engineers, and operation managers constantly debate. Industrial networks are the nervous systems of our machines and factories. Selecting the wrong one can delay a launch, complicate integration, or lock you into a vendor ecosystem for decades.

So, is there a winner? One protocol to rule them all?

Not quite. And maybe that's missing the point.

The key isn't picking a single “best”. It's about choosing flexibility, openness, and readiness for change.

How to judge an industrial network: The 4 critical criteria

1 Determinism and real-time performance

In automation, timing isn't everything- it's the only thing. From synchronized multi-axis motion in robotics to precise I/O timing in packaging lines, milliseconds matter.

This is where deterministic protocols shine. EtherCAT and Sercos offer exceptional real-time behavior, often achieving cycle times under 1ms. PROFINET IRT and POWERLINK are also highly deterministic, especially with hardware support.

Other Ethernet-based protocols like EtherNet/IP and Modbus TCP offer good performance for general automation but may need tuning or extensions to meet strict real-time needs.

If you're in motion control, speed isn't negotiable.

2 Scalability and topology flexibility

Is your application a single device in a small machine, or hundreds across a distributed system? Networks like PROFINET and EtherNet/IP scale beautifully from a handful of nodes to entire production floors. They support flexible topologies: line, star, ring, and allow device-level additions without full system reconfiguration.

These networks also offer evolution and integration from their legacy fieldbuses like PROFIBUS or DeviceNet. Wireless variants further expand the range.

Scalability isn't just about size. It's about adaptability across lifecycle stages.

3 Interoperability and ecosystem support

Even the best-designed protocol falls flat without a strong ecosystem. What matters is how many vendors support it, how rich the toolchain is, and how easily it integrates with engineering software.

PROFIBUS and PROFINET owe their success to Siemens' ecosystem. EtherNet/IP thrives thanks to Rockwell Automation. EtherCAT has become a force in motion control and machine building. CC-Link IE has deep penetration in Asia due to Mitsubishi. Each of these technologies is supported by strong communities driven by well-organized organizations like (PI, ODVA, ETG or CLPA).

It's not what a protocol can do, it's who's helping you do it.

4 Diagnostics, transparency and maintenance tools

The silent killer in industrial automation? Downtime- and it often begins with invisible problems. That's why modern networks increasingly build in deep diagnostics: link health, signal quality, fault codes, and device metadata. Concrete examples matter here: PROFINET's I&M functions and CIP's device diagnostics (within the CIP ecosystem used by EtherNet/IP) support predictive maintenance and faster root-cause analysis. Older fieldbuses can be opaque—fault finding can feel like detective work—while smart factories need diagnostics that are as clear and actionable as traffic lights.

Visibility is not a luxury. It's your best insurance against unexpected downtime.

CYBERSECURITY AND DIGITALIZATION: THE EXTENDED FEATURES THAT MATTER

Two forces increasingly shape what “best” means: cybersecurity and digitalization.

Cybersecurity: The invisible backbone

In an age of ransomware attacks and nation-state cyber threats, industrial networks can no longer afford to be open doors. Standards are evolving with encryption (TLS), access control (roles, certificates), and traffic filtering.

Protocols like CIP Security (for EtherNet/IP), Modbus Security or PROFINET Security Classes show how mature standards are adopting IT-style protections. Firewalls and secure gateways are no longer optional, they’re essential.

And let’s not forget segmentation. A flat network is a vulnerable network. Protocols need to support VLANs, subnetting, and access zones.

Digitalization: from sensors to the cloud

Collecting massive amounts of information from the plant floor to increase quality and efficiency is key for competitiveness. And networks are the data highways enabling it.

Protocols that support IT/OT integration, like OPC UA, MQTT, or those embracing Time Sensitive Networking (TSN)- are more than buzzwords. They’re the foundation for smart analytics, remote maintenance, AI-based optimization, and edge computing.

The best networks don’t just move packets. They enable progress.

REAL-WORLD COMPLEXITY: NO WINNER, JUST SURVIVORS

If the “best” were obvious, the industry would have converged. It hasn’t—because the real world isn’t uniform.

- Regions have strong biases: PROFINET in Germany, EtherNet/IP in North America, CC-Link in Japan.
- Suppliers drive ecosystems: Siemens, Rockwell, Mitsubishi, Beckhoff, each pushing their “home” network.

- Installed base systems still run PRO-FIBUS, DeviceNet, or even CANopen. They work. They stay.

HMS’ market study repeatedly shows that the global market is still deeply fragmented with over 20 protocols holding meaningful market share. Ethernet-based networks are growing, but no clear winner dominates.

FLEXIBILITY WINS: THE PRACTICAL ALTERNATIVE TO STANDARDIZING

So, what’s the smart move? Stop chasing the “best” and start enabling the rest.

The best-performing industrial teams treat networking like logistics, it’s about compatibility, adaptability, and long-term resilience. They don’t just select a network - they prepare to interface with many.

This kind of flexibility pays off in:

- Best performance and optimization for each application
- Reduced integration costs (faster adaptation to customer’s needs)
- Greater global reach (sell in Japan, Europe, and the US without network headaches)

THE ANYBUS CONCEPT: COMMUNICATE WITH ANY NETWORK

This is where HMS Anybus comes in - not

to pick a side, but to remove the problem altogether, enabling them all.

By enabling communication across multiple industrial networks, devices and machines can be designed once and connected to different environments without redesign. Instead of committing to a single protocol, the focus shifts to ensuring compatibility across PROFINET, EtherNet/IP, EtherCAT, PROFIBUS, and others.

CONCLUSION: IT’S NOT ABOUT THE BEST, IT’S ABOUT THE FIT

So, what’s the best industrial network? It’s the one that lets your machine, your device, your plant do its job- in any context, on any continent, with any partner.

It’s the one that doesn’t just meet a spec- it supports your strategy.

It’s the one that talks to all the others.

For many companies, achieving that level of flexibility requires more than choosing the right protocol. It requires choosing the right approach to industrial communication.

Because in this race, there’s no finish line. But with the right communication tools, you can keep moving forward- fast, flexible, and future-ready.



What the industry is telling us

Findings from the “Future of Industrial Networks Survey”

The observations in this article are drawn from the Future of Industrial Networks Survey, conducted by HMS Networks (see page 23 for this year’s survey). Respondents from across the automation industry shared what they use today, what they expect to rely on tomorrow, and where the friction sits.

The findings suggest a more nuanced market reality. Industrial companies are not simply moving from one network generation to the next. They are learning to manage a wider communication landscape, where established industrial Ethernet networks remain strong and legacy fieldbuses continue to matter. Meanwhile, IIoT technologies are moving closer to devices, wireless is finding specific but important use cases, and cybersecurity is becoming a design factor rather than a late-stage IT concern.

The result is not convergence around one single network. It is convergence around a new requirement: industrial communication must be easier to integrate, easier to scale, easier to secure, and easier to main-

tain over long product lifecycles.

That shift is now visible in the survey results.

INDUSTRIAL ETHERNET REMAINS THE BACKBONE — BUT THE EDGE IS BECOMING MORE DIVERSE

The most commonly used networks in the survey are still the familiar industrial Ethernet leaders. PROFINET, EtherNet/IP and EtherCAT appear at the top of current usage, confirming that the core automation network landscape remains highly protocol-driven and regionally influenced.

This is not surprising. These networks are deeply embedded in automation architectures, machine designs, PLC ecosystems, certification processes and customer specifications. For machine builders and device manufacturers, they are not optional. Supporting the right industrial networks is still a basic requirement for entering many markets.

But the more interesting finding is what happens when respondents look ahead.

When asked which networks they expect to remain relevant over the next five years, PROFINET, EtherNet/IP and EtherCAT still lead. However, OPC UA and MQTT move into a much more visible position. These technologies do not replace the real-time automation networks, but they clearly represent another communication layer that industrial companies expect to use more. This points to a market that is becoming layered.

At the control level, deterministic industrial Ethernet remains essential. At the information level, technologies such as OPC UA and MQTT are becoming increasingly important for data access, monitoring, analytics, service models and integration into higher-level systems.

In other words, the future industrial network is not a single protocol. It is a stack of communication needs.

THE BIGGEST CHALLENGE IS NOT SPEED — IT IS MAKING EVERYTHING WORK TOGETHER

It is easy to assume that industrial networking challenges are primarily technical: latency, bandwidth, performance, or real-time behavior. These issues remain important, but they were not the top concern in the survey.

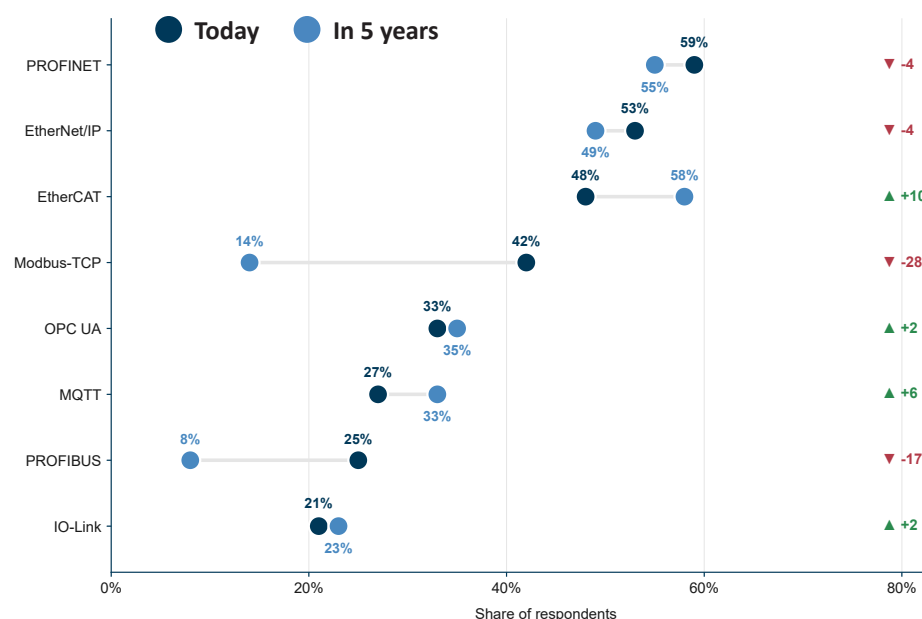
The leading challenge was compatibility between different vendors. Cybersecurity followed closely. Complexity in setup and maintenance was also a major theme.

This is an important signal.

Industrial communication has matured to the point where raw performance is no longer the only measure of success. The harder challenge is making communication work reliably across devices, vendors, protocols, generations, and security expectations.

For device manufacturers, this creates a difficult balancing act. Their customers expect support for the right networks. Their engineering teams need to keep products reliable and cost-efficient. Their product managers need to protect time-to-market. Their support teams need to deal with in-

Established industrial Ethernet remains strong, while information-oriented technologies gain future relevance.



stallations that may remain in operation for decades.

At the same time, the network landscape is not becoming simpler. Even if some legacy networks decline, new requirements are added. Industrial Ethernet, fieldbus, IIoT communication, wireless, cybersecurity and cloud/edge integration do not arrive as separate projects. They accumulate.

That accumulation is where complexity becomes expensive.

The survey indicates that companies are not only asking, “Which network should we support?” They are increasingly asking, “How do we support all required networks without making our products, development processes and lifecycle commitments too complex?”

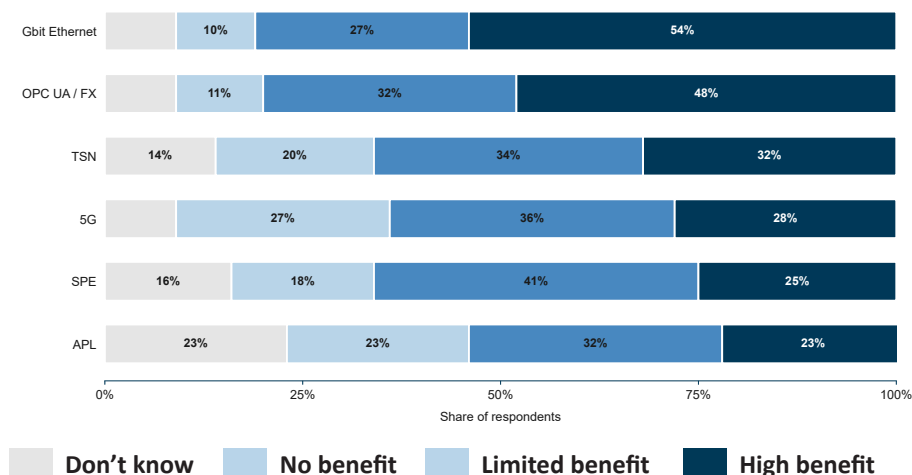
FUTURE TECHNOLOGIES ARE INTERESTING — BUT VALUE MUST BE PRACTICAL

The survey also asked respondents to rate the potential benefit of several future-oriented technologies: TSN, Advanced Physical Layer, Single Pair Ethernet, Gigabit Ethernet, OPC UA / OPC UA FX and 5G.

The responses show clear interest, but not blind enthusiasm.

Gigabit Ethernet and OPC UA received some of the strongest benefit signals. This suggests that respondents see practical value in higher bandwidth, stronger information models, and more capable communication architectures. TSN and Single Pair Ethernet also show meaningful interest, but with more uncertainty. 5G is viewed as

Interest is clear, but the market separates practical value from technology hype.



potentially valuable by some, but not as a universal answer.

This is an important distinction. The market is not rejecting new technologies. But it is asking for relevance.

Industrial users and device designers are pragmatic. A technology becomes interesting when it solves a real application problem: more data, better synchronization, simplified cabling, improved diagnostics, easier integration, or new machine concepts. It becomes less interesting when it is presented as a general revolution without a clear implementation path.

This is especially visible in the 5G results. Some respondents see 5G as valuable, but

many remain unsure or do not see it solving their immediate industrial networking problems. That does not mean 5G lacks potential. It means its value will likely be application-specific, especially where mobility, large sites, remote assets or private networks create a strong use case.

The same pattern applies more broadly. The technologies that succeed in industrial communication are not always the most advanced on paper. They are the ones that can be implemented, supported, secured and justified in real machines and devices.

IIOT IS MOVING CLOSER TO THE MACHINE — AND CLOSER TO THE DEVICE

IIoT communication is no longer just a cloud discussion. A clear majority of the respondents described it as either important or critical to their application.

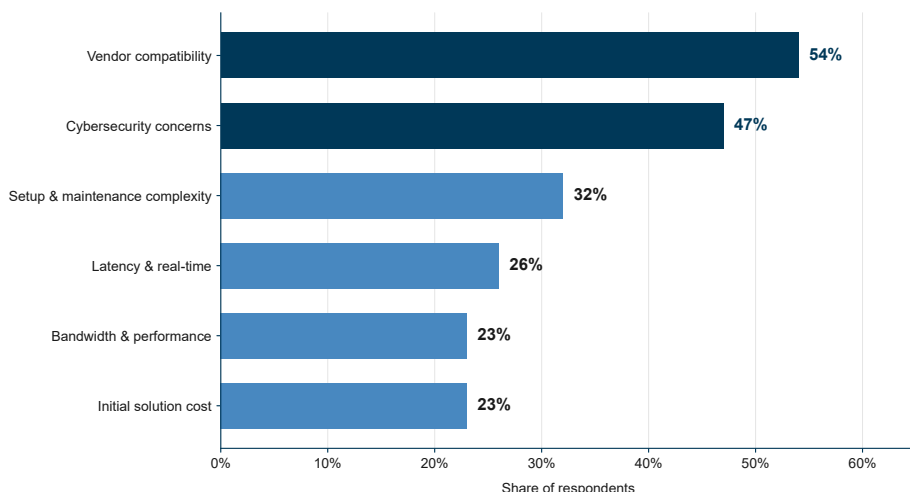
The reasons are familiar, but still significant. Predictive maintenance, access to more production data and improved production quality were the most common drivers. These are not abstract digitalization ambitions. They are operational goals.

What stands out is where respondents expect IIoT communication to happen. The answers point not only to plant-level systems or cloud platforms, but also directly to automation devices such as drives, sensors and I/O modules, as well as machine-level PLCs and edge gateways.

This suggests that IIoT is becoming more distributed.

Industrial data is no longer expected to

The market pain is shifting from pure connectivity to scalable, secure and maintainable connectivity.



be collected only at a higher system level. More intelligence, diagnostics and communication capability are moving into the machine and device layer. This creates new expectations for device manufacturers. A product that once only needed to exchange cyclic control data may now also need to expose diagnostics, asset data, energy data, condition data or configuration information.

MQTT and OPC UA were the most commonly expected technologies in these IIoT applications. That combination is telling. MQTT points to lightweight publish/subscribe data movement, often associated with cloud and edge architectures. OPC UA points to structured industrial information exchange. Together, they indicate that industrial companies are looking for both efficient transport and meaningful data models.

For device manufacturers, this creates a new product design question: how much communication capability should be built into the device from the start?

The answer will differ by product category. But the direction is clear. Communication is no longer only about connecting to the PLC. It is also about making the device visible, understandable and useful in a broader industrial data architecture.

WIRELESS IS USEFUL WHERE CABLES BECOME THE PROBLEM

Wireless communication in industrial environments has often been treated with caution, and the survey results reflect a similar pattern. Wireless is not presented as a replacement for wired industrial networks across the factory. Instead, respondents point to specific applications where wireless can solve practical problems.

The most common use cases include machine connectivity to factory infrastructure, mobile or moving vehicles such as AGVs and AMRs, new IoT sensors, and moving or rotating applications where cabling is difficult or costly.

Wi-Fi is the most commonly used wireless technology among respondents, followed by IO-Link Wireless, RFID and Bluetooth. This again shows a practical rather than revolutionary pattern. Industrial wireless adoption is not one thing. It is a set of technologies used for different purposes.

The barriers are equally practical. Connection stability and real-time communication

concerns were the strongest challenges. Cybersecurity, data throughput and installation expertise were also mentioned.

This means wireless adoption will continue, but selectively. The opportunity is strongest where the application pain is obvious: moving equipment, temporary installations, hard-to-wire assets, sensor retrofits and machine-to-infrastructure communication. Wireless will grow where it removes a physical limitation. It will struggle where it is positioned as a general replacement for a stable cable.

CYBERSECURITY IS BECOMING PART OF THE CONNECTIVITY DECISION

Perhaps the clearest strategic shift in the survey is the role of cybersecurity.

Cybersecurity is no longer only an IT topic or a final compliance step. Respondents indicate that it is influencing decisions about industrial network connectivity, driven by regulations, customer expectations and internal security initiatives.

The challenges are also revealing. Lack of in-house expertise, limited development resources, unclear requirements, process limitations and additional implementation costs all appear as barriers.

This tells us something important about the state of the market: companies understand that cybersecurity matters, but many are still working out how to implement it efficiently.

For device manufacturers, the challenge is especially difficult. Security must be designed into products that may have long

lifecycles, multiple protocol variants, different customer requirements and limited hardware resources. It is not enough to add a security feature. Companies need secure development processes, update strategies, vulnerability handling, documentation, and a clear understanding of how regulations affect their products.

The survey also shows that expectations for OT security are evolving. Respondents see a future where industrial communication becomes more secure, where devices implement stronger hardware and software security features, and where network protection alone is not always enough.

This does not mean every industrial device will suddenly become fully encrypted, cloud-connected and security-certified. Industrial markets move more carefully than that. But it does mean that security is becoming part of the connectivity architecture.

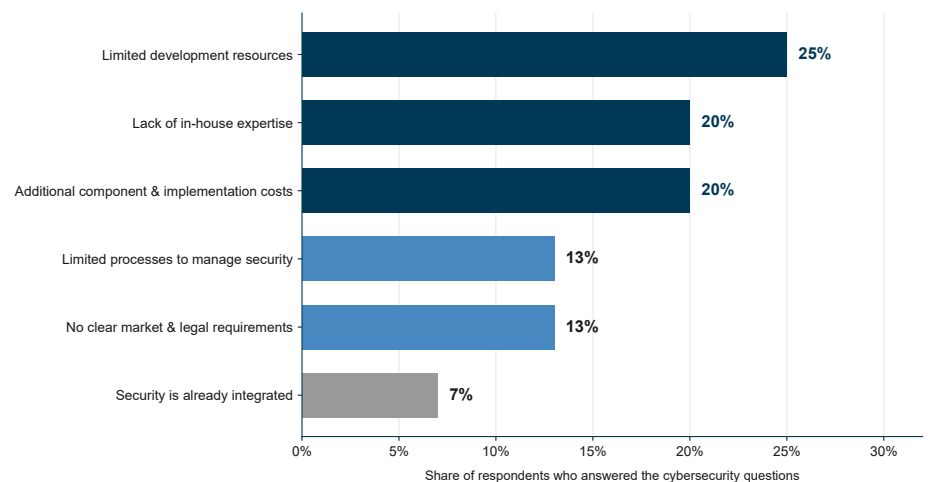
In the past, the communication question was often: "Which network do we need to support?"

Now, the question is becoming: "How do we support the required networks in a way that is secure, maintainable and compliant over time?"

DEVICE MANUFACTURERS ARE OPTIMIZING FOR TIME, RISK AND SCALABILITY

The device manufacturer responses are especially relevant because they show how communication decisions are made inside product development.

Cybersecurity is accepted as important, but implementation capability is the bottleneck.



External gateways, multi-protocol chips, ready-made modules, single-protocol ASICs and protocol stacks all appear in the responses. This confirms that there is no single preferred integration model across the market. Different companies choose different approaches depending on product type, volume, cost pressure, engineering capability and lifecycle strategy. However, the decision criteria are highly consistent.

Fast integration for shorter time-to-market was one of the strongest factors. Easy integration to reduce risk was also highly ranked. Compatibility with existing protocols and scalability for future needs stood out strongly when respondents were asked what matters most when integrating communication into devices.

This is a critical insight.

The value of an industrial communication solution is not only the network interface itself. It is the reduction of uncertainty around the interface.

- Can the product reach market faster?
- Can the engineering team avoid unnecessary protocol complexity, while keeping the product updated and compliant throughout its lifecycle?
- Can the same approach scale across

several product families?

- Can future network and security requirements be handled without redesigning everything?
- Can the supplier be trusted over the product lifecycle?

These questions are becoming more important as communication requirements multiply.

For many device makers, industrial connectivity has become too important to ignore, but too complex to treat as a small side task. It sits in an uncomfortable position: essential for market access, but rarely the core differentiator of the product.

That is why integration risk, time-to-market and lifecycle maintainability now matter so much.

THE MARKET IS NOT SIMPLIFYING — SO THE SOLUTIONS MUST

The overall conclusion from the survey is clear: industrial networking is not becoming simpler.

The established industrial Ethernet networks remain strong. Legacy networks still matter in many environments. OPC UA and MQTT are gaining relevance. IIoT communication is moving closer to devices. Wireless is expanding in specific use cases. Cybersecurity is becoming a core product and

architecture concern. New technologies such as TSN, SPE, Gigabit Ethernet, OPC UA FX and 5G are being evaluated, but with practical expectations.

This creates a more demanding connectivity environment.

The winning companies will not be those that bet everything on one network or one technology trend. They will be the ones that can manage diversity without letting complexity take over.

For industrial users, that means choosing architectures that can evolve.

For machine builders, it means designing machines that can communicate across customer environments.

For device manufacturers, it means building products that support the right networks, expose the right data, meet security expectations and remain maintainable over long lifecycles.

The future of industrial networks is not one network. It is a more connected, more secure and more layered industrial communication landscape.

And in that landscape, the real competitive advantage will be the ability to make complexity manageable.

Voices from the industry

To look beyond the numbers, HMS asked selected industry leaders for their view on the future of industrial networking. Here, Rob Johnson, Technical Director at Fortress Safety, shares what he sees coming next.

"With machines becoming more complex and production environments demanding greater throughput and flexibility, there is a growing need for safety-related devices such as interlocks to communicate over major industrial fieldbuses. At Fortress Safety, we have seen a clear shift in recent years towards the adoption of network-enabled solutions, delivering operational advantages and valuable data for maintenance and diagnostics.

Today, safety is no longer just about stopping machines, but about ensuring interconnected systems can communicate effectively to reduce risk in real time. There is a

need for solutions that account for interactions across platforms, driven by the widespread adoption of industrial robots and the increasing use of mobile equipment.

IO-Link Safety is expected to enable easier integration through standardised connectors and device descriptions, while supporting real-time data access and simplified maintenance. As safety masters become available, we are seeing strong interest in how interlocks will integrate into these systems.

At the same time, wireless communication – including industrial Wi-Fi and 5G – is be-



Rob Johnson, Innovation Director, Fortress Safety

coming increasingly relevant, particularly with the accelerated growth of AMRs and AGVs. As these technologies mature, we expect wireless communication to play a significant role in supporting safer, connected industrial environments."

A semiconductor recovery in Germany. A labor shortage in Japan. A new physical-layer wave in China. A push for richer device data in the United States. Four very different cues — all driving the same demand for secure, flexible, standards-aligned communication. Here's what our regional leaders are seeing on the ground.

Voices around the globe. Industrial networking,



EMEA (EUROPE AND MIDDLE EAST)

"Europe and the Middle East in 2026 continue to operate in what VDMA describes as an environment of geopolitical tension, weak investment and rising competitive pressure, resulting in an uneven industrial recovery across EMEA. While the macro backdrop remains fragile, the German speaking area is showing the strongest recovery in our business, supported by improving momentum and early signs of stabilization in German manufacturing. By contrast, the UK remains subdued in our performance, reflecting a more cautious investment environment and weaker demand conversion. End-market demand remains clearly differentiated. Automotive-linked segments are still cautious, but OEMs with exposure to the semiconductor market are performing better, supported by a stronger semiconductor outlook for 2026. In parallel, we continue to see healthier activity in food, dairy and industrial processing equipment, where customers remain focused on productivity, automation, and robust communications infrastructure. Despite continued uncertainty and selective capex behavior, the underlying demand for secure, flexible, and compliant industrial connectivity solutions remains structurally positive."



Michael Neidhöfer,
Vice President, Sales,
HMS EMEA



AMERICAS

"In the Americas, devices and machines continue to evolve toward more complex data communication. Protocols supporting richer communication environments continue to expand their share of the market. EtherNet/IP remains the dominant industrial network across most applications, while protocols such as OPC UA and PROFINET are also gaining popularity.

Machines are adding additional diagnostic information including device meta and status data in addition to the data managed by the machine controller. Security is also an area of focus as a higher percentage of machines are connected directly to corporate networks to support data telemetry solutions and remote diagnostic tools.

These trends signal a broader transformation as industries modernize connectivity to support digitalization and safe, secure operations."



Tom McKinney,
Vice President, Sales,
HMS Americas

region by region



JAPAN

"In Japan, the industrial networking market is entering a new phase. Automation remains a key driver, especially in the automotive, semiconductor, logistics, food & beverage, and pharmaceutical industries, where automation and networking continue to be major growth drivers. This trend is supported by Japan's severe labor shortage caused by its declining birthrate and aging population, the increasing automation and robotization of manufacturing sites, and the growing risk of cyberattacks in the OT domain.

The Japanese market is no longer looking for "connectivity" alone. Instead, it is increasingly seeking communication solutions that are secure, scalable, and capable of supporting functional safety. At the same time, leading Japanese industrial manufacturers are beginning to shift toward software-defined automation systems, including the use of Physical AI, to enable more flexible and multi-purpose solutions.

In addition, regulations such as the Cyber Resilience Act (CRA) and the new Machinery Regulation (EU) 2023/1230 are having an impact on Japanese device manufacturers and machine builders, particularly those exporting equipment to Europe. As a result, cybersecurity, functional safety, and lifecycle support are becoming the next key requirements for industrial networking solutions in Japan."



Hideto Oguri,
Business Excellence Manager
HMS Japan



CHINA

"For factory automation, Industrial Ethernet is now standard across most Chinese devices (notably supporting PROFINET, EtherCAT, and EtherNet/IP). Driven by global expansion, demand for multi-network support, functional safety, and cybersecurity has increased significantly.

In process automation, national strategies and market forces are accelerating APL adoption, expected to trigger a new wave of Ethernet networking.

Meanwhile, several Chinese companies are setting local network standards that are gaining both national and international (IEC) recognition."



Jiliang Wang,
Sales Director,
HMS Greater China

The hidden cost of in-house connectivity

The real total cost of ownership and why time-to-market pressure demands an evolved approach

CONNECTIVITY AS A PREREQUISITE, AND A HIDDEN BURDEN

Industrial communication is no longer optional. It is a prerequisite for competing in modern automation environments. Yet for many device manufacturers, the true cost of developing and maintaining communication solutions remains underestimated. While component cost and initial development effort are visible and easy to quantify, the real burden emerges over time. Slower time-to-market, ongoing maintenance, portfolio scalability challenges, and increasing cybersecurity and regulatory obligations all contribute to a growing total cost of ownership (TCO), often long after

the first product has shipped. Connectivity decisions are therefore being re-evaluated. Not to replace what already works, but to extend it in a way that reduces cost, risk, and complexity across the product lifecycle.

THE VISIBLE COST ILLUSION

Industrial communication is often treated as a well-defined engineering task: select a chipset or module, integrate a protocol stack, validate functionality, and move on. On paper, this looks manageable. In reality, this view only captures the visible part of the cost. Once products move into production and remain in the field for years

*The iceberg problem
Component cost and initial development effort are only the visible tip. Most connectivity costs emerge over time.*

or decades, communication interfaces continue to require updates, maintenance, certification support, and adaptation to new requirements. The result is a growing gap between assumed cost and actual cost over the product lifecycle.

THE HIDDEN COSTS OF IN-HOUSE COMMUNICATION DEVELOPMENT

The individual challenges described below are often familiar to engineering and product teams. Viewed in isolation, each may seem manageable. Taken together, they significantly increase total cost of ownership and introduce risk that is difficult to predict or plan for.

TIME-TO-MARKET DRAG

Industrial communication has become significantly more complex. Beyond basic data exchange, modern devices must support profiles, diagnostics, cybersecurity mechanisms, certification requirements, and interoperability across heterogeneous environments. Each additional requirement increases integration effort and validation time.

Projects seldom fail outright. Instead, time is lost through:

- late validation issues
- iterative certification fixes
- dependency on scarce expertise

Even small delays can have a large business impact—missed opportunities, increased price pressure, and weaker market positioning—all of which contribute directly to higher total cost of ownership.

MAINTENANCE AND LIFECYCLE BURDEN

Unlike many other subsystems, industrial communication interfaces require continuous attention throughout the entire product lifetime.

This includes:

- protocol updates
- bug fixes and vulnerability handling
- certification updates
- hardware and software evolution

Over time, maintenance consumes a growing share of engineering capacity and limits the ability to invest in innovation.

SCALABILITY ACROSS THE PRODUCT PORTFOLIO

For many large device manufacturers, the

real challenge is not a single product, but the entire portfolio.

Different devices require different performance levels, protocols, and feature sets. When communication is developed independently per product, this leads to:

- Duplicate engineering work
- Inconsistent behavior and documentation
- Increased test and certification effort
- Fragmented maintenance responsibility

What starts as “small adaptations” quickly turns into parallel development projects. Over time, this lack of scalability drives up cost and complexity, making it harder to introduce new variants or respond quickly to market demands.

COMPLIANCE AND REGULATORY PRESSURE

Cybersecurity and regulatory requirements introduce a new category of cost.

Requirements such as the Cyber Resilience Act and IEC 62443 impose ongoing obligations, including monitoring, documentation, updates, and vulnerability management.

These costs are often not visible up front. Instead, they appear as ongoing interrup-

tions, re-prioritizations, and unexpected work.

BUILD VS PARTNER

Once the hidden costs of connectivity become visible, the question shifts from how to implement communication to where responsibility should sit.

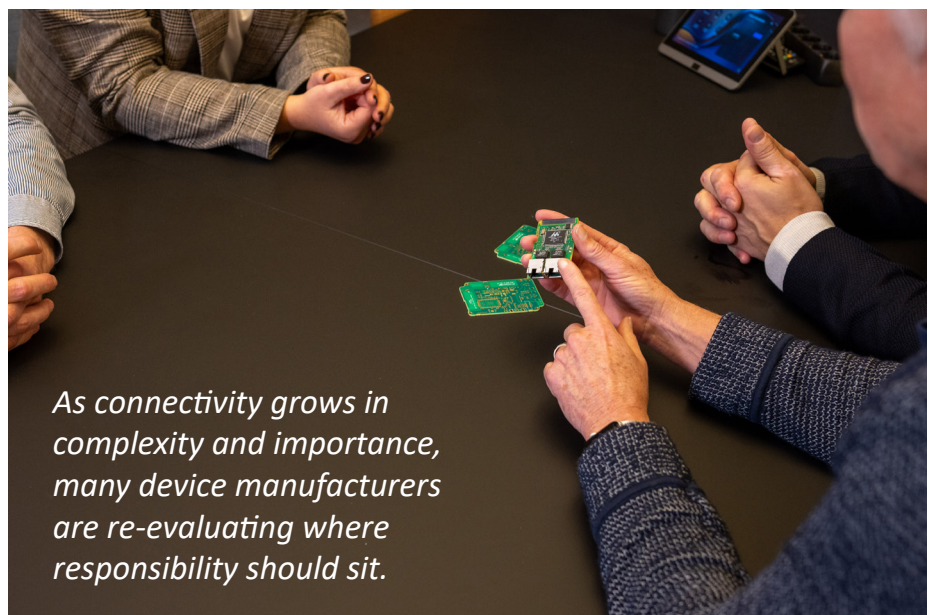
In-house approach

Developing communication in-house provides control, but it also means taking full ownership of protocol maintenance, certification, cybersecurity, and support. Over time, connectivity becomes a permanent operational workload, competing directly with core product innovation.

The partner approach

A partnership approach takes a different path. Connectivity is treated as a managed discipline rather than a one-time development task, with lifecycle responsibilities shared externally. This reduces internal complexity and allows teams to focus on differentiation and performance.

For Product Managers, the key factor is not minimizing upfront cost, but controlling total cost of ownership over time. A structured approach to connectivity makes effort more predictable, reducing unplanned work and improving long-term planning.



As connectivity grows in complexity and importance, many device manufacturers are re-evaluating where responsibility should sit.

This is not just a technical choice—it directly shapes time-to-market, portfolio scalability, regulatory risk, and the availability of engineering resources for innovation.

PARTNERING WITH HMS

As connectivity grows in complexity and importance, many device manufacturers are re-evaluating where responsibility should sit.

Managing industrial communication over the full product lifecycle requires continuous investment. Protocols evolve, cybersecurity requirements grow, and regulatory expectations increase. Maintaining this internally demands sustained focus and specialized expertise.

Partnering with HMS Networks shifts this model. Connectivity is treated as a long-term managed discipline, where updates, compliance, and lifecycle considerations are handled systematically. This reduces the need for repeated internal effort and enables organizations to keep pace with change.

One of the key advantages is predictability. In-house development often leads to unplanned work caused by certification

changes, security updates, or supply chain disruptions. A partnership approach reduces these interruptions, making connectivity a more stable and manageable cost element.

EVOLVING A PROVEN APPROACH

Partnering with a specialist to handle industrial communication is not new for many device manufacturers. For decades, manufacturers have successfully deployed Anybus products to address the core challenges of in house communication development: complexity, maintenance, certification, and long term lifecycle responsibility. What has changed is the environment around that approach. Faster time-to-market expectations, larger device portfolios, and rising regulatory and cybersecurity requirements have created the need to extend the proven Anybus model to better support scale, reuse, and compliance.

ANYBUS ONE: EXTENDING THE MODEL

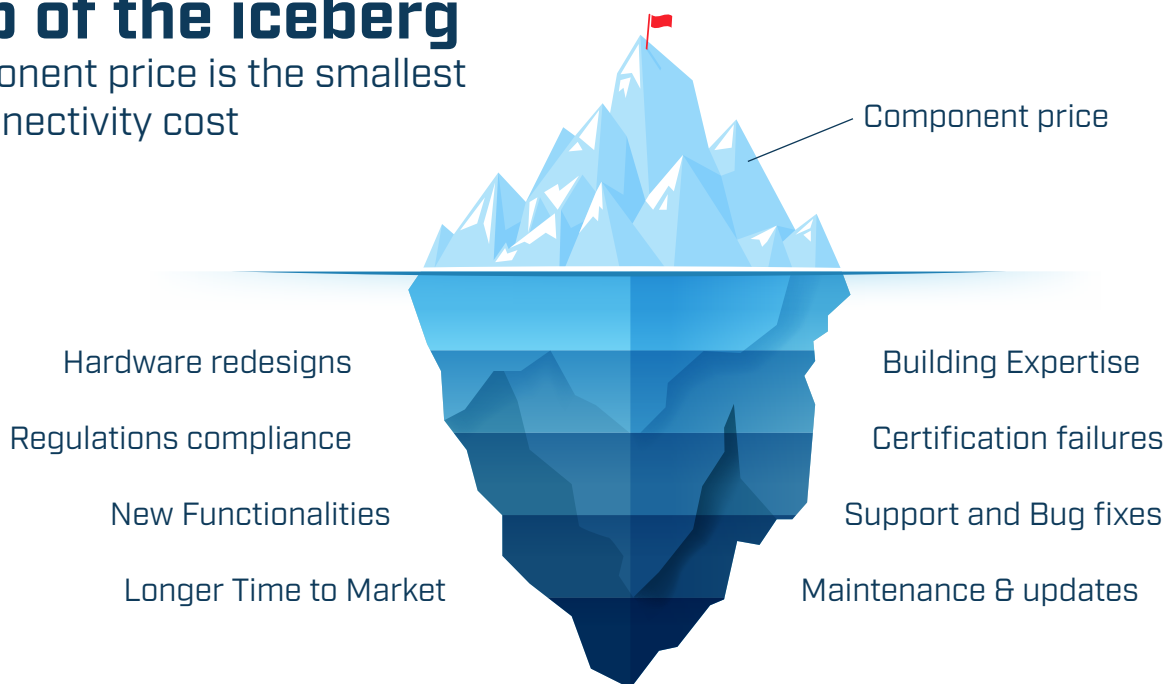
Anybus ONE represents an evolution of the established approach. Rather than treating connectivity as a per-product task, it introduces a plat-

form-based model that enables:

- **Scalable functionality and cost across a device portfolio**, allowing device makers to choose the right solution for each device, from simple to advanced, rather than implementing a single, over specified solution across all products
- **A shared architectural foundation** across products and performance levels
- **A common hardware footprint** across variants, allowing device makers to reuse the same design across multiple product variants without redesign
- **A configure instead of program** approach via Anybus Studio, enabling reuse, faster development, and simpler maintenance
- **Security and regulatory readiness built in by design**, supporting CRA and cybersecurity requirements as ongoing responsibilities
- **Hardware and software decoupling**, improving resilience to supply chain changes and enabling future updates without re engineering

The tip of the iceberg

Why component price is the smallest part of connectivity cost



These elements do not replace the Anybus philosophy — they extend it. The result is a connectivity approach better suited to modern device portfolios and long term Product Management requirements.

WHAT THIS MEANS IN PRACTICE

In practice, this approach changes how connectivity is managed across a product portfolio.

Development teams can reuse the same communication concept across multiple products, rather than implementing similar functionality repeatedly.

Entry-level devices can use only the functionality they require, while more advanced products can build on the same foundation. This reduces unnecessary complexity, avoids over-specification, and makes it easier to introduce new product variants.

At the same time, updates, certification, and compliance can be handled more consistently across the portfolio, reducing fragmentation and improving long-term maintainability.

The result is a more predictable development process and a lower total cost of ownership over time.

Connectivity keeps products relevant. Managing its complexity keeps organizations competitive.

CONCLUSION: FOCUS WHERE YOU CREATE VALUE

Connectivity has become a fundamental requirement for almost every industrial device. At the same time, connectivity itself rarely represents true differentiation. What does differentiate is how effectively organizations manage the cost, risk, and complexity that come with communication over the full product lifecycle.

As industrial communication evolves, total cost of ownership becomes the defining factor in connectivity decisions.

The key question for Product Managers is no longer whether communication can be developed in house, but whether it should be, and whether this is where scarce engineering and organizational capacity creates the most value.

Is your connectivity TCO under control? A 7-point self-check

Each item is a yes/no question. Score yourself.

1. Can you state your total connectivity engineering hours across the last 24 months?
2. Do you know how many protocol-related certifications are due for renewal in the next 18 months?
3. Is your communication architecture shared across product variants, or rebuilt per device?
4. Have you allocated engineering capacity for CRA compliance obligations from 2027 onward?
5. When a new vulnerability is disclosed, do you know within 48 hours which of your products are affected?
6. Can you add a new protocol variant to an existing device without redesigning the hardware?
7. Is connectivity development competing with feature development for the same engineers?

5–7 "yes" answers: you're managing TCO actively.
3–4: TCO is partially visible. Hidden costs are accumulating.
0–2: Connectivity has likely become a permanent operational tax on innovation.



PROFINET in Six Weeks, EtherNet/IP in Two Days

How ELOTECH Restored Delivery Capability Under Severe Time Pressure

When an existing communication platform approaches end-of-life, manufacturers often face a difficult choice: continue investing in a legacy solution or transition to a new technology platform. For ELOTECH Industrieelektronik GmbH, based in Hilden, Germany, this decision became increasingly urgent as product lifecycle challenges and communication-related quality issues began to threaten product availability.

With more than 30 years of experience in industrial temperature control and automation, ELOTECH develops customized solutions for plastics processing, extrusion, and industrial furnace systems. Today, the company offers more than 5,000 product variants and is recognized as a leading provider of multi-zone temperature control solutions. To maintain delivery capability and support future requirements, ELOTECH needed a reliable communication solution that could be integrated quickly and efficiently.

In the following interview, Florian Black, Electronic Engineer at ELOTECH, shares insights into a recent project involving the integration of a new communication solution and discusses the challenges, decision-making process, and results achieved. From supply risks to a strategic platform change

Thierry Bieber, HMS: What triggered the search for a new communication solution?

Florian Black, ELOTECH: Several factors came together at the same time. Our existing communication solution was approaching the end of its lifecycle, and the communication module we were using was being discontinued. This created additional pressure because customer demand was increasing and product deliveries were expected. We were facing the risk of supply shortages.

Our priority was to restore delivery capability as quickly as possible while establishing a stable foundation for future developments. Ultimately, we decided that a new, more reliable solution was the best long-term option.

Choosing a solution that could scale

HMS: What were your most important selection criteria?

ELOTECH: Reliability was our top priority. We wanted a proven solution from an established supplier that we could rely on for many years. We also needed a highly compact solution, ideally in a stamp-sized form factor that could be hand soldered for quick prototyping as well as optimized for serial production costs. Support for multiple industrial protocols to minimize the number of product variants. And given the situation, immediate availability and the fastest possible integration were key elements.

We were already familiar with Anybus from a previous evaluation, so we had a good

overview of the concept. What convinced us was the combination of technical capabilities and promised low implementation effort. That aligns very well with our product strategy and simplifies future developments.

PROFINET implemented in six weeks

HMS: How did the integration process unfold?

ELOTECH: The process was very structured from the beginning. We started the week after our initial discussion directly with a hands-on workshop that introduced the most important tools, processes, and development resources. That gave us a clear starting point and allowed us to become productive very quickly.

There is a continuous guidance throughout the project, from the starter kits, documentation, code examples, configuration tools, and ongoing technical support. The API and Host application code generator allowed us to focus only on the functionality we needed for our device rather than spending time on unnecessary API coding details. This enabled us to start testing quickly an initial prototype and improve the implementation iteratively. Questions could usually be resolved quickly, which helped maintain development momentum.

The result was remarkable. From the initial workshop to a customer-ready PROFINET solution, the entire process took approximately six weeks, including both hardware

and software development. Considering the time pressure we were facing, this was a significant achievement. EtherNet/IP added in only two days

HMS: What happened after the PROFINET implementation was completed?

ELOTECH: Once the platform was established, expanding to additional protocols became much easier. Our immediate focus had been PROFINET because it represented the highest volume requirements and the greatest business urgency. After successfully completing that implementation, we were able to add EtherNet/IP with very little additional effort. In fact, the implementation required only about two days of effective development work. Faster delivery capability and greater flexibility

HMS: What impact has the new solution had on ELOTECH and your customers?

ELOTECH: The first major benefit was restoring our delivery capability. We were

able to respond to customer demand quickly and avoid the long-term risks associated with the previous solution. At the same time, we gained a significantly more flexible platform for future developments. Today, many configuration changes can be implemented entirely through application software. That allows us to respond faster to new customer functionality requirements while reducing development effort. Our customers also benefit. Firmware updates are easier to manage, maintenance becomes simpler, and multiple communication protocols can be supported on the same hardware platform. This reduces product variants and simplifies deployment across different markets and applications.

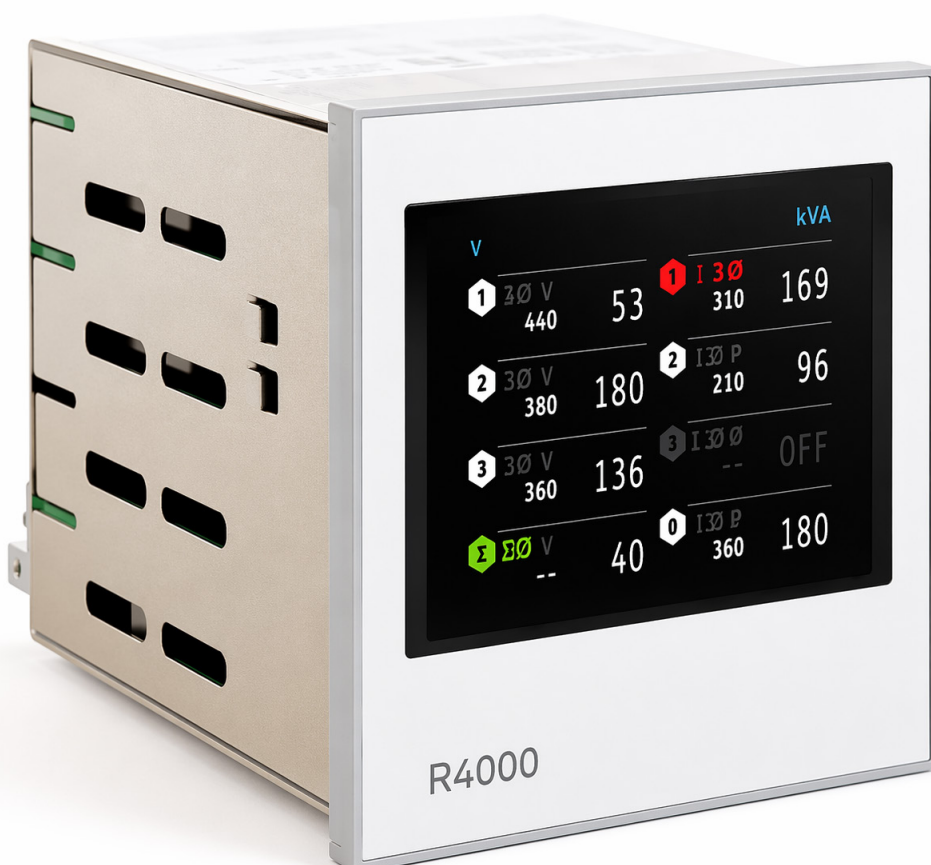
HMS: If you had to quantify the benefit, how would you describe it?

ELOTECH: The biggest impact is clearly on time-to-market. In the past, communication implementations had taken more than a year before reaching production readiness. With the new platform, development cycles have been significantly shortened,

while future protocol integrations and product adaptations can be completed with far less engineering effort.

BUILDING FOR THE FUTURE

For ELOTECH, the implementation was much more than a technical upgrade. It was a strategic step that helped secure short-term delivery capability while creating a future-proof communication platform. By combining fast integration, strong technical support, and multiprotocol flexibility, the company was able to accelerate development, simplify future expansions, and improve responsiveness to customer requirements. And in the context of increasing Cybersecurity regulation, this transition positions ELOTECH with a communication solution designed to support CRA compliance. The results speak for themselves: PROFINET in six weeks, EtherNet/IP in two days, and a communication platform ready for the next generation of industrial products.



ELOTECH
INDUSTRIELELEKTRONIK

Company: Elotech Industrie-elektronik GmbH

Location: Hilden, Germany

Founded: 1994

Focus: Electronic temperature controllers for industrial applications

Products: PID controllers, hot runner controls, indicators, custom solutions

Connectivity: PROFINET, EtherNet/IP, PROFIBUS, OPC UA

Web: elotech.de

What's new in cybersecurity?

**FROM
AWARENESS
TO EXECUTION!**

A SHIFT THAT IS NOW IMPOSSIBLE TO IGNORE

In the *State of Industrial Networks 2025*, the growing importance of cybersecurity in industrial communication was already clear. One year later, that shift has accelerated significantly.

Cybersecurity is no longer a question of *if*, but *how* fast and how *effectively* it can be implemented.

What was previously discussed at a strategic level is now becoming operational reality. Regulations are entering enforcement phases, technology ecosystems are aligning, and both manufacturers and users are integrating cybersecurity into their products and infrastructures.

At the same time, this transition is not happening in isolation. It is supported by stronger frameworks, maturing standards, and a growing ecosystem of solutions. Together, these elements are transforming cybersecurity from a complex constraint into a more structured and manageable discipline.

UPDATE ON REGULATIONS

Cybersecurity in industrial automation is being driven by a combination of increasing threat levels and a strong wave of regulation.

The **Radio Equipment Directive (RED) delegated act on cybersecurity** became fully applicable on **August 1, 2025**. While it has raised the overall cybersecurity level of wireless solutions, it has also led to difficult trade-offs. Some mature products have been discontinued because the effort required to meet the new requirements was too high. In other cases, wireless functionality has been removed entirely.

The **NIS2 directive**, which was scheduled to be implemented by EU member states by **October 17, 2024**, is progressing more gradually. Some countries have completed the process, while others are still finalizing their frameworks. Despite this uneven rollout, NIS2 is already influencing market expectations. It places new responsibilities on industrial companies, including risk management, incident reporting, and supply chain accountability. While many of these measures are organizational, they are also

driving demand for technical cybersecurity capabilities in devices and machines.

The most significant development is the **Cyber Resilience Act (CRA)**, which entered into force on **December 10, 2024**, with product requirements becoming mandatory on **December 11, 2027**. This represents a fundamental shift: cybersecurity becomes a mandatory characteristic of the product itself.

Manufacturers are now expected to:

- design products with security-by-design principles
- implement secure update mechanisms
- manage vulnerabilities across the product lifecycle
- provide documentation such as a Software Bill of Materials (SBOM)

At the same time, the path to compliance is still evolving. Many of the required harmonized standards remain in draft form, particularly those aligned with IEC 62443. This creates a transitional phase where companies must prepare and invest, even as implementation details are still being defined. This regulatory shift is not limited to Europe. Similar approaches are emerging globally, targeting both connected products and industrial operators. The overall direction is clear: cybersecurity requirements are increasing worldwide, and industrial automation is firmly within scope.

UPDATE FROM PROTOCOL STANDARDIZATION ORGANIZATIONS

As regulatory pressure increases, the industrial communication ecosystem is evolving in parallel. Protocol organizations, once focused on performance and interoperability, are now placing cybersecurity at the center of their development strategies.

One key topic is secure industrial Ethernet. CRA requires protection of data in transit, but its applicability depends on risk analysis. In many industrial environments, networks can still be considered trusted, meaning non-secure communication remains acceptable. In other cases, additional protection mechanisms are required.

This use-case dependency is reflected in

the position of the main protocol organizations:

PROFIBUS & PROFINET International (PI) takes a scalable and modular approach, enabling manufacturers to gradually increase security depending on application needs and installed base constraints.

As explained by PI Chairman Xaver Schmidt: “Manufacturers who rely on PROFINET already have a solid basis for CRA compliance today. If higher security requirements are needed, manufacturers can gradually expand their products with PROFINET security features — from authenticated secure communication to complete encryption.”

ODVA (CIP / EtherNet/IP) follows a practical, implementation-driven approach, integrating widely used IT security concepts such as authentication, identity management, and secure communication into industrial systems.

As highlighted by ODVA at SPS Nürnberg 2025:

“The implementation of CIP Security involves device identity management, secure communication protocols, and vulnerability mitigation, which are essential for compliance with the EU Cyber Resilience Act.”

EtherCAT Technology Group (ETG) takes a security-by-design approach, relying on architectural characteristics to reduce attack surfaces rather than adding additional security layers.

As stated by ETG Executive Director Martin Rostan:

“We are convinced that EtherCAT already meets the requirements of IEC 62443 and the CRA for almost all common applications without the need for changes or extensions to the protocol.”

In addition, standards such as EN 50742, linked to the EU machinery regulation, are introducing new requirements for cryptographic protection in cases where networks cannot be assumed to be physically secure.

Despite these developments, real-world adoption of secure industrial Ethernet remains limited. In many installations, cyber-

security is still achieved through a combination of organizational measures, physical protection, and network segmentation. This highlights an important reality: Cybersecurity adoption is not binary. It is gradual, use-case dependent, and shaped by practical constraints.

POSITION OF MAKERS AND USERS (SURVEY INSIGHTS)

Survey results confirm that cybersecurity is now firmly established as a concern in industrial communication driven by regulatory requirements, customer expectations, and internal initiatives. However, the transition from awareness to implementation remains challenging. Companies typically face:

- lack of in-house expertise
- limited development resources

- unclear regulatory requirements
- additional costs and complexity

This highlights a clear gap: cybersecurity is understood, but not yet fully integrated into product development processes.

HMS TAKE ON CYBERSECURITY AND NEXT STEPS

In this evolving landscape, cybersecurity must be approached as an integral part of industrial communication. The challenge is no longer defining requirements, but implementing them efficiently in real products.

For device manufacturers, this means addressing cybersecurity alongside multiple networks, long product lifecycles, evolving regulations, and ongoing performance and cost constraints.

At HMS Networks, the focus is on helping customers reduce complexity and move

from requirement to implementation by aligning communication solutions with established standards, integrating security into product design, and providing practical guidance for implementation.

MOVING FORWARD

Cybersecurity in industrial networks is entering a new phase.

Regulations are becoming enforceable. Standards are evolving. Technology ecosystems are integrating security into their foundations.

At the same time, adoption remains gradual, shaped by practical constraints and varying requirements across industries.

The direction is clear: cybersecurity is becoming part of how industrial communication is designed, implemented, and maintained.

Voices from the industry

Hans-Joachim Fröhlich, Director of Technology and Portfolio at Endress+Hauser on how regulation, lifecycle thinking, and collaboration are redefining industrial cybersecurity.

“The focus has evolved from simply choosing the right protocol to enabling secure, compliant, and highly interoperable connectivity across ecosystems.

With regulations such as NIS2 and the Cyber Resilience Act, customers are increasingly investing in solutions that deliver long-term security across the entire lifecycle – moving beyond devices toward holistic security strategies.

In a rapidly converging OT/IT landscape, this creates an opportunity to transition from proprietary approaches to open, standardized solutions. Success in this space is driven by strong collaboration across the industrial ecosystem, including Standard Development Organizations and joint working groups.

Organizations that embed cybersecurity as a core element of connectivity not only ensure compliance but also strengthen their position as trusted partners in the evolving digital industrial landscape.”

Endress+Hauser 



Hans-Joachim Fröhlich is the Director of Technology and Portfolio at Endress+Hauser

Help shape next year's report

Last year we opened up the conversation. Industrial and automation professionals from around the world shared how they see the future of industrial networking and much of what you've read in this report comes directly from what they told us.

Now we're asking again.

The Future of Industrial Networks survey

takes a few minutes. You can answer the core questions and stop there, or go deeper on the topics most relevant to your work: IIoT, wireless, cybersecurity, or designing industrial communication interfaces.

Everyone who contributes receives the full 2027 report ahead of public release.

Scan the code or go to the URL. Add your voice.
See your industry through the eyes of your peers.

<https://emea.dcv.ms/HiR3OKBjV5>



STATE OF INDUSTRIAL NETWORKS *2026*



| Hardware Meets Software™