IT-OT Convergence Impact on Networking

An Industry IoT Consortium Tech Brief

2022-08-02

Authors

Marinos Charalambides (Huawei), David Lou (Huawei).

In recent years, information technologies (IT) have been progressively integrated into operational technologies (OT) to enhance the value these systems deliver by sharing data between them. This is known as IT/OT convergence [CIG19]. It allows traditional manufacturing equipment to communicate beyond the boundaries of industrial installations, enabling remote monitoring and analysis and control of physical devices. Key benefits of IT/OT convergence include improved system efficiency and flexibility (since the physical operations of devices can be managed centrally), reduced operational expenditure (by allowing extended autonomous operation) and improved uptime (based on, for example, predictive maintenance analytics).

With IT penetrating industrial infrastructure, traffic is no longer confined to the control domain; rather, it is communicated over the internet to remote management stations and data centers. This causes a paradigm shift, which poses new requirements on the network. This technical brief identifies such requirements based on a representative set of scenarios and discusses them in reference to the limitations of current networking technologies. Solutions can be used in the design of future industrial networks to meet the needs and constraints of industrial applications.

1 Scenario-Driven Requirement & Analysis

There are three types of scenarios emanating from controlled environments, known as *limited domains* [CAR20] that are used to derive network requirements. Analysis of these requirements aims to identify the limitations and challenges of current technologies.

1.1 Low-Power IoT Networks

With the goals of low power consumption and low total cost of ownership, IoT networks comprise inexpensive devices that are constrained in terms of computational capacity, memory and energy consumption. Low device complexity defines the properties of communication technologies developed for this limited domain, which use short (16-bit) addresses to reduce the header size, communication overheads and memory requirements. IPv4 32-bit addresses are already long, resulting in expensive operations in multi-hop routing scenarios, while IPv6 128 bit-addresses worsen the problem and would not fit within the maximum transmission unit of some IoT protocols [SET17]. Header-compression techniques can decrease the IPv6 overhead. But they involve power-hungry operations inappropriate for resource-constrained IoT devices and so require gateways. Expensive operations are also necessary when separate IoT networks need to connect through the internet as short, local addresses require translation to and from IP addresses.

Addresses can take various forms to identify communication end-points, physical objects, data types and locations within a geographic area [AIOTI18]. Due to its inherent rigidity with only a single addressing semantic of topological location, IP is not able to offer the flexibility expected by many application scenarios. Support for multiple semantics would be lost in a scenario where translation between local and IP addresses is needed when connecting IoT networks.

1.2 Highly Dynamic Network Topologies

1.2.1 Satellite Networks

Based on their wide coverage, satellite networks can provide global Internet connections in cases where terrestrial networks are hard to deploy or present an economically non-viable solution. Examples include unpopulated or low user density areas, the majority of seas and all oceans, which, according to [LOU21], constitute at least 80% of the Earth's surface. Hence, providing internet connectivity to aircraft, ships and users in remote locations can be achieved only with satellites. Satellite networks are characterized by constantly changing network topologies [HAN21]. This renders the fixed IP semantic of topological location restrictive because the relation between network nodes and the user endpoint changes all the time. As identified in [JIA21], IP requires maintaining and updating the topological addresses frequently, which is a challenge.

1.2.2 Vehicular Networks

Another limited domain with highly dynamic topologies is vehicular networks, where the communication is over direct links between vehicles and roadside infrastructure. The latter has better processing capabilities but can involve multi-hop connections between vehicles [JEO21]. Example services include collision avoidance using collaborative object recognition across vehicles, and conveyance of road-status information for safety and for the reduction of journey times. As with satellite networks, the topology of these networks changes constantly due to the dynamic nature of the communicating nodes and IP, thus faces the same challenges.

1.3 Proprietary Small-Scale Networks

1.3.1 Power Utility Networks

The communication infrastructure in utility networks, such as the smart grid, is mainly responsible for transporting data between utility equipment and the control center. This acts as an enabler for several use cases, such as:

- advanced metering to collect and analyze energy consumption data for outage detection and billing purposes,
- demand-side management for regulating the consumption of electric energy,
- monitoring of electricity generation from distributed renewable energy sources,
- selection of charging stations for electric vehicles,
- remote monitoring and control of assets for fault detection and automated power restoration and
- wide-area situational awareness for preventing power supply disruption.

Due to the diversity of use cases, power utility networks present various types of requirements. Reliable communication is prime, especially for wide-area situational awareness (i.e. the last use case that may need up to six 9s), and some use cases that require low communication latency, (20 ~ 200ms). While current technologies can support the expected reliability and latency levels, internet providers find it challenging to guarantee such levels in their networks.

Another key requirement is security. Attacks on utilities that result from exposure to the internet can disrupt the supply of electricity and have an adverse effect on daily lives and economies. Privacy is also a concern when sensitive data is transmitted over public networks, such as the first and fourth use cases. When intercepted, such data can reveal power consumption patterns of individuals, which is a violation of privacy laws. Network-level solutions are needed that go beyond current point-to-point security and realize strong encryption and anonymization.

1.3.2 Manufacturing Networks

Flexible and highly automated smart factories are part of the Industry 4.0 vision, where machines and production assets are augmented with ubiquitous connectivity and compute capabilities that allow management processes to make autonomous decisions. The networking requirements in this limited domain are deterministic performance guarantees to ensure tight synchronization between components of the production line, high reliability and strong security to avoid misconfigurations and costly downtime.

While isolated, small-scale manufacturing plants can have extremely low latency (and high reliability) thanks to technologies such as time-sensitive networking (TSN), this is difficult to achieve in large scale networks. Traffic exchanged with management/control processes running in data centers, or even edge micro-clouds, is affected by the limitations of a shared network infrastructure in terms of performance and security.

1.3.3 Healthcare Networks

The vision of future healthcare establishments is digitally enhanced and highly connected. Traffic on hospital networks is dominated by patient data, which can be generated by medical equipment (e.g. imaging devices) or manually (e.g. medical record updates) and subsequently accessed for diagnostic or monitoring purposes. Such data is personal, so when it is stored in a data center or shared over the internet, care must be taken to avoid leaks. Remote surgery, for example, requires strict performance guarantees for latency, bandwidth and reliability, which cannot be supported by current internetworking technologies.

2 Discussion

We now focus on addressing security and performance.

2.1 NETWORK ADDRESSING

Extending the communication beyond the boundaries of industrial environments,[1] requires using standardized L3 protocols. While the Internet Protocol is the de facto L3 protocol for internet-based communications, it has inherited several scalability and applicability limitations in its original design. Although IPv6 solves the problem of address depletion, it inherits a number of IPv4 problems, such as the fixed number of address bits and the fixed semantics associated with them. Significantly more flexibility in network addressing, both in terms of length and semantics, is needed to support aforementioned networking scenarios.

Flexibility in the address length, which can also be seen as elasticity in the address space, caters to an increasing number of specialized network deployments. It would allow networks to use the length that best fits their scale and constraints. This feature is driven by the long-standing recognition of the IP-header overhead and would be particularly beneficial to low-power scenarios, like IoT networks that cannot handle long addresses. Although header compression techniques [GOM17] have been proposed to address this, they involve non-trivial processing and so would require additional network equipment. In addition, flexible addressing in IoT networks enables seamless communication between nodes, bypassing the need for expensive address mappings, and thus simplify the network architecture.

IP addresses are semantically rigid and refer only to the topological location of a network interface. The address structure should be flexible enough to support multiple semantics and related locators that apply to environments with highly dynamic topologies, such as those in satellite and vehicular networks. In addition to reducing the complexity of such networks, a flexible addressing scheme allows for richer policies that enhance packet treatment in terms of routing performance and security. A representative example is the approach in [ZHE21], which uses semantic addresses to represent virtual switches at the fixed space locations (based on geo-coordinates) being traversed by satellites. Reduced service disruptions caused by the satellite handover events have been reported as the key benefit.

Key takeaway: Flexibility in network address length and structure can enable seamless communication between limited domains and the internet and extend the semantics that allow for enhanced packet treatment.

2.2 SECURITY AND PRIVACY

Historically, many OT systems had little or no connectivity, so security was an issue only when physical access was obtained. When there was connectivity, the castle-and-moat security model was used to protect resources from unauthorized access. This involves the implementation of a

[1] These environments mainly rely on L1 and L2 communication protocols such as Industrial Ethernet [ROJ10], Fieldbus [NAY12][KAU19], and LPWAN [WAL18][ISM18] technologies.

strong network perimeter with firewalls and intrusion detection/prevention systems to block external attacks [SUN18].

Connecting the OT infrastructure externally and maintaining data in remote locations (e.g. data centers) puts immense pressure on this model due to the increased risk of attacks to the security and privacy of assets and processes. This is especially relevant for critical power utilities, manufacturing, and healthcare establishments that handle sensitive patient data. The current networking layer security mechanism (IPSec) is complex, lacks adequate communication latency and end-to-end support and lacks privacy mechanisms.

IT/OT convergence requires new security models. One such model is zero-trust security [ROS20], which assumes risks from any type of communication, both within and outside the network perimeter, and requires strict verification for every user and device on the network. The main principles of this model include:

- least-privilege access to users,
- network segmentation into small security zones that enable access to the intended applications and systems without requiring complex firewalling,
- access control on a per device basis and
- multi-factor authentication.

The zero-trust model is a core component of the secure access service edge architecture (SASE) [MAC19], an attractive security solution that can connect users to enterprise networks from any location via any device. SASE overcomes the complex and silo management of traditional access control solutions by streamlining the implementation of network security controls (e.g. DDoS protection) at the edge, for example through unified policy management across all network traffic.

Key takeaway: New security models are required to protect against increased risk of attacks in limited domains, which should implement strong access control and authentication mechanisms.

2.3 Network Performance

In many industrial scenarios data, is exchanged over relatively short distances and dedicated network links, which results in extremely small delivery latencies thus creating highly reactive conditions and enabling tight synchronization among processes [IEC19]. Connecting the equipment with remote management stations and data centers implies that data might need to travel over considerable distances and shared network infrastructures. This can affect the communication performance, which needs to adhere to strict QoS expectations.

While some internet providers support MPLS and DiffServ technologies that have been developed for this purpose (e.g. [VER16]), service quality is difficult to guarantee even over a single administrative domain. More recent technologies can reduce communication latency by bringing processes executing in the date center closer to the industrial infrastructure [LIN20].

This is useful in the smart manufacturing domain where control processes can be offloaded to compute nodes located at the edges of operator networks. The in-network computation paradigm can also support other processing needs like digital twinning, advanced data analytics and inference, e.g. for quality assurance. To complement latency reduction based on local computation, virtualization technologies and slicing of 5G network resources can provide soft communication performance guarantees.

Key takeaway: To satisfy the high expectations on communication performance, computational resources can be installed close to manufacturing plants, for example at provider network edges, so as to maintain short communication distances.

3 CONCLUSIONS

The penetration of IT into industrial installations undoubtedly brings significant advantages that increase the value of such infrastructures, but at the same time pose challenges for the network given that traffic is no longer isolated. This technical brief followed a scenario-driven approach through which network requirements are identified and discussed. Based on current networking technologies and their limitations, key takeaways were derived concerning network addressing, security and performance.

4 REFERENCES

- [AIOTI18] Alliance for Internet of Things Innovation, “Identifiers in Internet of Things,” February 2018. Available at: *https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf*
- [CAR20] B. Carpenter, B. Liu, “Limited Domains and Internet Protocols,” RFC8799, July 2020.
- [CIG19] Cigref report, “IT/OT convergence: A fruitful integration of information systems and operational systems,” December 2019. Available at: *https://www.cigref.fr/cigref-report-it-ot-convergence-a-fruitful-integration-of-information-systems-and-operational-systems*
- [GOM17] C. Gomez, J. Paradells, C. Bormann, J. Crowcroft, “From 6LoWPAN to 6Lo: Expanding the Universe of IPv6-Supported Technologies for the Internet of Things,” IEEE Communications Magazine, Vol. 55, No. 12, pp. 148-155, December 2017.
- [HAN21] L. Han, R. Li, ”Problems and Requirements of Satellite Constellation for Internet,” Internet Draft, July 2021.
- [IEC19] International Electrotechnical Commission, “Industrial communication networks - Fieldbus specifications,” IEC 61158, International Standard, 2019.
- [ISM18] D. Ismail, M. Rahman, A. Saifullah, “Low-power Wide-Area Networks: Opportunities, Challenges, and Directions,” International Conference on Distributed Computing and Networking, January 2018.

- [JEO21] J. Jeong, "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases," Internet Draft, September 2021.
- [JIA21] Y. Jia, et al., "Challenging Scenarios and Problems in Internet Addressing," Internet-Draft, July 2021.
- [KAU19] A. Kaur, M. Corsar, B. Ma "Application of Fieldbus Technology to Enable Enhanced Actuator Control of Automated Inspection for Offshore Structures," Applied System Innovation, Vol, 2, No. 3, 2019.
- [LIN20] P. Lin, S. Carlini, "Industry 4.0: Minimizing Downtime Risk with Resilient Edge Computing," Schneider Electric White Paper 287, 2020. Available at: https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=WP287_V1_EN.pdf&p_Doc_Ref=SPD_WP287_EN
- [LOU21] D. Lou, et al., "The Industrial Internet of Things Networking framework," Industrial Internet Consortium, July 2021.
- [MAC19] N. MacDonald, L. Orans, J. Skorupa, "The Future of Network Security Is in the Cloud," Gartner, August 2019.
- [NAY12] C.G. Nayak, et al., "A case study on application of Fieldbus in the automation of Coke Oven Battery," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 1, No. 9, November 2012.
- [ROJ10] C. Rojas, P. Morell, "Guidelines for Industrial Ethernet infrastructure implementation: A control engineer's guide," IEEE-IAS/PCA 52nd Cement Industry Technical Conference, pp. 1-18, March 2010.
- [ROS20] S. Rose, O. Borchert, S. Mitchell, S. Connelly, "Zero Trust Architecture," Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2020. Available at: *https://doi.org/10.6028/NIST.SP.800-207*
- [SET17] P. Sethi, S.R. Sarangi, "Internet-of-Things: Architectures, Protocols and Applications," Journal of Electrical and Computer Engineering, January 2017.
- [SUN18] C.C Sun, A. Hahn, C.C. Liu, "Cyber Security of a Power Grid: State-of-the-art," International Journal of Electrical Power & Energy Systems, Vol. 99, pp.45-56, 2018.
- [VER16] Verizon, "Making the Case for MPLS in the Modern Enterprise," White paper, 2016. Available at: https://www.verizon.com/business/resources/whitepapers/2016/mpls_whitepaper.pdf
- [WAL18] J. Walsh, "Low Power Wide Area Technologies for IoT Use Cases," SCTE-ISBE and NCTA October 2018. Available at: https://www.nctatechnicalpapers.com/Paper/2018/2018-low-power-wide-area-technologies-for-iot-use-cases-technology-assessment-for-msos/download
- [ZHE21] G. Zheng, et al., "Virtual Data-Plane Addressing for SDN-based Space and Terrestrial Network Integration," In proceedings of 22nd IEEE International Conference on High Performance Switching and Routing (HPSR), 2021.

AUTHORS & LEGAL NOTICE

Authors: The following persons contributed substantial written content to this document:

Marinos Charalambides is a senior researcher at Huawei, Belgium. Prior to this he was with University College London for twelve years. He received a B.Eng. in electronic and electrical engineering (first class), an M.Sc. in communications networks and software (distinction), and a Ph.D. in policy-based network management, all from the University of Surrey, United Kingdom, in 2001, 2002, and 2009, respectively. He has worked in a number of European and UK national projects since 2005, and his research interests include software-defined networking, IoT, dynamic resource management, distributed systems, and in-network computing/caching.

David Lou graduated as Ph.D. in Electronic Engineering at Ghent University in 2005. In the same year he joined the Alcatel-Lucent Bell Labs as an Innovation Researcher. He had a leading involvement and management role in several European and national research projects (Giant, Smart Touch, Metaverse1, Mistra, Shift-TV, etc.), and standardization bodies (MPEG). In 2016 he joined Huawei Technologies as a Chief Researcher based in Munich, Germany. He is responsible for defining the research strategy, steering disruptive network innovation and coordinating collaboration with industrial and academic partners. He is also leading the standardization activities in various SDOs (e.g. ITU-T, IETF, ETSI, etc.) His interests mainly cover IoT/IIoT/I4.0, next generation industrial networking architecture, deterministic communication, network privacy, video streaming and transportation, and immersive communication. He is the co-chair of the IIC Networking Task Group and has been actively involved in relevant industrial development activities. He has (co-) authored more than 30 scientific publications and white papers. He has been granted with more than 20 patents.