ADVANTECH
Enabling an Intelligent Planet

intel partner Titanium

Securing Real-Time Operations: Integrating TSN and Cybersecurity in Industrial Systems

In today's evolving industrial environment, integrating Time-Sensitive Networking (TSN) with cybersecurity measures is crucial for improving operational efficiency and security.

Advantech Authors:

- Kunhong Chen <Kunhong.Chen@advantech.com.tw>
- Frank Kuo <Frank.Kuo@advantech.com.tw>

Abstract

This white paper delves into the structure, advantages, and obstacles of merging TSN with robust cybersecurity protocols. TSN offers deterministic, low-latency communication, which is vital for time-sensitive applications, while cybersecurity ensures the protection of assets and the integrity of systems. The document explores the synergies and compromises between these technologies in various sectors such as transportation, energy, utilities, maritime, and factory automation. By adhering to standards like IEC 62443 and TS 50701, it offers a roadmap for optimizing performance and defending against cyber threats, empowering industries to navigate digital transformation confidently.

01 Foreword

In today's rapidly evolving industrial landscape, the integration of TSN and security stands as a pivotal frontier, shaping the course of operational efficiency and security across diverse sectors. As industries push for greater precision, responsiveness, and resilience in their operations, the need to incorporate TSN technologies alongside robust cybersecurity measures presents both a necessity and a challenge.

This exploration navigates the complex terrain where real-time demands intersect with the imperative of safeguarding assets against cyber threats. It delves into the intricate architecture, functionalities, benefits, and potential drawbacks of integrating TSN into time-critical processes, while also addressing the critical aspect of cybersecurity for asset protection. TSN embodies performance and productivity, while cybersecurity underscores caution, protection, and meticulous verification—two seemingly opposing directions in designing industrial systems.

As industries strive to optimize performance and enhance defenses in an increasingly interconnected environment, comprehending the synergies and trade-offs between TSN and cybersecurity becomes essential. Through an examination of the technological intricacies, operational benefits, and strategic implications inherent in this convergence, this article aims to offer stakeholders a comprehensive roadmap for navigating the complexities of modern industrial systems.

By exploring the synergies and trade-offs inherent in these technologies, organizations can develop holistic strategies that prioritize both performance and protection. Our goal is to provide insights into overcoming the challenges posed by this intricate convergence, empowering stakeholders to leverage the full potential of TSN while fortifying systems against cyber threats in today's dynamic industrial landscape.

02 Time-Sensitive-Network (TSN)

TSN, or Time-Sensitive Networking, comprises a series of IEEE 802.1 task forces focused on refining Ethernet network capabilities to meet the stringent demands of time-sensitive applications. Its goal is to facilitate deterministic, low-latency communication while ensuring high reliability and scalability. One significant challenge lies in configuring critical and non-critical data flows within the same infrastructure without compromising real-time performance.

In the transportation sector, TSN plays a crucial role in addressing the exacting requirements of various applications, particularly those related to safety, reliability, and real-time communication. It finds applications across diverse transportation domains, including autonomous vehicles, railway systems, aviation, fleet management, and traffic management systems.

Here we would like to give you some examples to show how it can do in the future.

1. *Existing network technologies over TSN:*

According to the OSI 7 Layer model, certain layer modifications do not necessarily impact others. This characteristic opens opportunities for technologies like IEEE 802.11 Wi-Fi (WTSN), EPON, MPLS (DETNET), among others, to potentially incorporate aspects or even full implementations of TSN technology. For instance, the IEEE 802.1CB standard facilitates data replication within MPLS networks.

2. *FA Process control and Emergency shutdown:*

Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Emergency Shutdown systems are pivotal applications in process control automation. Presently, numerous vendors are integrating TSN technology into their equipment, potentially replacing traditional Industrial Ethernet in automation systems. Examples include CC-Link IE TSN, OPC UA TSN, and similar solutions.

*To learn more about **Time-Sensitive Networking**, please download **[White Paper]***

3. V2X over TSN

With Advanced Driver Assistance Systems (ADAS) and Electric Vehicle (EV) technology gaining significant traction, car manufacturers are increasingly integrating TSN technology across various components such as on-board switches, embedded PCs, and engine control computers. Leveraging TSN technology, ADAS-equipped vehicles can now communicate with other vehicles or road infrastructure seamlessly, so called V2X.

4. TSN for Maritime Autonomous Surface Ship (MASS) and Drones

As unmanned ships, trucks, drones, UAVs, and robotic vehicles continue to advance, TSN emerges as a valuable asset for facilitating remote control and access with minimal latency and precise operation. When integrated with Data Distribution Services (DDS), TSN further enhances deterministic communication, allowing engineers to design distributed avionic systems that define and uphold Quality of Service (QoS) standards for critical data streams, marking a significant advancement in operational efficiency and reliability.

5. TSN for Military & Aerospace

As time progresses, humanity increasingly sets its sights on space exploration, with endeavors such as missions to Mars gaining momentum. Cutting-edge technology is being incorporated into spacecraft as well as various military equipment, including radar, sonar, and control or navigation systems (C4ISR). TSN/Wireless Time-Sensitive Networking (WTSN) emerges as a critical asset in these applications, offering advantages such as low latency, precise timing synchronization, and data duplication capabilities to mitigate misunderstandings in object detection or ensure accurate delivery of action commands.

6. TSN for Infrastructure and transportation (Roadway / Railway)

When it comes to infrastructure like power utilities or transportation, which are integral to our daily lives and play crucial roles in various scenarios, ensuring low latency, preventing data loss or errors, and enhancing safety are paramount. TSN is now being deployed in these mission-critical applications to achieve these objectives. With the

integration of TSN, we anticipate improved quality of data acquisition and control, particularly for applications covering long distances and involving large quantities of devices. Furthermore, TSN enhances human safety and system reliability, contributing to the overall efficiency and resilience of these vital infrastructure systems.

03 Security

The merging of IT (Information Technology) and OT (Operational Technology) systems has fostered greater connectivity between once-separate environments. This integration has yielded enhanced efficiency, heightened visibility and operational control, and improved decision-making for organizations. However, IT and OT systems possess distinct security needs and confront unique cyber threats.

Consequently, specialized security measures and collaboration between IT and OT security teams are essential to safeguarding systems against cyber threats. To achieve this, organizations must enlist security professionals proficient in both IT and OT security. This ensures the safety and security of critical infrastructure and processes.

ADVANTECH IT/OT TOTAL SECURITY

The IEC 62443 series serves as a global standard focusing on cybersecurity for operational technology within automation and control systems. On the other hand, TS 50701 offers more targeted guidance specifically tailored to addressing cybersecurity within the railway sector. TS 50701 aims to strike a balance between being self-contained and avoiding redundancy with the existing content covered in IEC 62443.

By drawing upon the foundational principles and methodologies established in IEC 62443, industries can craft standards tailored to their specific sectors, effectively addressing the unique cybersecurity challenges and requirements of their operational environments. These sector-specific standards offer a comprehensive framework for mitigating risks, protecting critical assets, and cultivating resilience against cyber threats across a wide array of industries.

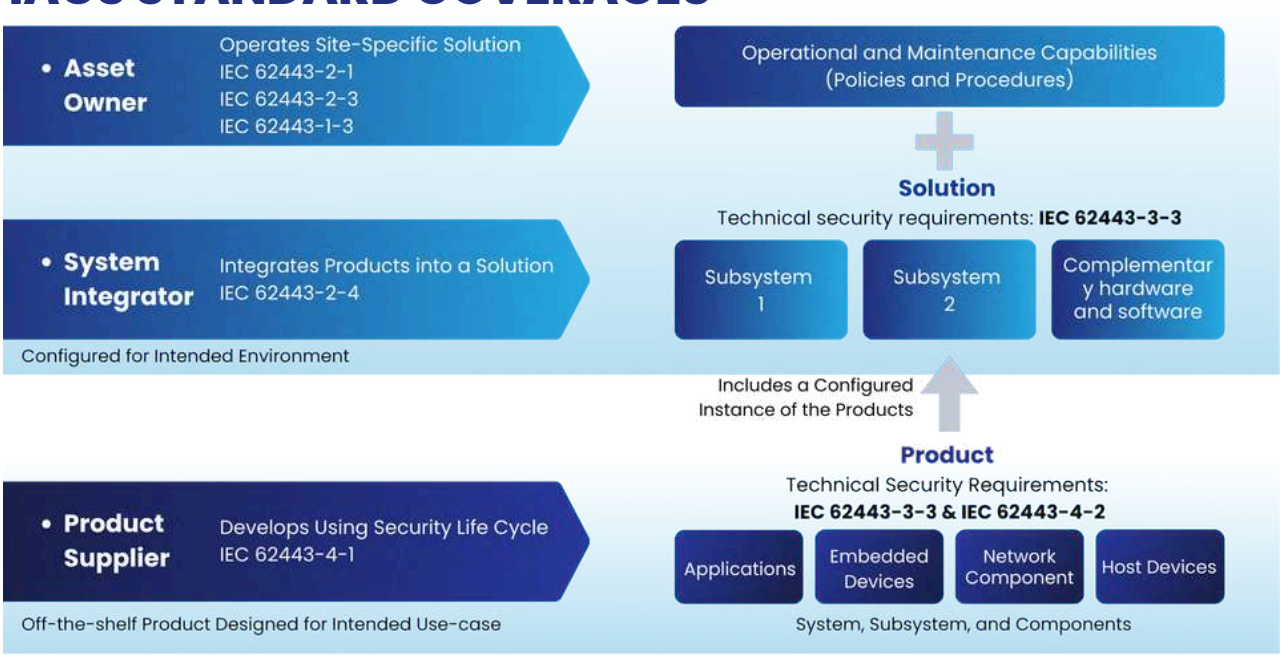
MANY STANDARDS REFER TO IEC-62443

IEC 62443 offers a comprehensive framework tailored to assess, implement, and sustain cybersecurity measures, specifically designed to meet the unique needs of industrial sectors. Serving as a cornerstone for enhancing cybersecurity in industrial automation and control systems (IACS), this framework provides invaluable guidance, standards, and best practices to empower organizations in safeguarding their critical infrastructure assets against cyber threats. Key components and features of IEC 62443 span various areas, including system scope and overview, risk management, security management systems, technical security requirements, lifecycle considerations, and compliance and certification protocols.

The IEC 62443 standard is structured into four primary categories: General,

Policies and Procedures, System, and Components, each addressing different aspects of cybersecurity in industrial environments. This globally recognized standard establishes a framework for implementing robust cybersecurity measures across the entire lifecycle of IACS.

IACS STANDARD COVERAGES



To ensure compliance with IEC 62443-4-2 and enhance the security of industrial control systems, leveraging advanced technologies and solutions is crucial. Advantech Embedded Systems, equipped with pre-integrated security features, play a significant role in meeting the standard's requirements and ensuring robust cybersecurity measures.

To provide a clearer understanding of security requirements and how they align with Advantech, a set of security primitives (SP) has been identified. These security primitives establish a common language across standards, facilitating a more transparent mapping of security features in IoT systems to the security requirements of IEC 62443-4-2. Here are key security primitives where Advantech Embedded Systems offer valuable capabilities.

Refer to the figure on the next page for a comprehensive view of the architecture, which elucidates the IEC 62443 standard, highlights the benefits of leveraging Advantech's Embedded System, aligns security requirements with corresponding security primitives, and furnishes practical examples demonstrating how an Advantech Embedded System can fulfill the specific mandates of IEC 62443-4-2.

SECURITY STACK FOR IEC 62443 REQUIREMENTS

Advantech provides robust security capabilities such as secure boot, access control, secure communication, security monitoring, firmware updates, and physical security measures. These features align with the foundational requirements outlined in IEC 62443-4-2, empowering OEMs to construct secure and resilient industrial control systems.

To ensure the safety of Industrial Automation and Control Systems (IACS), countries and industries widely adopt the concepts, methods, and models delineated in IEC 62443 when formulating policies. Notably, IEC 62443-4-1 and IEC 62443-4-2 are instrumental in ensuring that system components meet safety requirements, ensuring compliance with safety regulations throughout the development and production phases, covering both process and product verification.

In 2020, Advantech secured the IEC 62443-4-1 certification for its product safety development system, affirming its commitment to adhering to stringent safety standards. Subsequently, in November 2021, Advantech obtained the IEC 62443-4-2 certification, marking another milestone in its dedication to cybersecurity. This certification, validated by TUV NORD Taiwan, underscores Advantech's unwavering commitment to providing secure solutions for industrial control systems.


TUV NORD

Certificate

04 Balance between TSN and Security

Integrating TSN (Time-Sensitive Networking) and cybersecurity features into our industrial automation systems presents a challenge in balancing optimal performance and security. This is akin to choosing between TCP and UDP, where prioritizing one comes at the expense of the other. Cybersecurity measures often require significant CPU and memory resources to analyze data flow, whereas TSN is designed to improve the efficiency and accuracy of data transmission.

Balancing these priorities effectively has become crucial. Achieving the right equilibrium between cybersecurity and performance optimization is now a significant concern. Although cybersecurity is essential, extensive data protection and inspection consume CPU and memory resources and cause data transmission delays. Integrating both TSN and cybersecurity can be problematic because TSN/QoS/Time Synchronization already occupies a lot of hardware resources, and adding cybersecurity exacerbates the issue. TSN aims to ensure smooth traffic flow, while cybersecurity introduces delays. Achieving both simultaneously is challenging. How can we solve this problem when designing an ideal network system?

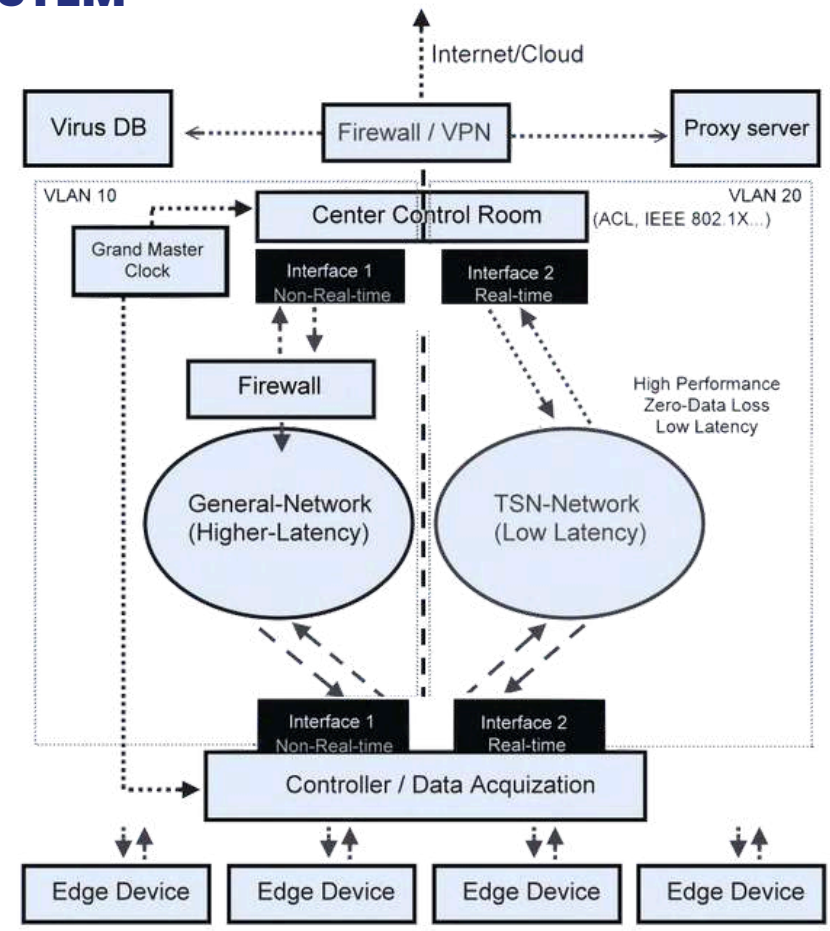
Besides being a target for attacks, the timing aspect also affects the application of certain security measures. For instance, if an OT system requires firewall protection but the firewall cannot check data packets in real time due to hardware performance limitations or software load capacity issues (such as with Deep Packet Inspection, DPI), this creates a transmission delay. If not considered from the start, this can cause a conflict between data and their intended time slots.

One solution to this issue is using firewall technologies that filter in real time, although these can be expensive and difficult to implement. Another factor contributing to delay is the network devices themselves, which typically operate using store-and-forward technology with internal buffers. Data experiences delays when entering and exiting these devices, and the more devices involved, the longer the delays.

To mitigate this, the calculation of the TDMA (Time Division Multiple Access) method schedule can be integrated to reduce the impact of data transmission delays in the network system.

Depending on the application requirements, even visible delays can trigger alarms or cause system control failures. Therefore, network planning should involve segmentation and boundary setup. Whether through VLAN group settings or media path control, it's essential to consider the performance of both time-sensitive and non-time-sensitive segments and integrate them properly into the network. The diagram below illustrates the concept of this network design and device allocation.

TSN & CYBERSECURITY SEAMLESS INTEGRATION FOR IT/OT SYSTEM



This approach aligns with the established methods of zones and conduits, adding an additional TSN aspect. Subdividing a network into communication zones separates areas and restricts communication to what is strictly necessary. TSN networks introduce an extra layer of time requirements, addressing not only the need to communicate but also the timing of communication. In other zones, a general time frame might be sufficient for information collection and overall operation. While all zones need to sync from the master clock, the required level of accuracy can vary between them.

In this way, an additional established security concept, "Defense in Depth and Diversity," is implemented alongside zones and conduits. This concept involves connecting various security mechanisms in series to create an in-depth defense. On one side, there are classic security mechanisms at the network access level (Network Access Layer Security), such as IEEE 802.1X, ACL, encryption, account/password (defined by IEC-62443 standard), and even VPN tunnels. These mechanisms are implemented in switches and routers to protect direct access to the TSN network. On the other side, the TSN specification also includes mechanisms designed for this purpose.

05 Design TSN & Security Architectures

We will guide you on how to design an architecture that leverages the benefits of TSN and optimizes security in industries including railway, roadway, power & utility, marine, and factory automation.

1. Railways

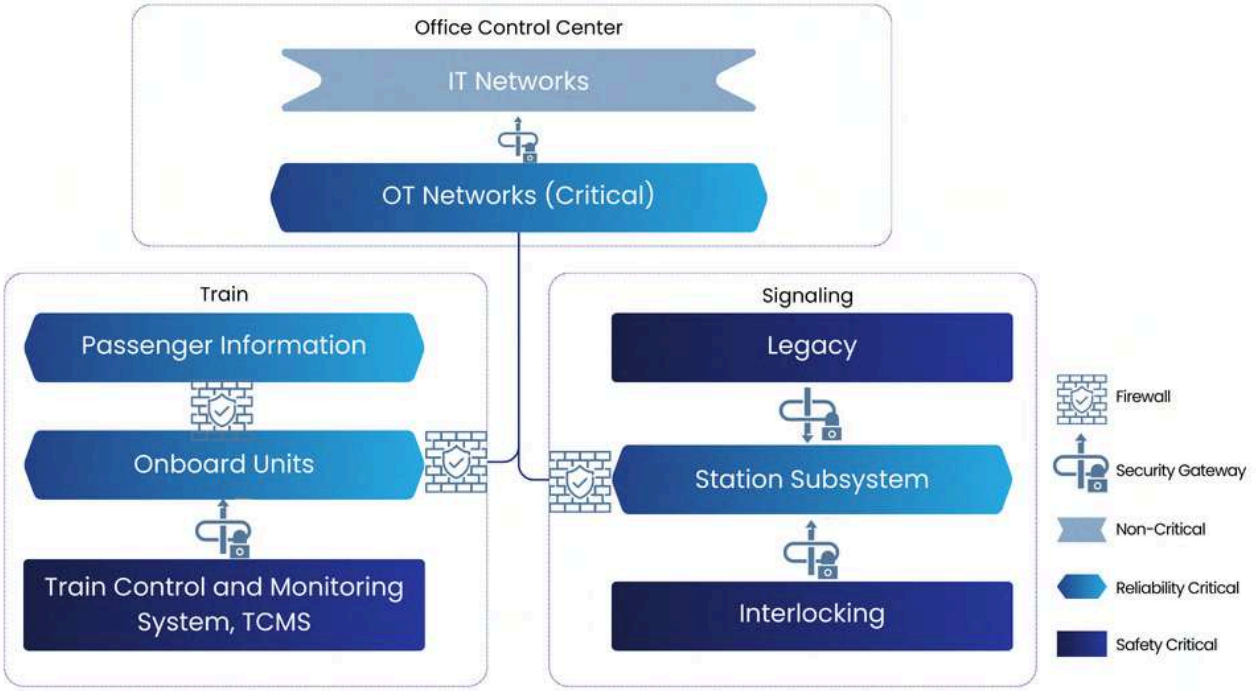
The digitalization of rail systems has significantly improved efficiency and customer service. However, this transformation requires increased connectivity, exposing previously isolated networks at the Operations Control Center (OCC) to IT networks and the Internet. This expanded connectivity greatly increases the rail system's vulnerability to cyber threats, posing significant risks to rail operators and the public.

This heightened cyber risk is especially concerning for vital networks at control centers, such as those responsible for signaling, train safety, and energy management. Safety and security in these critical systems are governed by distinct standards and regulations, managed by different stakeholders, and cannot be easily unified into a single program. Nevertheless, cybersecurity in these vital networks is essential for ensuring safety. Standards such as EN 50129 mandate strict control over cyber operations to meet safety requirements. Consequently, rail system operators urgently need robust cybersecurity designs and solutions capable of thwarting sophisticated cyber-attacks on vital networks, both now and in the future.

In modern railways, the routine exchange of information between vital networks and non-critical IT systems within the OCC, or with external networks via the OCC, is crucial for digital operations. However, this connectivity must not compromise the safety and reliability of operations due to potential cyber-attack vulnerabilities.

Since all cyber-attacks involve the transmission of information, rail operators must establish robust controls over data flow, especially regarding any information or embedded attacks from less secure zones entering safety-critical or reliability-critical areas. All equipment within these zones must be managed with the same level of security as the most sensitive devices, as attacks can propagate within a connected environment. To enhance performance and safety in safety-critical zones, TSN technology is utilized, along with latency and redundancy mechanisms. While firewalls can segment sub-networks within a security zone, communication between zones with different security levels should occur only through unidirectional gateways. This approach ensures that critical systems remain protected from potential cyber threats originating from less secure areas.

RAILWAY SYSTEMS FACING POTENTIAL CYBER THREATS



Security zones, as defined by IEC 62443, group logical or physical assets that share common security requirements. These zones can be hierarchical and include subzones, which help segregate equipment based on different communication needs. Categorizing networks into three levels of criticality—safety, reliability, and efficiency—simplifies network security procedures and protocols.

Subzones are essential for distinguishing equipment with varying communication requirements. However, it is crucial to carefully manage interfaces between zones of different criticalities. Less-critical equipment may reside in more critical networks, but stringent management ensures that all equipment in the more critical network meets its criticality level. For example, computers and networks essential for efficient operations typically belong to non-critical zones since they are neither safety-critical nor reliability-critical. However, when it is more cost-effective or practical to host efficiency-critical equipment in reliability-critical or safety-critical zones, it is permissible as long as the efficiency-critical systems are secured to the same level as the hosting zone.

Many industrial security standards advocate for unidirectional gateways over firewalls, citing several reasons for their superiority:

- ***Unidirectional Protection***

  All cyber attacks involve the transmission of information, and firewalls permit bi-directional communication. This inherent directionality makes firewalls

vulnerable to certain types of cyber attacks, even when communications are encrypted. Cryptosystems can encrypt attacks as easily as legitimate communications, making firewalls porous to infiltration.

- ***Vulnerability of Firewalls***

  Firewalls are software-based and consequently susceptible to security vulnerabilities. Regularly monitoring firewall vendors' websites reveals frequent security updates, indicating the discovery of new vulnerabilities. As adversaries exploit these vulnerabilities before patches are available, rail systems face significant exposure to cyber threats.

- ***Routed Traffic***

  Firewalls, acting as routers, forward allowed network traffic between networks. Attackers can exploit this functionality by embedding their attacks within seemingly permitted traffic. This makes it easier for adversaries to bypass firewalls and launch successful cyber attacks.

In summary, unidirectional gateways offer a more robust defense mechanism against cyber threats compared to firewalls, addressing vulnerabilities inherent in bidirectional communication, software-based systems, and routed traffic forwarding.

2. Roadway

In the realm of road transportation, the fusion of TSN technology with advanced security measures presents a transformative opportunity to elevate the performance and safety of autonomous vehicle systems.

TSN technology, an extension of Ethernet protocols designed for time-sensitive applications, ensures reliable and real-time communication. By leveraging TSN, vehicles can establish efficient communication with infrastructure and other vehicles, achieving precise timing and synchronization. This synchronization enhances the responsiveness and accuracy of autonomous vehicle systems, contributing to safer roadways.

A key advantage of TSN is its ability to seamlessly integrate IT and OT networks. This integration allows devices previously isolated within control networks to be configured and managed via TSN networks without needing communication reconfiguration. Additionally, TSN-capable network switches enhance

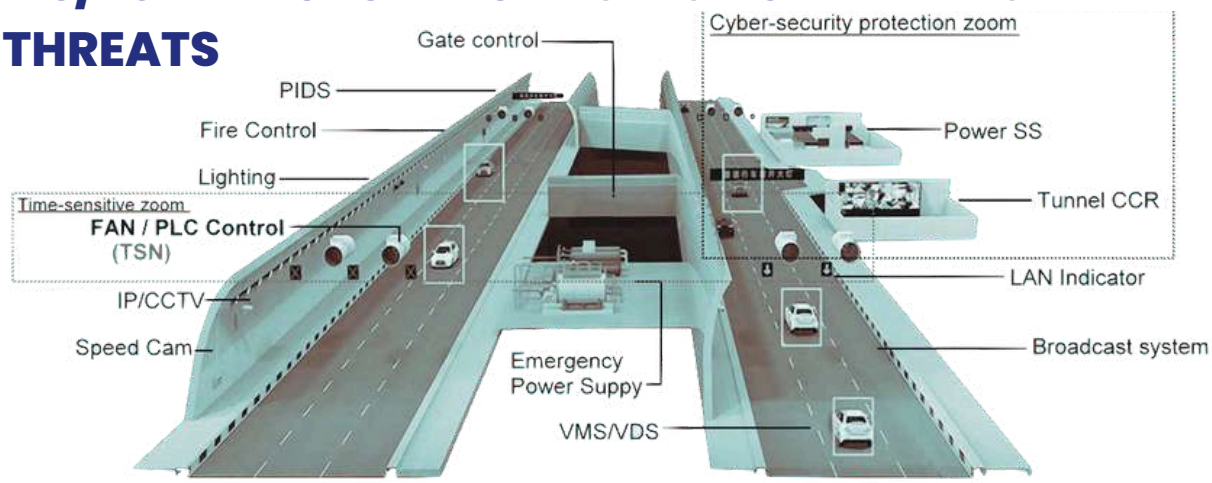
network management, while incorporating control networks into the information network enables Ethernet security solutions to monitor and protect a broader array of devices.

Consider a road tunnel application as an example. Modern tunnels longer than 500 meters require comprehensive safety and reliability systems for smoke exhaust and human safety. In the event of an accident, the top priority is ensuring people can escape quickly and safely, without interruptions or dangers. TSN can be implemented alongside SIL2-4 PLC/SCADA systems for fan control and air exhaust, which are critical during an emergency.

Moreover, various subsystems must be integrated and connected to the Center Control Room (CCR) for centralized control and monitoring. Cybersecurity is crucial in this context to protect the entire system from threats, viruses, and unauthorized access.

By marrying TSN technology with robust security measures in road transportation, we can realize heightened efficiency and safety in autonomous vehicle systems. This integration holds the promise of smarter, safer, and more sustainable traffic management, ushering in a new era of transportation innovation.

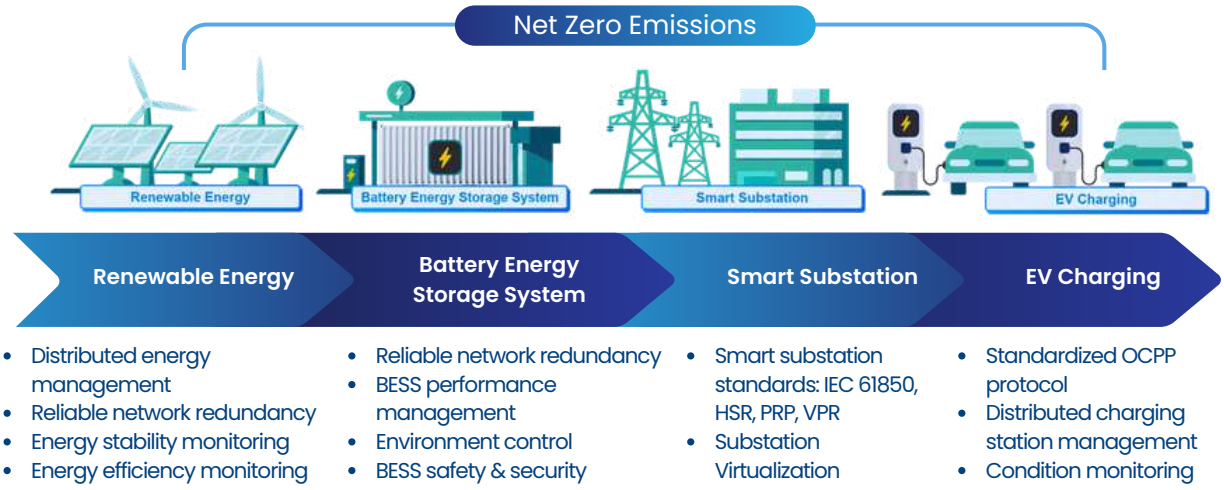
ITS/TUNNEL SYSTEMS FACING POTENTIAL CYBER THREATS



3. *Energy & Utility*

The Energy & Power utility sector has become a prominent topic of global discussion, driven by the rising demand for EV charging, smart home technologies, and energy storage solutions. Engineers are actively exploring innovative methods to fortify their systems against potential risks and external threats. By adhering to established standards such as IEC-62351 and referencing IEC-62443, proactive measures can be implemented to safeguard the latest IEC-61850 systems, ensuring their secure operation.

EMPOWERING ENERGY TRANSFORMATION WITH IIOT TECHNOLOGIES

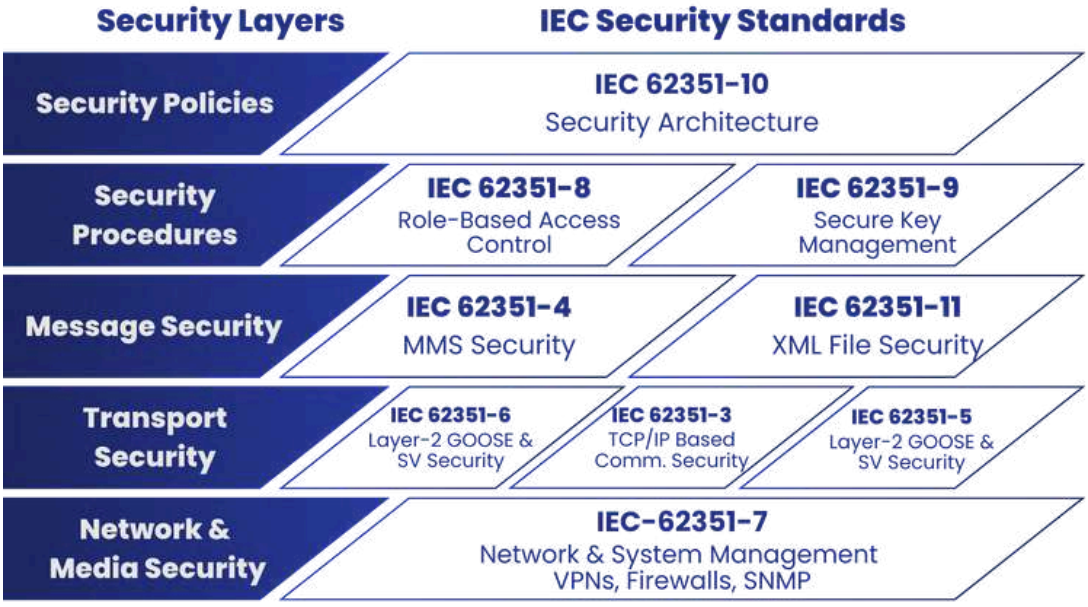


The Energy & Power utility sector has become a prominent topic of global discussion, driven by the rising demand for EV charging, smart home technologies, and energy storage solutions. Engineers are actively exploring innovative methods to fortify their systems against potential risks and external threats. By adhering to established standards such as IEC-62351 and referencing IEC-62443, proactive measures can be implemented to safeguard the latest IEC-61850 systems, ensuring their secure operation.

These standards provide a crucial framework for protecting critical infrastructure. IEC Technical Committee (TC57/WG15) and IEC-62351 play pivotal roles in shaping the development of standards for information exchange within power systems and associated domains, including Energy Management Systems, SCADA, and distribution automation. Their protocols and standards are essential for fostering interoperability and resilience against evolving challenges.

In substation automation, it is vital to consider the bay level, process level, and station/SCADA level. Along with network implementation, it's necessary to account for important assets, such as transformers, and ensure data transmission efficiency and low latency.

IEC SECURITY STANDARD STACK

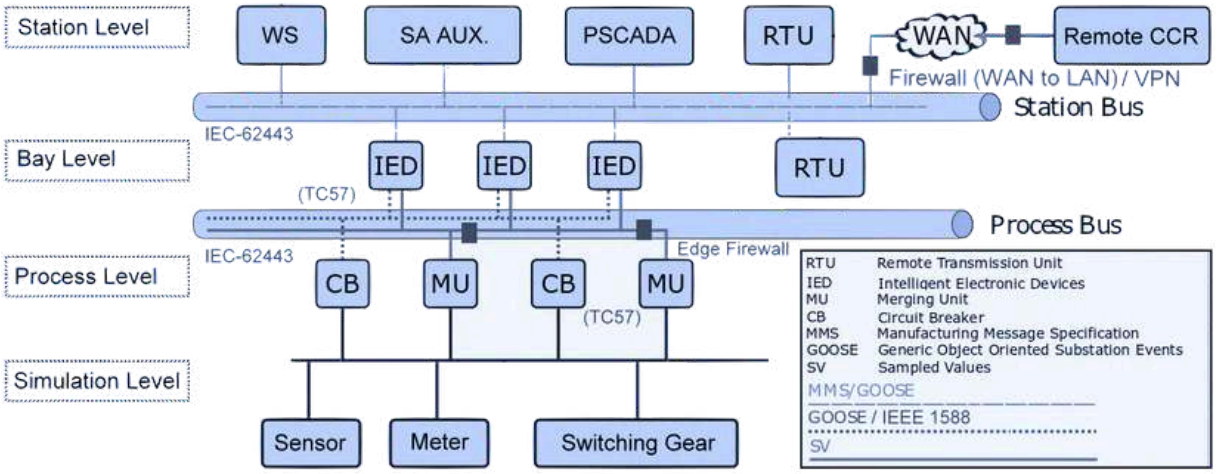


Cybersecurity in power utility infrastructure extends beyond traditional substation protocols to encompass the networking systems linking edge to core devices. IEC-62443 addresses this aspect specifically, prioritizing the security of networking infrastructure and devices. It emphasizes securing all network equipment, including edge devices, servers, gateways, firewalls, and wireless remote access, to ensure cybersecurity and site operational safety (Unman-site). Engineers need to configure L4 (VPN/Firewall) functions and implement access privileges with encrypted account/password to prevent external threats.

Moreover, given recent geopolitical tensions, reinforcing power utility infrastructure has become paramount globally. Ensuring the smooth and sustainable supply of energy sources and natural resources is essential for economic stability and national security.

On the other hand, while Time-Sensitive Networking (TSN) has not yet been widely adopted in power utility applications due to existing implementations such as NTP/SNTP, IEEE 1588 PTPv2, HSR/PRP functions running for several years, TSN, running alongside IEEE 802.1AS and IEEE 802.1CB, is crucial for time synchronization, data duplication, and other operations in substation automation. Although TSN adoption in power substations may be gradual, standardization with existing protocols is expected over time.

POWER SUBSTATION SYSTEM FACING POTENTIAL CYBER THREATS



4. Maritime

The Offshore & Maritime market holds significant importance in contemporary times. It not only facilitates global transportation but also plays a pivotal role in green energy, such as wind power generation, and traditional industries like Oil & Gas through offshore drilling. Additionally, it encompasses a vast number of marine vessels worldwide. Given its extensive scale and relevance to everyday life and national security, the critical assets within this sector require meticulous attention to security and safety.

The integration of cyber technologies has become indispensable for the operation and management of various systems crucial to ensuring shipping safety and safeguarding the marine environment. These systems often need to comply with international standards and regulations set by Flag Administrations. However, the inherent vulnerabilities associated with accessing, interconnecting, or networking these systems can pose significant cyber risks that must be addressed.

Vulnerable systems may include, among others, the following:

1. *Bridge systems and Central control & monitoring;*
2. *Cargo handling and management systems;*
3. *Propulsion and machinery management and power control systems;*
4. *Access control systems and position monitoring*
5. *Passenger facing public networks, servicing and management systems;*
6. *Administrative and crew welfare systems; and*
7. *Communication systems & C4ISR.*

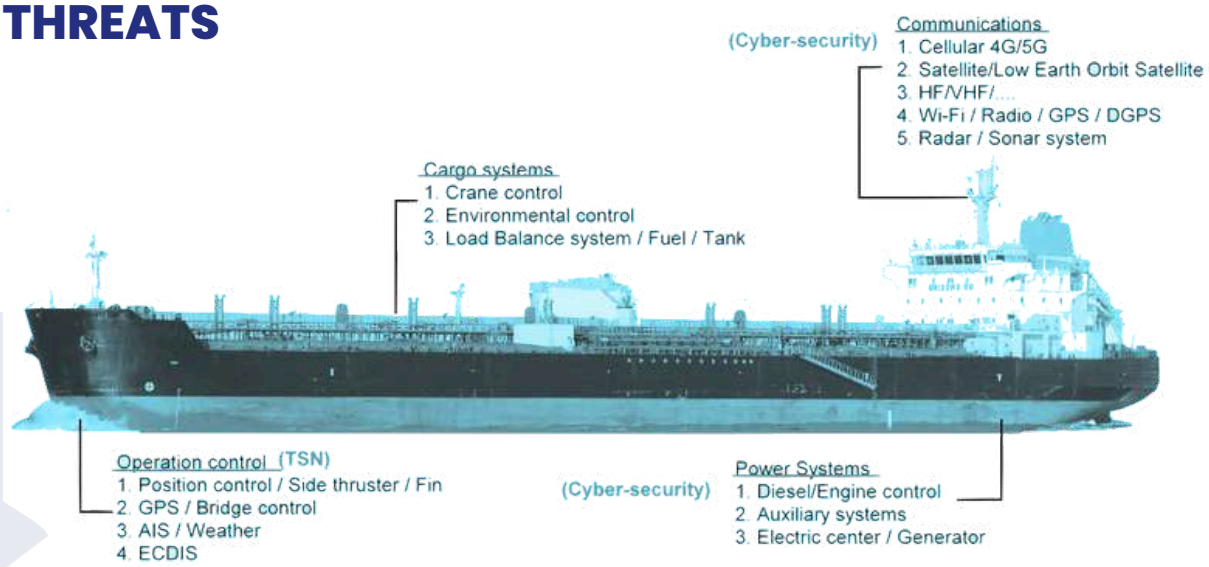
The maritime Operational Technology (OT) domain comprises various systems, including the Vessel Integrated Navigation System (VINS), Global Positioning System (GPS),

satellite communications, Automatic Identification System (AIS), radar systems, and electronic charts. While these technologies offer significant efficiency improvements for the maritime sector, they also present risks to critical systems and processes essential for shipping operations. These risks may arise from vulnerabilities related to the operation, integration, maintenance, and design of cyber-related systems, as well as from intentional and unintentional cyber threats. Addressing these cyber threats requires acknowledging the distinct nature of OT systems, given their control over the physical world.

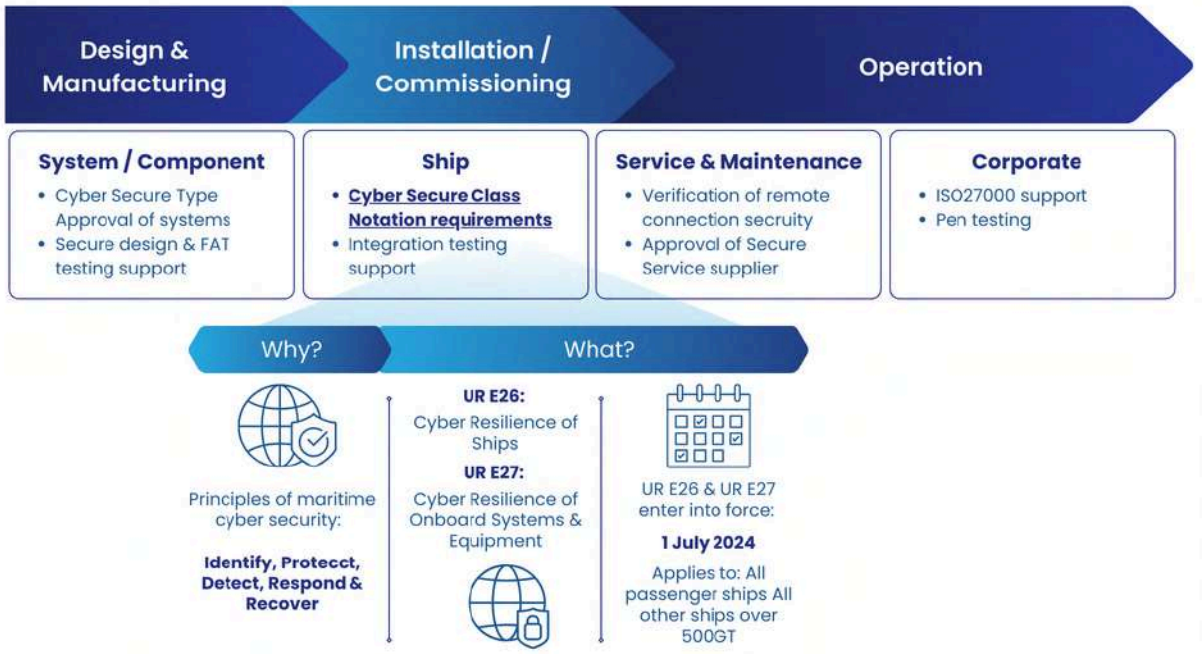
Given the escalating cyber threat landscape, cybersecurity protocols for maritime systems, based on IEC-62443, are outlined within the framework of the International Association of Classification Societies (IACS). The revised Unified Requirements (UR E26 and UR E27) for cybersecurity are set to become compulsory starting July 1, 2024. Compliance with these standards will require product certification in line with IACS UR E27 Cyber Secure regulations, particularly Security Profile 1, for each vessel delivery, covering design approval and surveys.

In addition to cybersecurity considerations, Time-Sensitive Networking (TSN) holds potential for vessel operations during harbor navigation, referred to as "Position Control." This aspect is crucial and time-sensitive due to the limited space within harbors. Accurate and low-latency position control is essential to safely dock vessels. Furthermore, advancements in "unmanned vessels" through GPS/satellite communication and TSN technology present an opportunity to revolutionize the freight industry in the near future.

MARITIME SYSTEMS FACING POTENTIAL CYBER THREATS



CYBERSECURITY STANDARD & PROCESS FOR SHIP



5. *Factory automation*

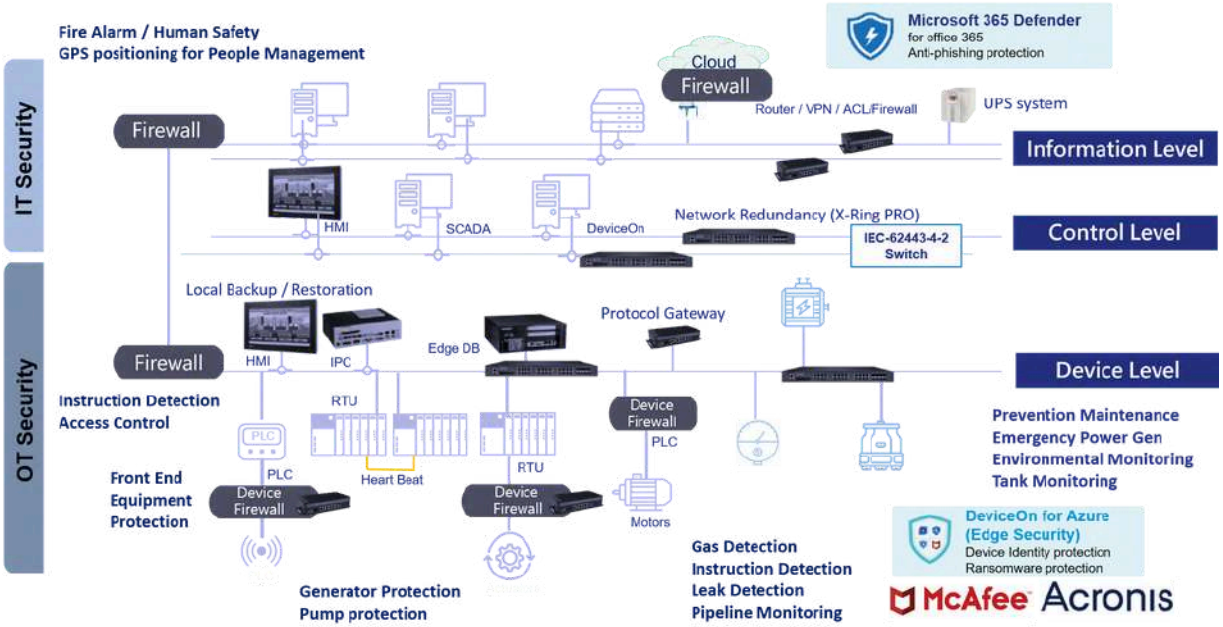
Recently, manufacturers have shown reluctance to adopt widely-used security technologies such as encryption and device authentication. They express concerns about the potential negative effects on system performance. This hesitation is compounded by a rapidly changing threat landscape, marked by the rise of advanced persistent attacks, especially aimed at industrial systems. Any disruption, whether in heavy industry or high-tech factories, could result in substantial losses or production delays.

Currently, the prevailing standard being embraced is IEC-63283-3 (TC65/WG23), with its primary objectives outlined as follows:

1. *Conduct a comprehensive review of smart manufacturing use cases to identify cybersecurity-relevant scenarios and requirements.*
2. *Propose additional smart manufacturing use cases if deemed essential to highlight potential cybersecurity concerns.*
3. *Compile a catalog of smart manufacturing requirements essential for ensuring cybersecurity across components, systems, design, integration, operation, and maintenance.*
4. *Recommend potential avenues for smart manufacturing-specific profiling to streamline the application of IEC 62443 (all parts).*

To safeguard our factory assembly line comprehensively, meticulous planning of security measures and thorough risk assessments are crucial. An examination of the traditional structure of factory automation systems highlights a clear division into IT and OT segments. The IT segment primarily handles remote access and cloud operations, while the OT system oversees process control (TSN), device management, and robotic operations. Furthermore, it's essential to activate relevant functions and features in communication, control, and computing devices to protect against threats from all directions, whether internal or external.

TOTAL IT/OT SECURITY / SAFETY / ASSET PROTECTION



06 Conclusion

The intersection of TSN and cybersecurity presents a nuanced landscape filled with both opportunities and challenges across various industries. Throughout this white paper, we've explored the intricate relationship between TSN technologies and security measures, emphasizing their crucial roles in enhancing operational efficiency, safety, and resilience.

In transportation, TSN technology acts as a catalyst for real-time communication, empowering autonomous vehicles, railway systems, and traffic management systems with unmatched precision and reliability. However, increased connectivity also brings a corresponding rise in cybersecurity risks. Adhering to established standards like IEC 62443 and TS 50701 enables stakeholders to develop customized cybersecurity frameworks tailored to their operational needs.

Similarly, in the energy and utility sectors, the integration of TSN and robust cybersecurity protocols becomes essential for protecting critical infrastructure against evolving threats. Compliance with standards such as IEC-62351 and IEC-62443 ensures interoperability, resilience, and regulatory compliance, thereby reducing risks and enhancing system reliability.

In maritime and factory automation, embracing TSN alongside cybersecurity measures is crucial for ensuring both safety and efficiency. By adopting international standards and implementing comprehensive security protocols, stakeholders can effectively mitigate cyber risks and safeguard vital assets, fostering resilience and sustainability in their operations.

As we navigate the complex interplay between TSN and cybersecurity, it becomes evident that balancing performance optimization and security is paramount. While TSN enhances operational efficiency and responsiveness, cybersecurity measures serve as defenses against cyber threats, preserving system integrity. Through the integration of TSN technologies with robust cybersecurity protocols, industries can leverage digital transformation while fortifying themselves against evolving cyber risks.

In conclusion, the convergence of TSN and cybersecurity marks a paradigm shift in industrial operations, offering unprecedented opportunities for innovation and efficiency. By embracing this convergence and adhering to established standards and best practices, industries can navigate modern industrial systems with confidence, resilience, and security.

Want to learn more?

Browse all Advantech Intelligent Transportation Systems on our main website here, or scan the QR code. You can also visit the Advantech Adaptive Traffic Control Systems for source materials at:

https://www.advantech.com/en/solutions/intelligent-transportation-systems/adaptive-traffic-control-system

Advantech Global Headquarters

Address: No. 1, Alley 20, Lane 26,
Rueiguang Rd.,
Neihu Dist., Taipei 114, Taiwan
Tel : 0800-777-111

- *Regional Contact Information:* *https://www.advantech.com/contact*
- *Technical Support:* *https://www.advantech.com/support*

Regional Service & Customization Centers

China	Kunshan 86-512-5777-5666	**Taiwan**	Taipei 886-2-7732-3399	**Netherlands**	Eindhoven 31-40-267-7000	**Poland**	Warsaw 00800-2426-8080	**USA**	Milpitas, CA 1-408-519-3800

Worldwide Offices

Asia Pacific

Taiwan

Toll Free	0800-777-111
Taipei	886-2-7732-3399
Taichung	886-4-2372-5058
Kaohsiung	886-7-392-3600

China

Toll Free	800-810-0345
Beijing	86-10-6298-4346
Shanghai	86-21-3632-1616
Shenzhen	86-755-8212-4222
Kunshan	86-512-5777-5666
Hong Kong	852-2720-5118

Asia Pacific

Japan

Toll Free	0800-500-1055
Tokyo	81-3-6802-1021
Osaka	81-6-6267-1887
Nagoya	81-052-291-4860
Nogata	81-949-22-2890

Korea

Toll Free	080-363-9494/5
Korea HQ (Seoul)	080-363-9494/5

Singapore

Singapore	65-6442-1000

Malaysia

Kuala Lumpur	60-3-7725-4188
Penang	60-4-537-9188

Thailand

Bangkok	66-02-2488306-9

Vietnam

Hanoi	84-24-3399-1155
Hochiminh	84-28-3836-5856

Indonesia

Jakarta	62-21-751-1939

Australia

Toll Free	1300-308-531
Melbourne	61-3-9797-0100

India

Bangalore	1-800-425-5070
Pune	91-94-2260-2349

Europe

Netherlands

Eindhoven	31-40-267-7000
Breda	31-76-523-3100

Germany

Munich	49-89-12599-0
Düsseldorf	49-2103-97-855-0
Amberg	49-9621-9732-100

France

Paris	33-1-4119-4666

Italy

Milan	39-02-9544-961

UK

Newcastle	44-0-191-262-4844
London	44-0-208-317-1380

Spain

Madrid	34-91-668-86-76

Sweden

Stockholm	46-0-864-60-500

Poland

Warsaw	48-22-31-51-100

Russia

Moscow	7-495-783-80-02
St. Petersburg	7-812-332-57-27

Czech Republic

Ústí nad Orlicí	420-465-524-421

Ireland

Galway	353-91-792444

Americas

United States

Cincinnati	1-888-576-9668
Milpitas	1-408-519-3800
Irvine	1-800-866-6008
Ottawa	1-800-346-3119
Chicago	1-513-742-8895
Boston	1-800-866-6008

Canada

Toronto	1-800-866-6008

Brazil

Toll Free	0800-770-5355
São Paulo	55-11-5592-5355
Itajuba	55-35-3623-5949

Mexico

Toll Free	1-800-467-2415
Mexico City	1-800-467-2415
Guadalajara	52-33-3169-7670

Middle East and Africa

israel

Kadima-Zoran	072-2410527

Turkiye

Istanbul	90-212-222-0422
Bursa	90-850-840-3995

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com