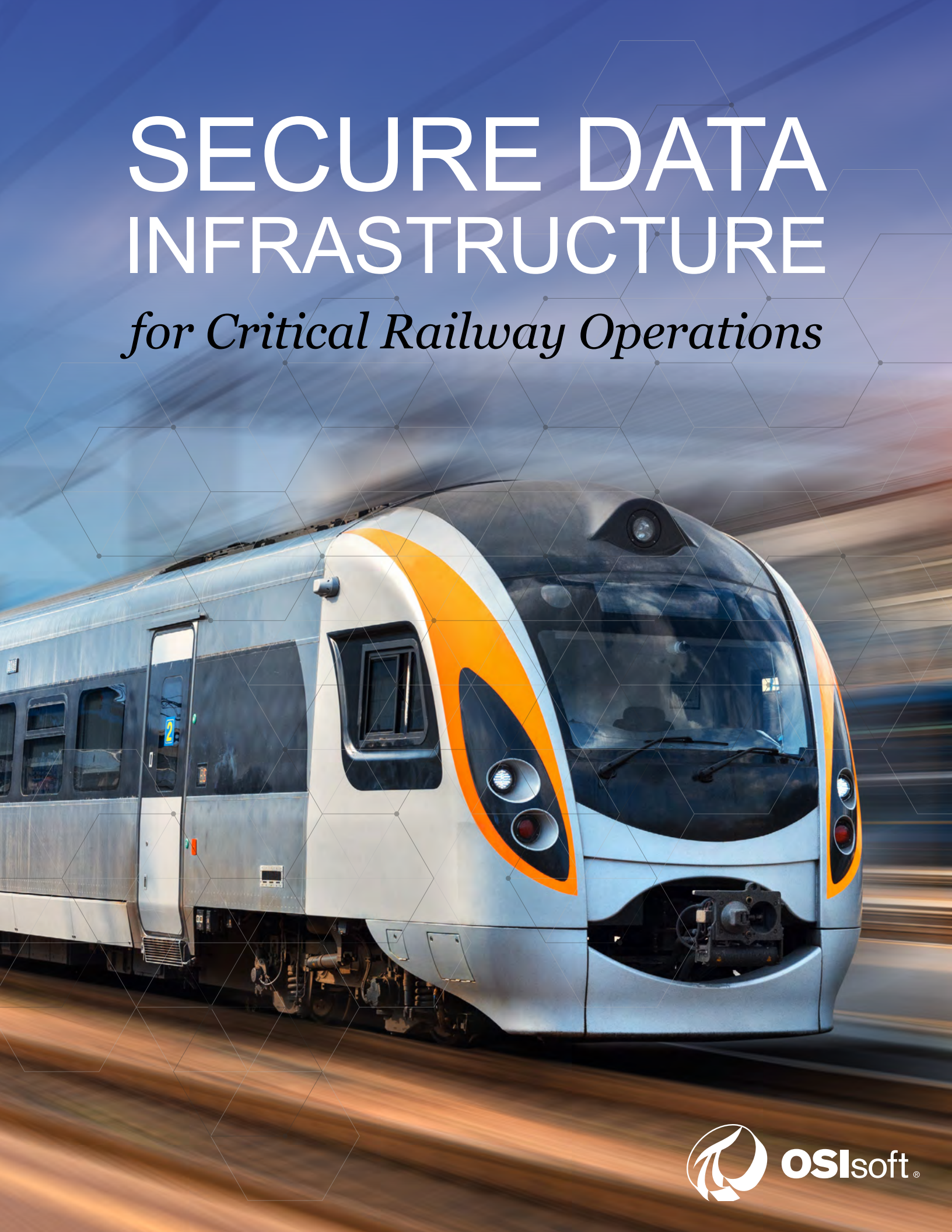
SECURE DATA INFRASTRUCTURE

for Critical Railway Operations



OSIsoft®

THE NEED FOR MORE SECURITY

With new digital technologies, modern railway companies can increase asset reliability and improve on-time performance. However, with more sensors on geographically dispersed equipment, rail infrastructures and signaling systems also become more exposed to cyber-attacks. This white paper shares cross-industry experience in creating a robust security solution for critical infrastructure data monitoring and management.

SITUATIONAL SUMMARY

Digital transformation has been slow to come to the rail industry... However, being a laggard has one big advantage: the opportunity to learn from the leaders.

With Internet of Things (IoT), Artificial Intelligence (AI), Big Data, and other megatrends impacting planning horizons, rail transportation organizations are challenged to use data about physical assets to provide digital tools to the workforce — without putting critical operations and public safety at risk. Fortunately, cybersecurity is a problem that has been tackled by other critical infrastructure sectors with proven outcomes, and much can be learned from the experience of these other industries.

RISKS & OPPORTUNITIES FACING THE RAIL TRANSPORTATION INDUSTRY

In many ways, the structure of rail organizations is similar to the structure of other sectors that own and operate large fleets of costly and geographically distributed mission critical assets. Until recently, surprisingly little had been done in much of the rail industry to closely monitor and manage physical assets by leveraging the data they generate. Rail control and safety systems have been in place for a long time, and organizations have been able to rely on human intervention for what cannot be overseen by computers. With the advent of driverless trains, automated ticketing machines, and pressure to better utilize human capital, companies need to effectively utilize data to make educated decisions regarding asset availability, capacity planning, maintenance cost, safety, and customers' and passengers' desires for timely and relevant information.

Other industries have already been through the process of adopting digital technologies to better run critical operations. We can think of power generation (nuclear, conventional, and renewables), utilities (water), process industries (oil and gas, chemicals, pharmaceuticals), and facilities (data centers, campuses) which face security challenges of their own, but have managed to harness the value from their operational data as part of their individual asset management strategy to increase efficiency and throughput, detect failures, and save costs while increasing safety.

What can be learned from the experiences of other industries? Even if operating within the paradigm of "If we cannot secure, we must shut down connectivity," security should never stop organizations from achieving their goals. Other industries show that very valuable real-time data can safely be consumed from reliability-critical and even safety-critical industrial control systems. The winning strategy is not opening holes for people to get into critical systems, but rather copying the data to a system where people can access it without creating vulnerabilities. Safe operational data collection provides immediate value and supports a long-term digital strategy without requiring a new funding qualification process for each subsequent project.

LESSON LEARNED:

Future proof your digital solutions by building in the right list of key security and connectivity requirements from the beginning.

IT-OT INTEGRATION IN CRITICAL INFRASTRUCTURE

We have all heard of the Information and Operation Technologies divide. For decades, these groups have operated in separate silos with very different mindsets and distinct technologies. With the digitization of industry, these silos can no longer stand as common technology platforms need to bridge the IT-OT divide. Operation technology practitioners are rightly concerned about wholesale deployment of IT security programs intended for office and enterprise environments, and organizations must ensure that IT and OT practitioners collaborate on proven, sustainable platforms that are capable of supporting mission critical operations while delivering real-time data needed for business objectives.

"SMART" PRODUCTS & DATA-DRIVEN SERVICES

Caterpillar helps transportation giants **save up to $1.5 million** per ship per year through after-market services for fuel reduction and maintenance.

GREATER OPERATIONAL EFFICIENCY

Xcel Energy **saved $46 million** and improved renewable integration with real-time data visualizations and weather forecasting.

TYPICAL OT SYSTEMS

All heavy industries utilize similar technologies that we can group under the umbrella of "control systems," which include PLC, DCS, SCADA, and safety systems. In rail, some common operational systems include:

- Centralized Traffic Control (CTC) / Traffic Management Systems (TMS)
- Integrated Control Systems (ICS)
- Automatic Train Protection / Operation / Supervision / Control (ATP/ATO/ATS/ATC)
- Interlocking Systems (switches, signals, crossings)
- Communications-Based Train Control (CBTC)
- European Rail Traffic Management System / European Train Control Systems (ERTMS/ETCS)
- Positive Train Control (PTC)
- Rolling stock automated inspection systems (wheels, structural components)
- Building Management System (BMS) (ventilation, pumps, lighting, escalators, elevators)
- Building Security Systems (cameras, fire and smoke detection, intrusion detection)
- Power Supply and Distribution systems
- Telematics
- Telecommunications systems (IP networking, radios, intercom, cameras)
- Structural Integrity monitoring (bridges, dam, rails, underground, tunnels)

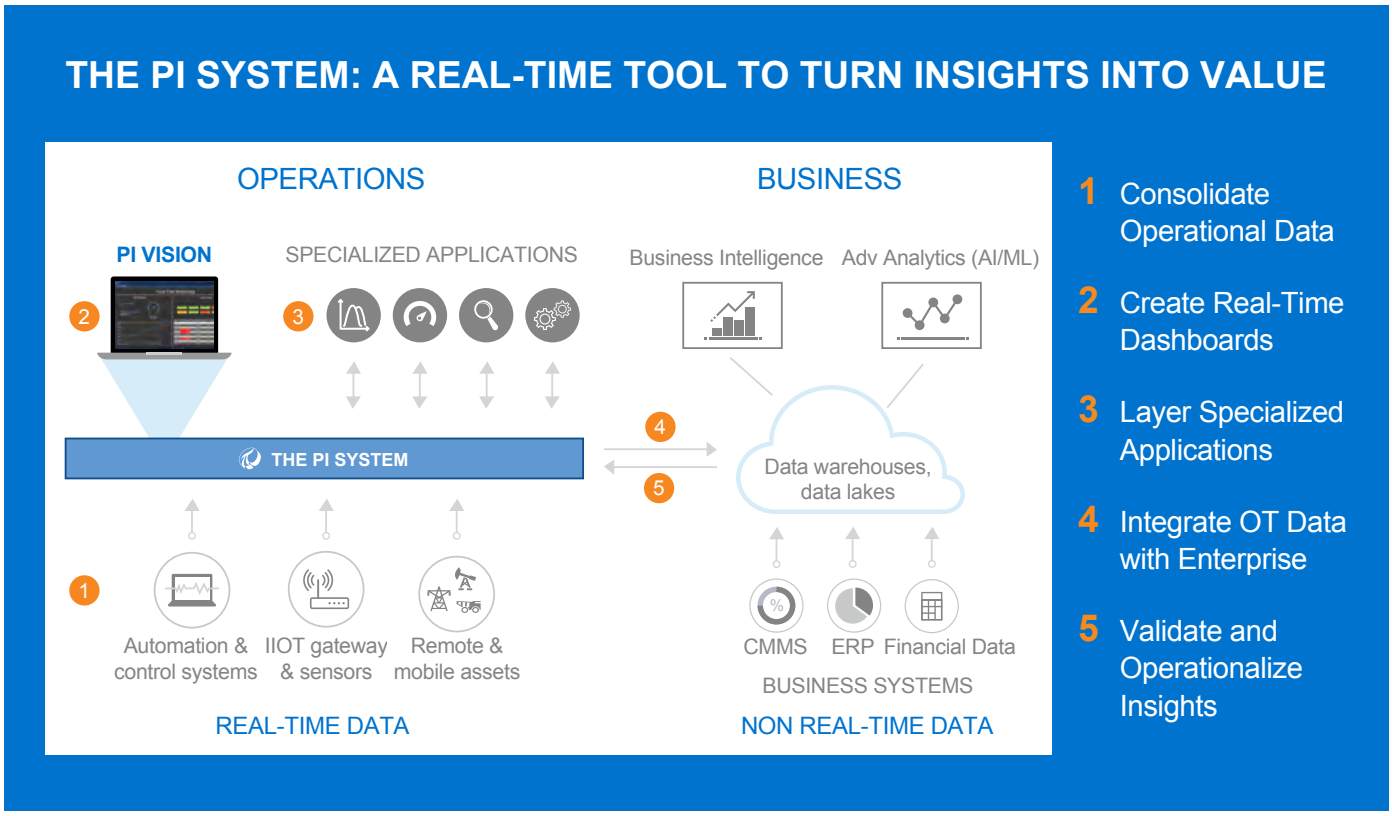
All these various systems generate continuous streams of time-series data, are highly protected, and should only be accessible from secured locations to dedicated personnel for operating the railway infrastructure.

TYPICAL IT SYSTEMS AND PLATFORMS

As information availability becomes ubiquitous among the public and workforce, users expect OT data to be readily available in IT systems to help drive capabilities, efficiencies, productivity, and quality of service.

Within rail organizations, the most important IT systems to integrate with OT include:

- Enterprise Asset Management (EAM)
- Computerized Maintenance Management Systems (CMMS)
- Enterprise Resource Planning (ERP)
- Fare Collection and Passenger counting systems
- Passenger Information Systems
- Business Intelligence (data warehouse and data lakes)
- Cloud and IoT platforms
- Data Science platforms (advanced analytics, AI, ML)
- Geographical Information System (GIS)
- Desktop IT applications
- Website hosting and publishing applications



The PI System provides a secure operational System of Record (SoR) fueling operational innovation & business process improvements.

MAKING THE CASE FOR REAL-TIME DATA

To help make the case for real-time data flow from operations systems to business systems, organizations must first identify quick wins with low risk. A quick win should aim at solving a key business issue by providing the visibility to the operations data underlying a specific issue. A dedicated monitoring system is low risk and much safer than solutions with control capabilities.

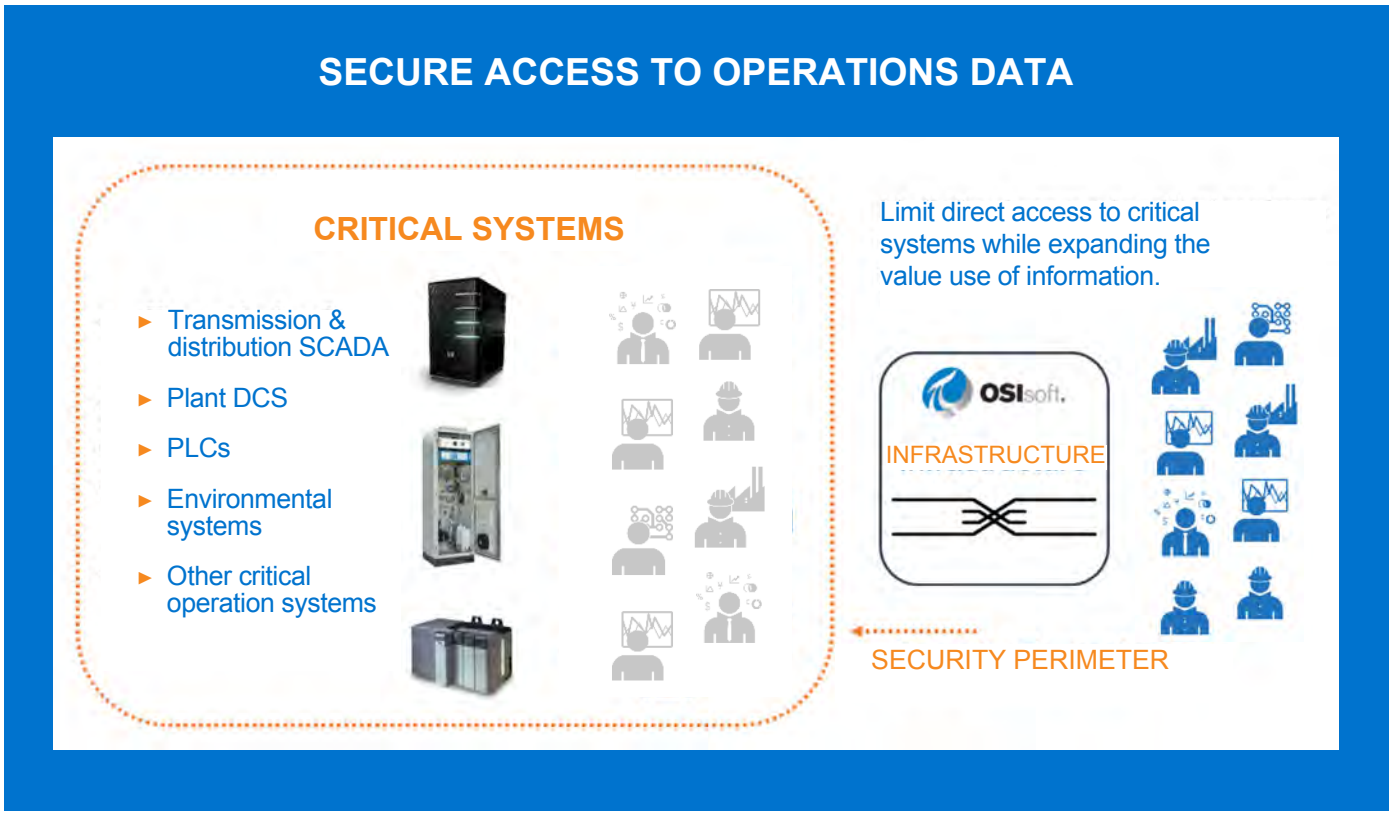
To identify these quick wins, companies should first identify which data sources are needed to resolve the problem. Next, they should select a data interface to collect the data. Often the data required, even for a simple use case, will come from multiple operational systems, requiring a vendor-agnostic platform to bring the data together. Finally, it is crucial for security to implement monitoring in a manner that does not open security holes into critical operational networks.

Thus, the real-time data monitoring system should perform three roles: data collection from multiple sources, data management that brings that data together into a single dataset, and data access so that users can make use of the data to drive positive impacts to the business. This will require bridging the IT-OT divide. Approaches to resolve this problem are further discussed in the next section.

Having a clear strategy for the end-to-end implementation around a use case does not mean implementing a tailored solution for each problem. Any platform for IT/OT integration must be able to support current and future needs without having to start from scratch and implement a new technology stack each time a new data access need arises. This approach enables incremental value to be captured, further contributing to the ROI of foundational technological investments and accelerating the digitization of industry.

COMMON PATTERNS FOR CRITICAL INFRASTRUCTURE

Most critical infrastructures adopt an approach that establishes a security perimeter for critical systems. This security perimeter is not only physical. Electronic mechanisms such as communication, networks, computers, hardware, users, and applications, as well as processes such as the definition of the perimeter, the definition of access, procedures for data access, training, and awareness are essential elements of an effective security perimeter strategy. The implementation of a data infrastructure is an effective approach to limit access into the critical systems' security perimeter while expanding the usage of information, assuming best practices for protection are carefully followed.



The OSIsoft data infrastructure limits direct access to critical systems by providing data access outside the security perimeter.

Operational technology lifecycle aspects also need careful consideration. These technologies tend to be long lived and inherently lag in security advances. Changes to critical systems, including security updates, are subject to strict validation procedures and limited deployment windows, thereby negatively impacting the flexibility to address business problems in an effective fashion.

CRITICAL INFRASTRUCTURE PROTECTION (CIP) BEST PRACTICES

While most of the rail industry is just beginning the IT-OT integration journey, other critical infrastructure sectors have pioneered well-defined architectural patterns for more than a decade, resulting in commercially-available-off-the-shelf solutions for security. Nonetheless, the industry has also started establishing best practices and guidelines for rail organizations as well. Some examples of both are described below.

NIST (National Institute of Standards and Technology, USA):

NIST has published a Practice Guide for Situational Awareness for Electric Utilities. This guide, authored by the National Cybersecurity Center of Excellence (NCCoE) Information Technology Laboratory, explains the use of commercially available products to provide a converged view of a utility's operational data while abiding to cybersecurity best practices. This guide highlights how the OSIsoft PI System can provide a mechanism for aggregating operational data from control systems and mirroring it in the enterprise network to provide capabilities needed for anomaly detection and analysis. This guide highlights the importance of firewalls and unidirectional gateways as part of the architecture.

Learn more >

NIST has also published a Guide to Industrial Control Systems (ICS) Security, which can provide a lot of relevant knowledge for the rail sector. This guide explores important security concepts such as network segregation, dual-hosted computers, firewalls between OT and IT networks, unidirectional gateways, and a wealth of other key topics for industrial security.

Learn more >

UIC (International Union of Railways):

Guidelines for Cyber-Security in Railway recommends implementing Demilitarized Zones (DMZs) with unidirectional traffic between zones. UIC also suggests segregating networks with firewalls and to consider unidirectional communications for lower delays and best efficiencies.

Learn more >

American Public Transportation Association (APTA):

Securing Control and Communications in Rail Transit Environments document defines how the electronic security perimeter boundaries should be set, as well as security measures recommended for each layer.

Learn more >

European Union Agency for Network and Information Security (ENISA):

Challenges of Security certification in emerging ICT environments document of December 2016 describes the security certification status for some of the most important equipment involved in critical infrastructure sites with a focus on Energy, ICT, Rails, and others. Key concepts applicable to Energy and ICT, including network segregation, historian databases feeding IT systems, firewalls and next gen firewalls, and unidirectional gateways are also transferable to the Rail sector.

Learn more >

Agence nationale de la sécurité des systèmes d'information (ANSSI):

Has published a document entitled Cybersecurity for Industrial Control Systems – Classification Method and Key Measures which proposes a risk classification system and associated mitigation strategies. In this guide, railway switch automation is categorized as a class 3 critical network, the highest level of criticality in their methodology. Architectures are proposed to enable data flow from the sensors to the enterprise, enforced by strictly unidirectional communication.

Learn more >

NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection):

Provides a set of requirements to secure assets that are part of the North American Bulk Electric System (BES). NERC CIP for the most part refrains from specifying technologies but requires the implementation of an Electronic Security Perimeter (ESP), with tightly controlled accesses. Data Historians, along with appropriate networking mechanisms, have long been associated with best practices to exchange data from OT to IT while abiding with NERC CIP ESP requirements.

Learn more >

Rail Delivery Group (RDG):

Published their Rail Cyber Security Strategy in January 2017. In this guide they acknowledged the increasing needs for operational systems to exchange data with business systems, and the underlying security implications. The strategy proposes to rest on common and recognized cybersecurity frameworks. It suggests addressing, amongst other things, the need for appropriate security management of systems and interfaces.

Learn more >

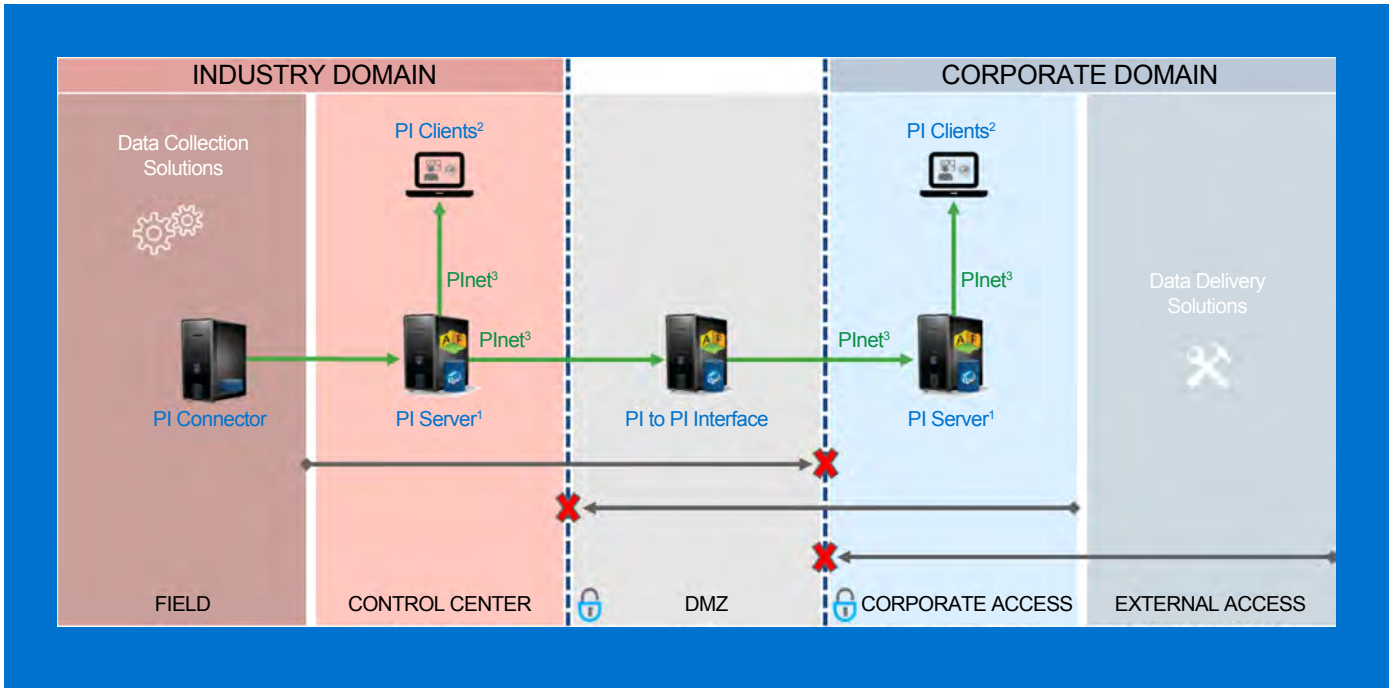
COMMON ARCHITECTURE PATTERNS

When it comes to implementing a secure mechanism to permit data from inside the security perimeter to be copied to a wider audience, most often in the corporate network, there are tried and tested options. These options offer progressive levels of security that comply with the most stringent requirements imposed by critical operations. These architectures reflect years of experience in the domains of nuclear generation, power, water and gas utilities, as well as military. These architectures are well understood, widely supported, and can be quickly implemented by most technical experts.

The PI System is currently the industry leader, deployed by 65% of the Industrial Fortune 500 to turn data from critical operations into insights while maintaining security. In the next section of this paper, we will look at some common architectures for providing secure access to mission critical data.

DATA REPLICATION THROUGH A DEMILITARIZED ZONE

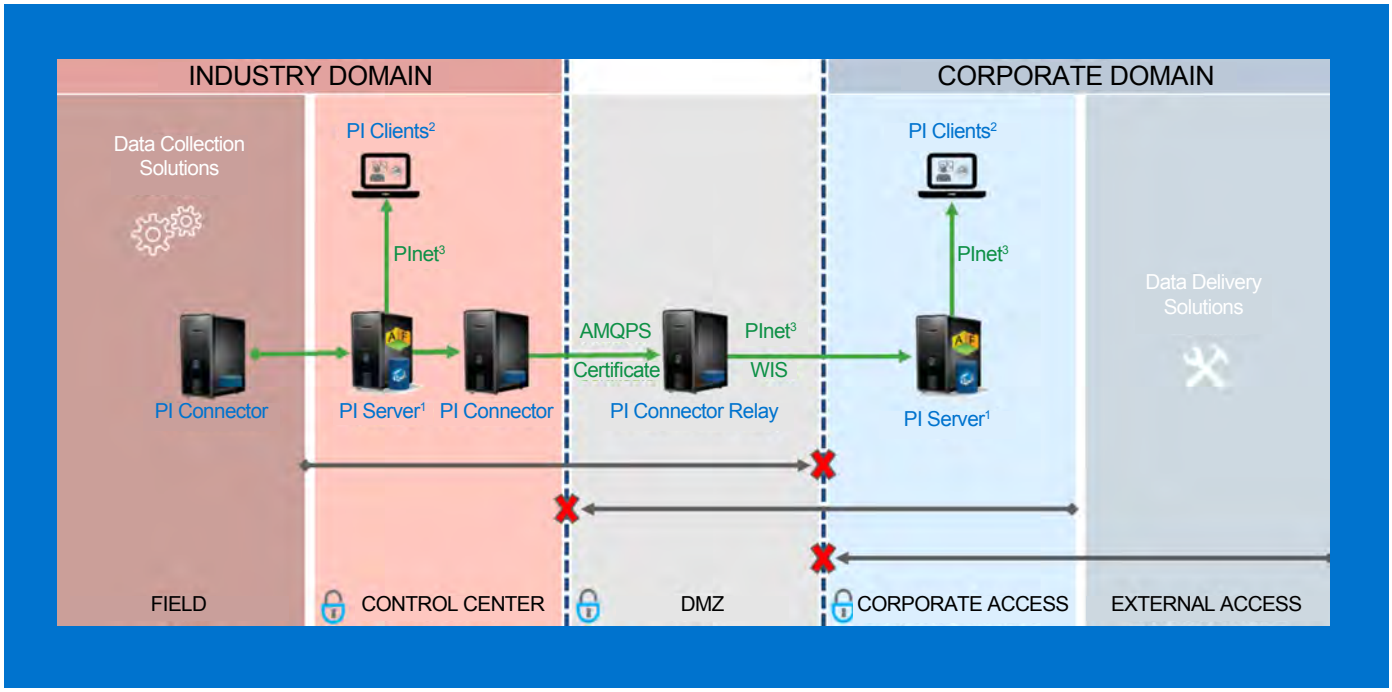
This option makes use of a software-based interface, positioned within a firewall-isolated protected demilitarized zone (DMZ). A DMZ allows logical separation and control over communications between two networks. The interface software is used as a middleware to replicate data collected in a PI Server located within the security perimeter into another PI Server instance located in the corporate network. The PI Interface provides real-time, fault-tolerant data replication with a minimum of open firewall ports. This option is suitable for low-security and medium-security industrial networks but may not meet the most stringent requirements imposed on some safety-critical networks.



Data Replication Pattern #1: PI to PI Interface

DATA RELAY THROUGH DEMILITARIZED ZONE

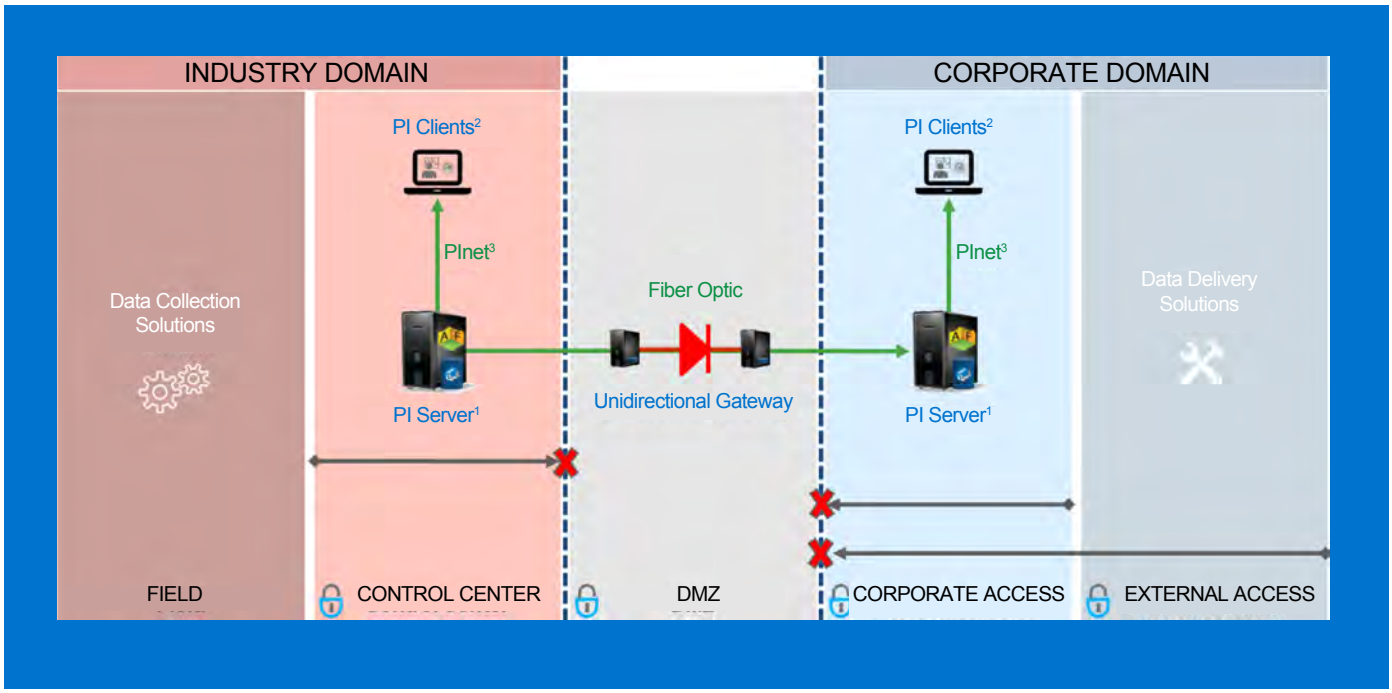
A second option leverages additional layers of replication and security, with data transfer through a DMZ using distinct security protocols. Data is collected within the security perimeter and can be archived in a PI Server or directly transferred to the corporate side. With this pattern, not only are TCP connections passing through the DMZ prevented, but also enforces a hop in communication protocol. Data flows into the DMZ using encrypted Advanced Message Queuing Protocol (AMQPS) and flows out of the DMZ using OSIsoft's encrypted PInet protocol. Similarly, the data relay enforces two authentication steps. The first authentication for inbound data is based on X509 certificates and outbound authentication is based on Windows credentials. The dual authentication and communication protocol hop combine to provide a highly defensible DMZ and control center.



Data Replication Pattern #2: PI Connector Relay

UNIDIRECTIONAL GATEWAY PHYSICAL ISOLATION

The third and most secure option relies on a unidirectional gateway to replicate data from the security perimeter to the corporate environment. This solution provides absolute protection for the industrial domain with no physical possibility of any communication from IT networks gaining access through the security perimeter. Unidirectional gateways are plug-and-play appliances that replace firewalls and are physically able to send information in only one direction across a fiber-optic cable. Unidirectional communication is guaranteed by the fact the secure side only has a fiber-optic transmitter / laser in the hardware, and the corporate side hardware contains only an optical receiver but no laser. Software agents sit on each side to replicate, in real-time, the data from the industrial domain to the corporate domain. This approach is suitable for even the most important industrial network, including rail signaling systems and other safety-critical networks.



Data Replication Pattern #3: Unidirectional Data Gateway

KEY REQUIREMENTS AND CONSIDERATIONS

When selecting solutions that can help rail organizations establish a safe infrastructure for critical operations data, some key requirements should include:

- A data platform that maintains the important security boundary around systems that control critical processes while providing access to operational data to business users.
- A data platform that leverages standards, well understood and familiar to industrial security practitioners.
- A data platform that is administered by IT and managed by OT supporting self-serve governance, analytics, visualization and reporting.
- A data platform that can be employed for various data streams and sources without reconfiguration each time or major impacts to enterprise architectures.
- Data replication providing strict unidirectional data transfer capabilities.
- Use of technologies with a long history and references in critical industrial operations such as nuclear generation, conventional generation, water treatment, military operations.
- Data replication permitting full data transfer, including historical data backfilling in the case of an interruption.
- Vendors who employ security development lifecycle methodologies for secure coding practices, emphasizing reliability and resiliency in all product testing and development.
- Vendors which participate third parties to independently audit, test, and validate their products such as Idaho National Laboratories, US Army NetCom, US NRC, NIST NCCoE, Windows Certification, Microsoft Azure auditing.
- Vendors with an ecosphere of partners deploying advanced security solutions such as those involving regulatory compliance, data flow enforcement, and innovation.
- Vendors providing hardware certified for the most stringent security requirements such as Common Criteria EAL4+, ANSSI CSPN and Singapore NITES.

CASE STUDY: SOCIÉTÉ DE TRANSPORT DE MONTRÉAL

MOTIVATION

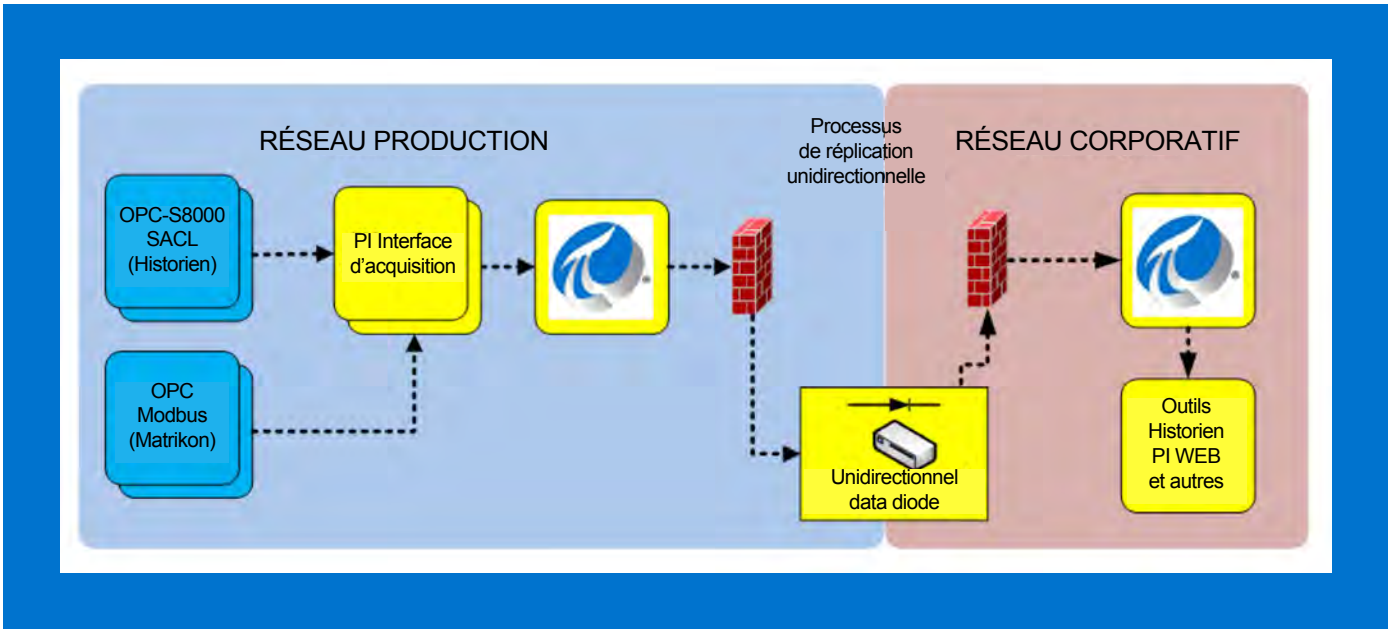
Société de transport de Montréal (STM), the public transit authority for the island of Montréal, has successfully implemented a robust architecture to capture operational data from fixed station assets. Workers can access this data to perform more targeted maintenance and increase asset availability, contributing to easier passenger flow in stations and overall trip satisfaction.

"The OPALE project, which combined new maintenance procedures, implementation of an Enterprise Asset Management software, as well as a real-time operational data store, was the key driver. The goal of this project was to increase of level of control over fixed asset maintenance efforts by providing the data and visibility to make informed decisions."

Pascal Dubois, Engineer,
Société de Transport de Montréal

OUTCOME

STM's technology partner Alizent, an affiliate of the Air Liquide Group, proposed and implemented a solution for STM comprised of the OSIsoft PI System, and a Waterfall Unidirectional Security Gateway for data replication. OSIsoft provided commercially available, off-the-shelf data connectors to all STM sensors and assets and the ability to seamlessly integrate with Waterfall Unidirectional Gateways, so STM provided workers with real-time visibility and decision-ready data.



STM Real-Time Data Infrastructure Architecture

"Our production network being completely isolated from the corporate network, we implemented the Waterfall Unidirectional Gateway to replicate OSIsoft PI Server data and enable transfers through a strictly unidirectional physical barrier. Our data gets replicated in real-time from the production network to the corporate network. We opted for an architecture, which circumvents the CC system, in order to both simplify the implementation and to reduce the load on the operations SCADA systems by sending maintenance related information directly to the workers through the PI System. We consider this architecture to be very robust and allows for near to no data loss."

Pascal Dubois, Engineer, Société de Transport de Montréal

"The integration of OSIsoft's technology with Waterfall's unidirectional gateway was seamless. Synchronization occurs automatically and there is no extra work involved to maintain the OSIsoft's components on both sides of the diode. The configuration of channels in the data diode itself for PI System data flow was initially challenging, but with the Waterfall's help we managed to configure it correctly. Now, the configuration of a new channel takes less than half an hour."

Alain Lecours, Engineering Manager, Alizent

CHALLENGES

Being public agencies, transit authorities must work through challenges imposed by purchasing constraints, including tender processes. Also, just like in many large organization, conflicting opinions on the best approach can lead to laborious negotiations.

In the end, having clear requirements for a robust, proven, tested, and secure data infrastructure, as well as selecting a knowledgeable technology partner (Alizent) proved to be a successful recipe to the STM project.

"We had some internal paradigm shifts to operate. For instance, avoiding the creation of custom solutions. Also, the concept of real-time data access was foreign to most internally. Before, one would have to physically get to where the data was, causing lots of delays – but we considered that real-time data flow was key to our project success, no matter the restrictions we had to deal with. Finally, the Operations people had to be convinced, so we had to demonstrate how we would mitigate any risk and concerns over security and unaffected metro operations."

Pascal Dubois, Engineer,
Société de Transport de Montréal

"One key requirement should be to pick compatible technologies from partner vendors. This allowed, in our case, for an easier integration between Waterfall and the PI System as well as support across future versions. Also, the centralized architecture leveraging a single data source for the unidirectional gateway configuration makes it easy to use and maintain. Finally, a proven track record is extremely important in ensuring a reliable product, in the case of STM the use of a proven technology resulted in a successful implementation that has been running continuously with minimal communication issues."

Alain Lecours, Engineering Manager, Alizent

BENEFITS

STM quickly realized benefits from the implementation. By targeting asset classes one at a time, its data infrastructure provided end-to-end connectivity — from sensors to workers — in no time. This approach has transformed work methodologies, addressed issues that are more pressing first, and allowed root cause analysis to be performed much faster.

At STM, OSIsoft PI System enabled rapid, effective and productive IT/OT integration, while Waterfall's Unidirectional Gateways eliminated IT/OT integration risks to physical operations. The combination of these industry-leading solutions is enabling the benefits of modern rails management systems, without introducing cybersecurity risks.

"Our maintenance crews had no access to data and no visibility on alarms. In order to de-risk operations, the Centralized Control (CC) system was the only point of access for this information, but the CC is highly protected, and additional functionalities needed to support our needs cannot be implemented just anytime we want and without careful assessment – for example, there usually is only one update per year, so missing an opportunity means long delays."

Pascal Dubois, Engineer,
Société de Transport de Montréal

ABOUT OSISOFT

For over 38 years, OSIsoft has been dedicated to helping people transform their world through data. Our software turns the vast data streams from sensors and other devices into rich, real-time insights for saving money, improving productivity or developing new products. Over 1,000 leading utilities, 95 percent of the largest oil and gas companies and more than 65 percent of the Fortune 500 industrial companies rely on the PI System to get the most out of their businesses. You'll find the PI System in oil refineries, mining sites, wind farms, national labs, pharmaceutical manufacturing facilities, distilleries, data centers and even stadiums helping people save energy, increase productivity and make better decisions. Worldwide, the PI System handles more than 2 billion sensor-based data streams. Founded in 1980, OSIsoft has over 1,300 employees and is headquartered in San Leandro, California. To learn more, please visit www.osisoft.com.

Corporate Headquarters:
1600 Alvarado Street
San Leandro, CA 94577, USA

OSIsoft.

WPSRAILEN-041719