WHITE PAPER

AVEVA™ PI System™ security for critical operations

Authored by:

Jonathan Pegg,
Technical Product Marketing Manager, AVEVA

Wade Potts,
Pre-Sales Engineer, AVEVA

Executive summary:

Digital transformation presents a massive opportunity for industrial organizations to optimize operations and improve asset performance. The Internet of Things (IoT), Artificial Intelligence (AI), big data, digital twins, and other tools and technologies can improve maintenance strategies and workplace safety, and help companies reach sustainability goals. Safe operations data collection provides immediate value and supports a long-term digital strategy without requiring a new funding qualification process for each subsequent project. However, industrial companies must find ways to use data about physical assets without putting critical operations and public safety at risk. Cybersecurity is critical, and any data management solution must meet IT and OT security requirements both now and in the future.

With AVEVA PI System, companies can democratize data and insights without compromising security or compliance.

The need for more security

With new digital technologies, industrial companies can increase asset reliability and improve on-time performance. However, with more sensors on geographically dispersed equipment, infrastructures and 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 and management and highlights how AVEVA PI System meets industrial operations' security and compliance needs.

Risks and opportunities facing industrial operations

Companies that own and operate large fleets of costly and geographically distributed assets must have visibility into asset performance to optimize operations and prevent unplanned downtime – and that requires access to real-time data and insights.

Under pressure to better utilize human capital, reduce emissions, meet sustainability goals, and prioritize asset updates or upgrades, companies must effectively leverage operations data to make educated decisions regarding asset availability, capacity planning, maintenance costs, safety, and carbon emissions.

Many companies across industries have already adopted digital technologies to better run critical operations. With the adoption of digital technologies, power generation (nuclear, conventional, and renewables), utilities (water and wastewater), process industries (oil and gas, chemicals, pharmaceuticals), transportation (rail), and facilities (data centers, campuses) all face security challenges of their own. However, these companies have managed to harness the value from their operations data as part of their individual asset management strategy. As a result, they've increased efficiency and throughput, detected failures much more quickly, and saved costs while increasing safety.

What can be learned from these industrial companies? Security should never stop organizations from achieving their goals. Real-time data has incredible value and can safely be consumed from reliability-critical and even safety-critical industrial control systems. There does not need to be a tradeoff between data access and protection of underlying control systems. A winning strategy involves centralizing and accessing the data in a single data management system where people can access it without creating vulnerabilities. Safe operations 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 the right list of key security and connectivity requirements from the beginning.

IT/OT integration in critical infrastructure

The divide between Information Technology (IT) and Operational Technology (OT) is nothing new. 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; common technology infrastructures must bridge the gap between IT and OT.

OT practitioners are rightly concerned about the wholesale deployment of IT security programs intended for office and enterprise environments. 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 to reach business objectives.

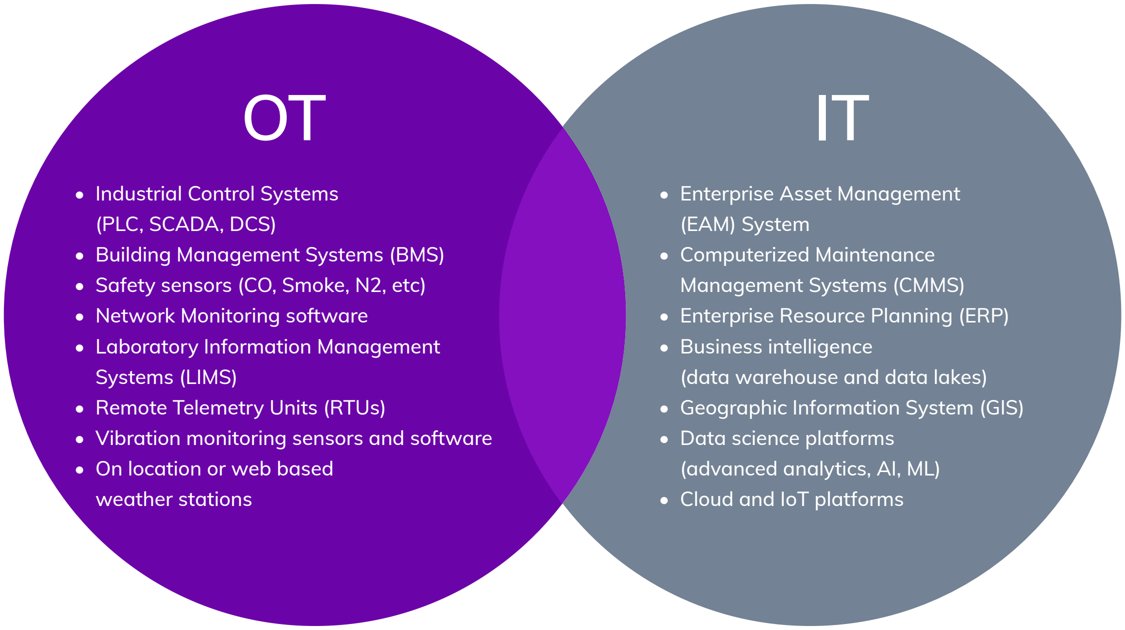
All OT systems generate continuous streams of time-series data. As that information becomes available, users across the enterprise expect OT data to be readily available in IT systems to help drive capabilities, efficiencies, productivity, and quality of service. Companies must enable secure integration between OT and IT systems to ensure users have the data they need to make decisions that benefit the bottom line.

Smart products and 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.



OT

- Industrial Control Systems (PLC, SCADA, DCS)
- Building Management Systems (BMS)
- Safety sensors (CO, Smoke, N2, etc)
- Network Monitoring software
- Laboratory Information Management Systems (LIMS)
- Remote Telemetry Units (RTUs)
- Vibration monitoring sensors and software
- On location or web based weather stations

IT

- Enterprise Asset Management (EAM) System
- Computerized Maintenance Management Systems (CMMS)
- Enterprise Resource Planning (ERP)
- Business intelligence (data warehouse and data lakes)
- Geographic Information System (GIS)
- Data science platforms (advanced analytics, AI, ML)
- Cloud and IoT platforms

Common Operations Technology (OT) and Information Technology (IT) systems and platforms

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 visibility into 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, stakeholders 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 solution to centralize data into one location. Finally, companies must implement monitoring in a manner that does not open security holes in critical operational networks.

Any 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 resolving this problem are discussed further 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 solution that supports IT/OT integration must be able to meet 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 just 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.

Companies must also carefully consider operational technology life cycles when choosing solutions. 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 effectively.

AVEVA PI System: Manage industrial data simply and securely

AVEVA PI System securely archives time-series and operations data and makes real-time, contextualized data available to the people who need it at every level of the organization. By centralizing disparate data sources and allowing users to curate data and insights at the source, AVEVA PI System creates a trustworthy, scalable, and foundational system of record for industrial operations data. With robust end-to-end security, AVEVA PI System users can rest easy knowing that data is protected and secure.

With AVEVA PI System, industrial operations can:

- Collect time-series data from other systems and provide appropriate data access to operators and other users.
- Divide AVEVA PI System across multiple architectural layers, each with its own set of barriers.
- Leverage flexible architecture and access control to securely move data out of the security perimeter and into a corporate network.
- Create a passive copy of real-time data to perform analysis and view control room data without risk to underlying critical systems.
- Give users access to real-time operations data to perform analyses without the risk of interfering with critical systems.
- Enable secure audit trails to ensure compliance with government and industry regulations.

The five pillars of AVEVA PI System security

As more and more critical devices and equipment go online, the attack surface for industrial operations also grows. AVEVA PI System operates under five security pillars to mitigate security risks and threats while enabling industrial operations to expand data collection efforts and subsequent insights.

1. Defend critical systems

AVEVA PI System helps to maintain the important security boundary around systems that control critical processes while providing business users access to operations data.

2. IT/OT security convergence

AVEVA strategic partners deploy advanced security solutions with AVEVA PI System – ranging from regulatory compliance solutions to innovations, such as data-flow enforcement based on optical diodes – to ensure secure integration between IT and OT systems.

3. Standard technologies

AVEVA PI System runs on Microsoft Windows Server and closely integrates with the Windows operating system. Customers can deploy AVEVA PI System on premises or in cloud environments from various cloud providers, including Microsoft Azure, Amazon Web Services, and Google Cloud. Because Microsoft technologies are standard and well-understood in most industries, and because security professionals are generally familiar with the procedures for hardening and securing Microsoft technologies, security teams can often use existing tools and skills to maintain AVEVA PI System products.

4. Security development lifecycle

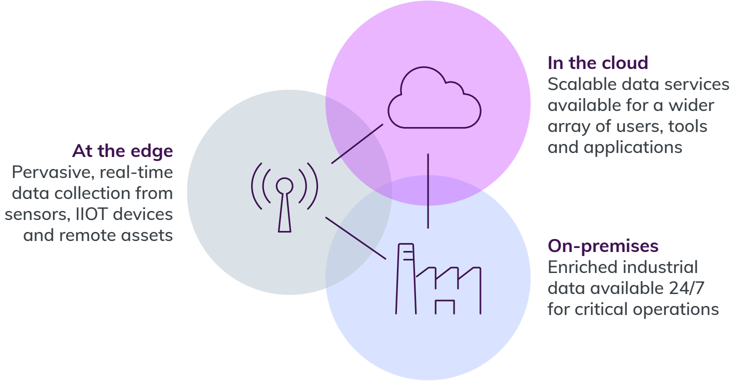
AVEVA PI System software developers employ Microsoft's Security Development Lifecycle methodology. All developers are trained in secure coding practices. AVEVA PI System developers model threats, follow secure coding practices, and regularly implement automated tools that test for security-related issues.

5. Assessed and verified

Good cyber security is a team effort. As part of AVEVA's software development lifecycle, the company regularly participates in third-party engagements to independently audit, test, and validate AVEVA PI System. Many AVEVA PI System customers turn to the same research and security vendors for similar assessments.

Securely deploy AVEVA PI System on-premises or via private cloud infrastructure

AVEVA PI System can be deployed on-premises or via the cloud to generate insights from the industrial edge to the plant floor. AVEVA PI System extends natively to the cloud with AVEVA™ Data Hub, a fully managed cloud service for aggregating, contextualizing, and sharing real-time and historical operations data, allowing companies to accelerate advanced analytics and easily and securely share data with remote workers, data analysts, business partners, and even end clients.


At the edge
Pervasive, real-time data collection from sensors, IIOT devices and remote assets
In the cloud
Scalable data services available for a wider array of users, tools and applications
On-premises
Enriched industrial data available 24/7 for critical operations

An integrated, edge-plant-cloud architecture supports OT, IT and IIOT uses cases

Edge Data Store is an Industrial Internet of Things (IIoT) and temporary storage solution to connect the edge and the cloud, enabling users to capture, access, and act on data from remote and hard-to-reach locations with sensor-enabled IIoT devices.

AVEVA PI System forms a secure, end-to-end solution to combine data from remote assets, plants, and other operating sites across the enterprise and throughout the extended ecosystem.

- AVEVA PI Server runs on Microsoft Windows and Windows Core OS to deliver the best possible performance.
- AVEVA PI Server uses Windows authentication to ensure full and tight security across all domains.
- AVEVA PI System can also be deployed using private cloud infrastructure.
- AVEVA deploys hosted, cloud-computing solutions on Microsoft Azure; and AVEVA PI System edge-computing solutions run on both Windows and Linux.
- AVEVA PI System customers employ Microsoft Active Directory to manage the authentication and authorization for access to and use of AVEVA PI System.
- AVEVA PI System also supports web-identity standards based on OAuth 2.0/OpenID Connect.
- Customers can use AVEVA PI System deployment tests and samples before full deployment, whether on-premises or on a private cloud, within AWS, Microsoft Azure, or Google Cloud Platform.

Data integrity and auditing

To protect data integrity, AVEVA PI System provides auditing tools to record all data activity and changes. These auditing tools support stringent industry electronic reporting requirements such as US FDA 21 CFR part 11 or rules imposed by the Environmental Protection Agency (EPA) and other quality-oversight agencies. For highly sensitive and regulated environments, AVEVA PI System can even be implemented in compliance with NERC CIP, NIST 800-53, and NIST 800-82 requirements.

AVEVA Data Hub: Secure, simplified real-time data sharing

AVEVA Data Hub removes the complexities of industrial data sharing and embraces a hybrid-cloud infrastructure, allowing users to extend data boundaries past the traditional IT domain by sharing data in real time with stakeholders in remote locations or outside of the company network, including vendors, partners, and regulators. A fully managed cloud service, AVEVA Data Hub's muti-tenant approach is simple, scalable, and protects access to underlying control systems and IT infrastructure. By enabling secure, cloud-based data sharing, industrial organizations can eliminate cybersecurity risks and avoid the pitfalls of other precarious alternatives, such as giving partners access to a virtual private network, company-issued devices, or sending spreadsheets of data via email.

AVEVA PI System disclosures and vulnerability response

The digital age demands that software vendors continuously look for, identify, and fix vulnerabilities. AVEVA has implemented many different practices for meeting the needs of modern industrial operations, including defining and enacting ethical disclosure policies that detail the essential response process for when a vulnerability affecting AVEVA PI System products is found.

With these policies, AVEVA takes a "do no harm" approach that avoids the sharing of vulnerability details that could put customers at risk while still working closely with customers' security teams. AVEVA PI System vulnerability disclosure and handling are consistent with industry standards, such as ISO 29147 and ISO 30111.

In general, AVEVA information technology practices align with industry standards and frameworks including NIST CSF, NERC CIP, FedRamp, and ISO 27001. Additionally, AVEVA has implemented many security best practices, such as requiring all software to use a digital authentication method in advance of NERC Critical Infrastructure Protection requirements. Additionally, AVEVA encourages customers to move from thick-client software, such as PI ProcessBook™, to web-based solutions like AVEVA™ PI Vision™.

AVEVA PI System development practices

Consistent with Microsoft's Security Development Lifecycle methodology, the company's developers seek advice from experts during major changes in product design or to components of AVEVA PI System that have critical security implications. AVEVA PI System developers engage experts as early as possible during product development, rather than late in development cycles when it is more difficult to make changes.

Third-party security toolsets

During development, AVEVA PI System developers use advanced third-party security toolsets to support security review and improvement activities. For instance, AVEVA has integrated Qualys Web Application Scanning (WAS) with the company's daily software builds. Qualys WAS automatically crawls and tests software applications in order to identify vulnerabilities.

Additionally, AVEVA runs an internal fuzzing test harness 24 hours a day, year-round. Fuzzing test harnesses modify inputs in a variety of ways in order to attempt to crash software, revealing potential vulnerabilities that hackers with malicious intent could exploit. This fuzzing practice helps AVEVA to anticipate and defend against attacks.

See **Appendix** for best practices for critical infrastructure protection (CIP).

Common architecture patterns

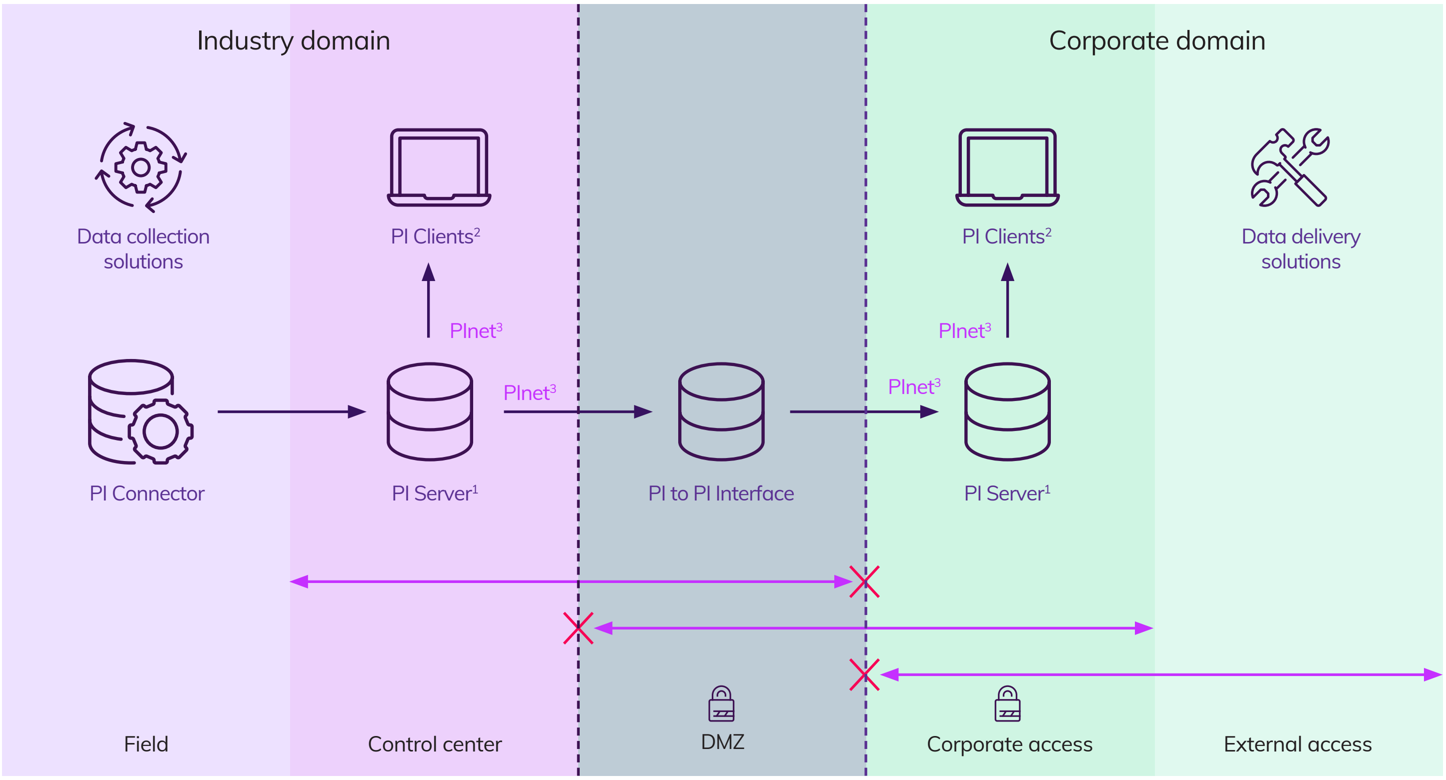
Companies can use a variety of tried-and-tested options to implement a secure mechanism to permit data from inside the security perimeter to be copied to a wider audience, most often in the corporate network. These options offer progressive levels of security that comply with the most stringent requirements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

AVEVA PI System is currently the industry leader and is deployed by 65% of Fortune 500 industrial companies. These companies rely on AVEVA PI System to turn data from critical operations into insights while meeting – or exceeding – security standards. 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 AVEVA™ PI Server located within the security perimeter into another AVEVA PI Server instance located in the corporate network.

AVEVA PI System replication 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.

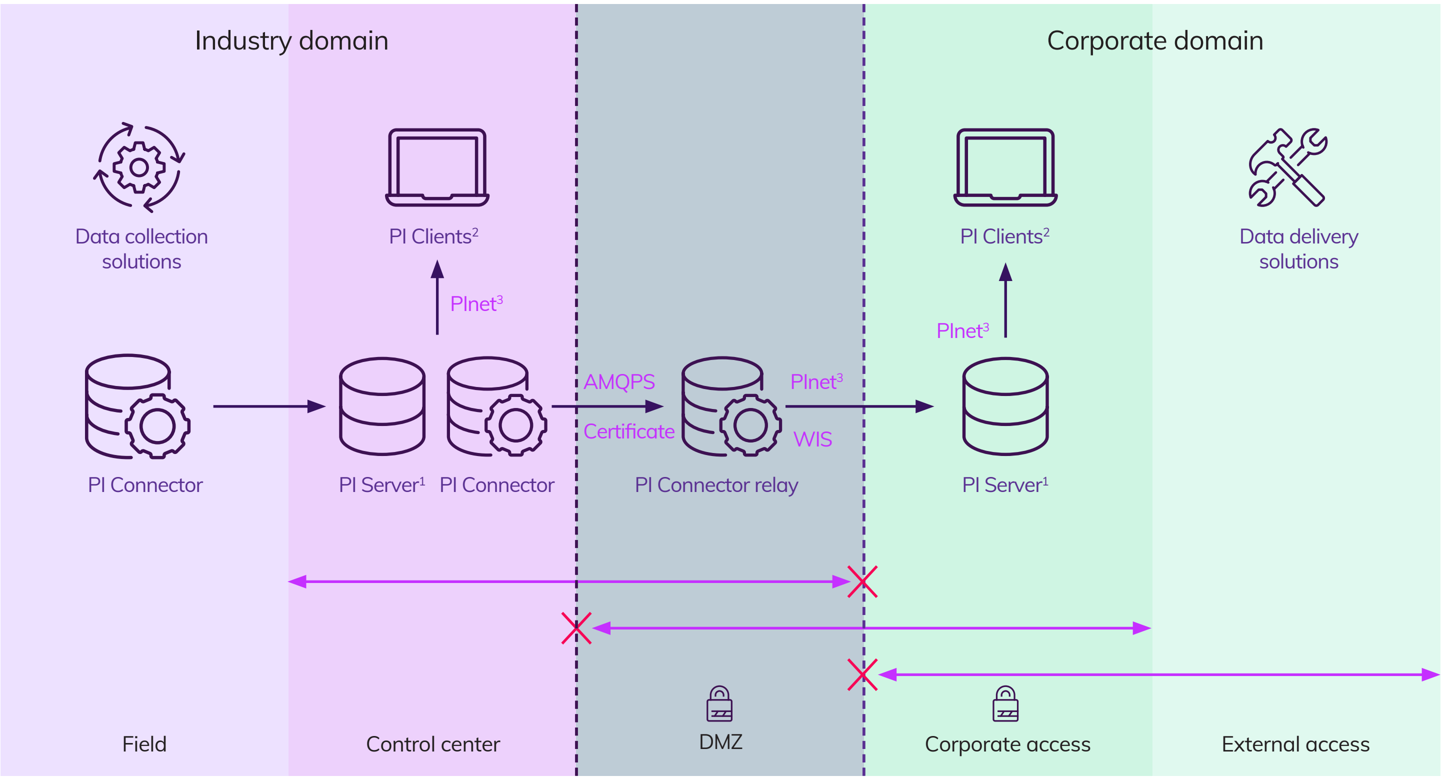


Data replication pattern #1: PI to PI Interface

Data relay through a 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 an AVEVA PI Server or directly transferred to the corporate side. With this pattern, not only are TCP connections passing through the DMZ prevented but also enforced using a hop-in communication protocol.

Data flows into the DMZ using encrypted Advanced Message Queuing Protocol (AMQPS) and flows out of the DMZ using 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.

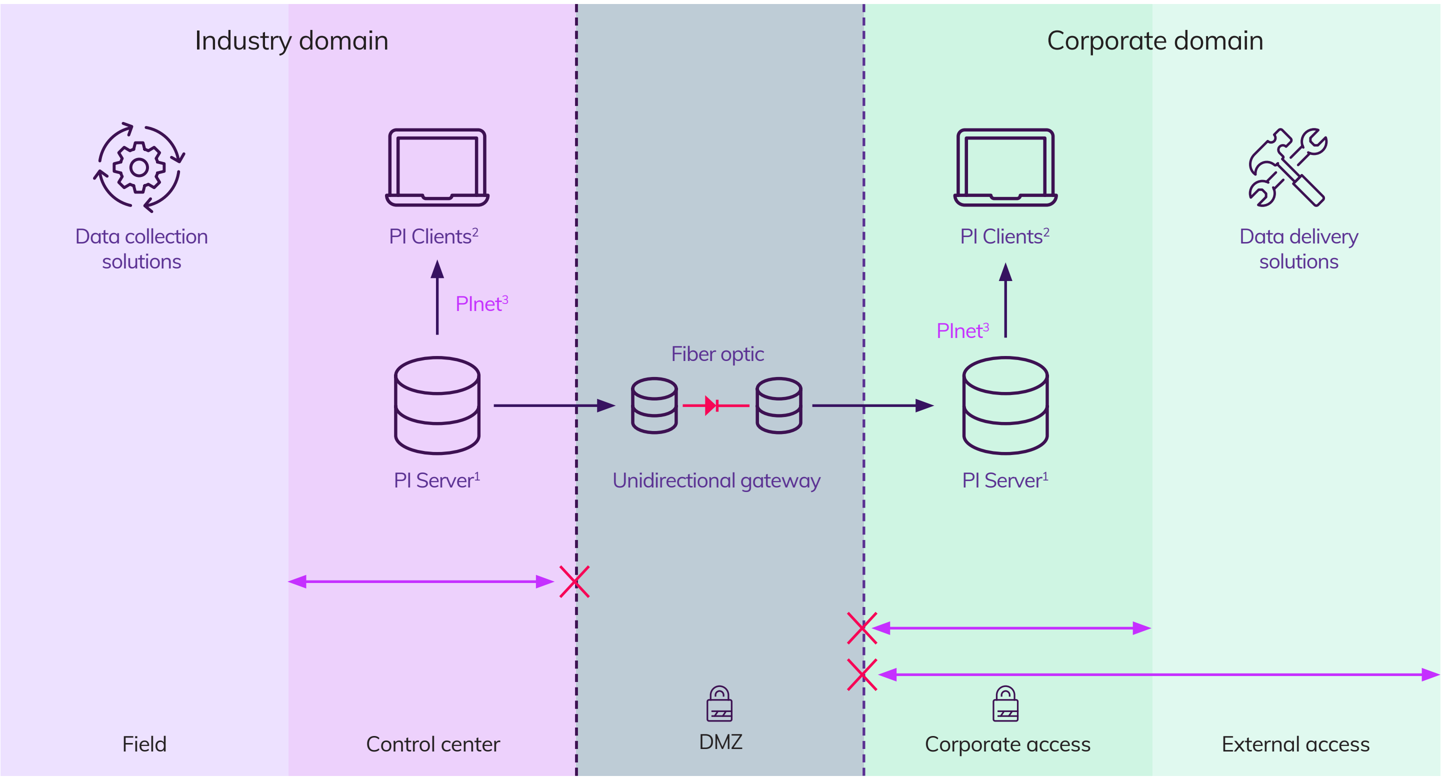


Data replication pattern #2: PI connector relay

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 the data in real time from the industrial domain to the corporate domain. This approach is suitable for even the most important industrial network.



Data replication pattern #3: Unidirectional data gateway

The cybersecurity checklist

Industrial organizations should select solutions that establish a safe infrastructure for critical operations data. These solutions should:

- Maintain the important security boundary around systems that control critical processes while providing access to operational data to business users
- Leverage standards well-understood and familiar to industrial security practitioners
- Be administered by IT and managed by OT so as to support self-serve governance, analytics, visualization, and reporting
- Employ various data streams and sources without reconfiguration each time or major impacts on enterprise architectures
- Provide data replication with strict unidirectional data transfer capabilities
- Have a long history and references in critical industrial operations, such as nuclear generation, conventional power generation, water treatment, and military operations
- Allow data replication with lossless data transfer, including historical data backfilling in the case of an interruption

Industrial organizations must also evaluate vendors to ensure a comprehensive security strategy. All vendors should:

- Employ security development life cycle methodologies for secure coding practices, emphasizing reliability and resiliency in all product testing and development
- Allow third parties to independently audit, test, and validate products such as Idaho National Laboratories, US Army NetCom, US NRC, NIST NCCoE, Windows Certification, and Microsoft Azure auditing
- Have an ecosphere of partners to deploy advanced security solutions. such as those involving regulatory compliance, data flow enforcement, and innovation
- Provide hardware certified for the most stringent security requirements. such as Common Criteria EAL4+, ANSSI CSPN, and Singapore NITES

Case studies

Société de transport de Montréal

Société de transport de Montréal (STM), the public transit authority for the island of Montréal, needed to improve its asset management strategies to allow workers to perform more targeted maintenance and increase asset availability.

Ultimately, these improvements would contribute to easier passenger flow in stations and increase overall trip satisfaction. For STM to reach these goals, the company needed to implement a robust architecture to capture operations data from fixed station assets and give workers real-time access to that data and subsequent insights.

Challenge

The concept of real-time data access was foreign to most internal stakeholders. Users traditionally had to go to where the data was stored, causing substantial delays. Real-time data was critical to project success, but that meant convincing operations teams that any new solutions and processes were both secure and would not affect metro operations.

Being public agencies, transit authorities must work through challenges imposed by purchasing constraints, including tender processes. It was important to avoid creating any custom solutions, and all chosen solutions had to be compatible with partner vendors.

> “One key requirement should be to pick compatible technologies from partner vendors. This allowed, in our case, for an easier integration between Waterfall and AVEVA 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

Solution

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

The STM network is completely isolated from the corporate network, so the team implemented the Waterfall Unidirectional gateway to replicate AVEVA PI Server data and enable transfers through a strictly unidirectional physical barrier. Data from the production network gets replicated in real time to the corporate network. To reduce the load on the operations and SCADA systems and simplify the implementation, the team opted for an architecture that circumvents the Centralized Control system and sends maintenance-related information directly to workers through AVEVA PI System.

Benefits

STM quickly realized the benefits of implementing an architecture that enabled real-time data. By targeting asset classes one at a time, the data infrastructure provided end-to-end connectivity – from sensors to workers – in no time. This approach has transformed work methodologies, allowed teams to address issues that are more pressing first, and quickly perform root cause analysis.

At STM, AVEVA 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 two solutions is enabling the benefits of real-time visibility and decision-ready data, 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

Pfizer

Intro

For more than 170 years, Pfizer has changed lives with its medicines, vaccines, and therapeutics, especially when the company delivered its COVID-19 vaccine in a mere nine months. Operations data is critical for Pfizer to have visibility into the drug discovery, development, and manufacturing process. The company built on its existing AVEVA PI System to securely compress vaccine time-to-market from nine years to nine months and ramp dosage production up from 100 million to 2.5 billion in another nine months.

Challenge

Delivering a vaccine in nine months is no small feat, especially when that process typically takes nine years. Under pressure to end a global pandemic, Pfizer accelerated its efforts to bring its vaccine to market. However, those efforts required full data visibility across existing and new assets in the company's COVID program. Regulatory compliance stakes were high because the company took an unprecedented approach of deploying Phase 2 and Phase 3 trials concurrently. In addition, Pfizer had to reinvent and innovate its equipment, delivery, and processes to meet timelines.

"To standardize the data, we have one global template creation center team split into the operational units [of the business]. Our template creation center team worked with site process and technical SMEs to create truly global standard templates to be instantiated at equipment across the sites at Pfizer. What this can essentially mean is that a tablet press in Nagoya, Japan can have the same data structure as a table press in Newbridge, Ireland having the data in a centralized and standardized repository, truly drove solution enablement, replication, and expansion across sites."

-

Sinéad McDonagh
Enterprise Historian Program Lead, Pfizer

Solution

Every site and team member had to work together to ensure that the company met its stringent goals. This required the company to centralize and standardize its operational data. Pfizer built on its existing AVEVA PI System investment at 18 sites and launched its Global Historian program across 29 sites. This program securely streamed data from local AVEVA PI Servers to a centralized global AVEVA PI Server to ensure every facility was on the same page.

Benefits

Thanks to a secure, centralized AVEVA PI System, Pfizer's four COVID vaccine manufacturing sites exceeded target production and delivered 3.2 billion doses of the vaccine by the end of 2021. The four sites shared and accessed the same data, collaborated across teams and sites, and even securely collaborated with external partners. AVEVA PI System data was instrumental in enabling the Freezer Farm Analytics Hub for cold chain monitoring, mRNA concentration prediction using AI and ML to ensure batch quality, and real-time scheduling for capacity modeling and lead time reduction by reducing bottlenecks.

AVEVA is committed to earning your digital trust. Read about our commitment to cybersecurity.

AVEVA Trust Center

Appendix

Best practices for critical infrastructure protection (CIP)

While some companies are beginning the IT/OT integration journey, other industrial operations have pioneered well-defined architectural patterns for more than a decade, resulting in commercially available off-the-shelf solutions for security. Best practices and guidelines are available across industries to ensure critical infrastructure protection. Some examples of both are described below.

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

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

The agency's document, titled Cybersecurity for Industrial Control Systems – Classification Method and Key Measures, proposes a risk classification system and associated mitigation strategies. The document proposes architectures to enable data flow from the sensors to the enterprise, enforced by strictly unidirectional communication.

Learn more

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 by cybersecurity best practices. This guide highlights how AVEVA 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

European Union Agency for Network and Information Security (ENISA)

The Challenges of Security certification in the emerging Information and Communications Technology (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.

Learn more

About the authors

Jonathan's interests focus on how technology and innovation power digital transformation in critical industries. He started working hands-on with AVEVA PI System 5 years ago as a technical product support engineer, working directly with customers to recommend best practices for architecture and data integrity, as well as deploying AVEVA PI System on customer systems. In his current role, Jonathan supports global product marketing strategy, product launch and sales enablement activities for AVEVA PI System. He has a background in physical chemistry and possess a PhD from the University of Bristol, UK.

Wade Potts is an engineer specializing in the operations space with a passion for problem-solving, particularly in the OT Space. At AVEVA, Wade is the AVEVA PI System's community lead for the EMEA Pre-Sales team. With 10 years of industry experience, he takes pride in collaborating with customers and internal teams to identify and address customers' pain points across industries. Beyond his work, Wade enjoys outdoor activities, such as long-distance running and hill walking, as well as participating in pub quizzes.

AVEVA