Case Study

Securing OT Connectivity on Manufacturing Floors

Corsha is an *Identity Provider for Machines* that secures automation and data movement from anywhere to anywhere

“Risk” takes on new meaning when it involves warfighting technologies. So, as the Warner Robins Air Force Sustainment Center (AFSC) began digitizing its manufacturing operations, they obviously set the bar for cybersecurity high.

As part of the initiative, the team at the Georgia-based Air Logistics Complex embarked on Industry 4.0 digital transformation to promote resilient data-sharing between legacy Operational Technology (OT) equipment and IT systems. Interconnecting OT and IT drives higher productivity, efficiency, and more predictive maintenance — but also brings new risk.

The added potential for cyberattacks poses a serious threat to production schedules, regulatory compliance, intellectual property (IP), reputation, and even public safety. AFSC is engaging with Corsha to enable secure connectivity by creating strong machine Identity and Access Management (IAM). Corsha is an ***Identity Provider for Machines*** that automates authentication workflows so data can be streamed securely between operational technology on production manufacturing floors and digital engineering (DE) platforms in meeting the government’s security and emerging Zero Trust guidelines.

Customer
Air Force Sustainment Center

Industry
Government/military

Mission
Bring Zero Trust connectivity between OT and IT systems to the manufacturing shop floor

IL4 ATO Accredited Solution
Using Corsha as an identity provider for machines to enable secure, automated movement of data and interconnection of systems to and from the shop floor

Corsha™
Security at the core.

OT Connectivity Exposes Advanced Manufacturing to Digital Risk

Across its three Air Logistics complexes, AFSC uses a diverse mix of advanced manufacturing systems including robotics, additive printing, inspection, digital engineering and logistics systems to provide mission-critical depot maintenance, supply chain management and installation support for the various weapons systems.

The data generated by the OT machines on the shop floors could provide valuable insight and optimizations like condition-based predictive analytics. To leverage this data in real time, AFSC needed to push past traditional standalone, air-gapped enclaves, a goal that presents new networking and cybersecurity challenges.

Today, the centers' manufacturing operations run within standalone, air-gapped enclaves of isolated equipment. Without access to network or Internet connectivity, sharing data from production systems requires a manual, disjointed process that adds cost and physical risk as technicians come and go. Failure to protect OT systems has never been an option, but convergence poses complex challenges around interconnecting legacy systems, compatibility gaps between protocols, and maximizing the use of very limited windows to maintain and patch systems.

"In the past, the ALCs could alleviate cybersecurity issues by simply choosing not to connect equipment on production floors to digital networks," says Roger Jones, AFSC Engineering Technical Director. "Industry 4.0 transformation combined with the need to get Authorities to Operate (ATOs) for manufacturing equipment makes it impossible to avoid digital exposure altogether, so now the focus shifts to *managing* risk, a much more complex and dynamic challenge. We are excited about the opportunity to work with a small business and the technology capability that Corsha brings."

The AFSC Engineering team has been an early implementor of the DoD-defined strategy and roadmap for adopting Zero Trust. The unique goals of secure OT to IT connectivity align well with the core tenets of Zero Trust – avoid implicit trust, treat everything as a resource regardless of what network it's in and challenge every access.

Zero Trust hinges on modern identity management and strong authentication to verify identities for both users and machines. The traditional machine identity approach, utilizing passwords, keys, service accounts, or PKI certificates, falls short in providing adequate security for machine-to-machine communication, particularly in hybrid environments. Interested in pushing past traditional boundaries, the AFSC is collaborating with Corsha for next generation Identity and Access Management for machines.

About AFSC

AFSC provides critical sustainment for the Air Force's most sophisticated weapons systems, including the F-35 Lightning, KC-46 Pegasus, A-10 Thunderbolt, B-1 Lancer, B-52 Stratofortress, C-5 Galaxy, C-17 Globemaster III, C-130 Hercules, E-3 Sentry, E-6 Mercury, F-15 Eagle, F-16 Falcon, F-22 Raptor, KC-135 Stratotanker, T-38 Talon, QF-16, Minuteman intercontinental ballistic missile, as well as a wide range of engines and component parts.

Industry 4.0 guidelines demand greater connectivity that propels manufacturing production enclaves into the digital realm. The industrial internet of things (IIoT), industrial cloud (or ICSaaS), and other initiatives offer increased efficiency but expose OT systems to digital risk often for the first time.

Corsha Secures the Path to Zero Trust Connectivity for OT

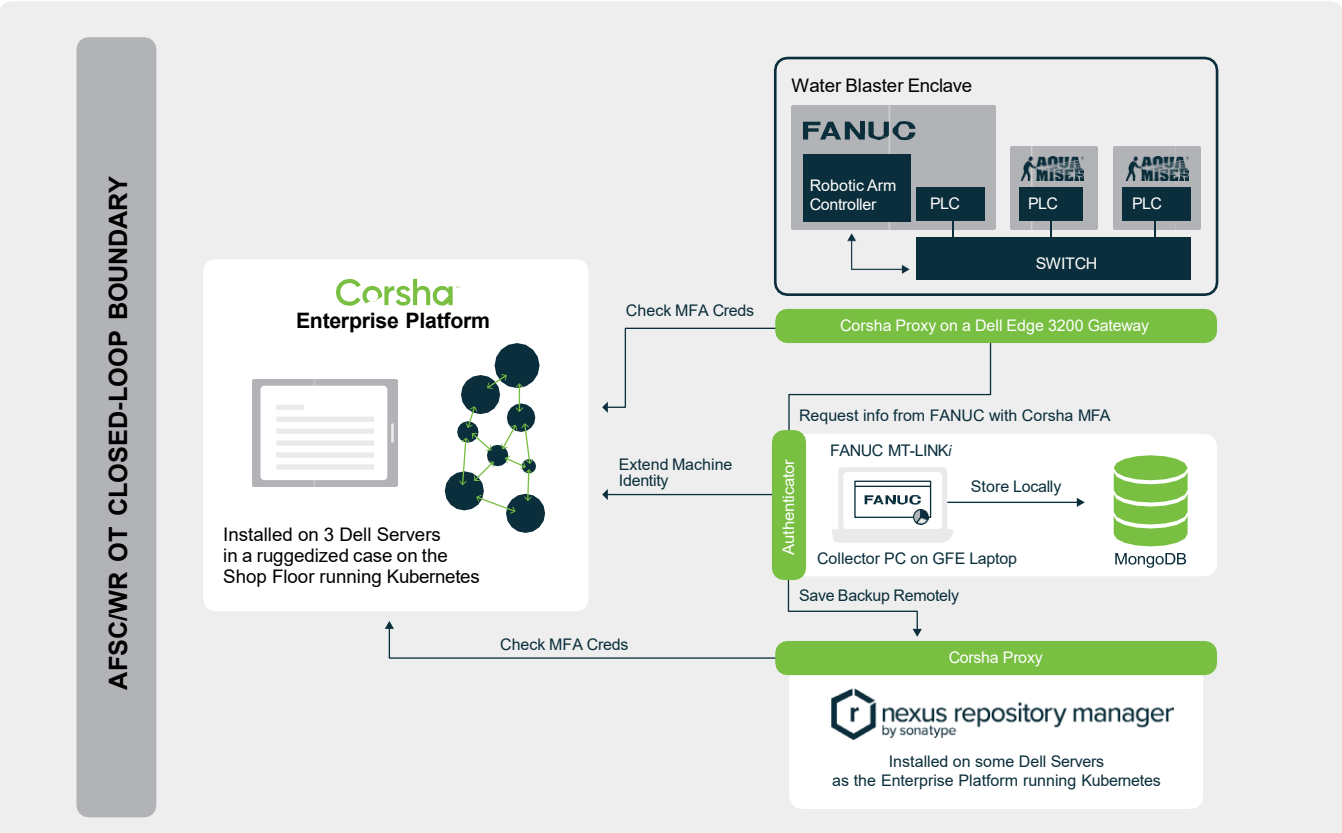
Corsha's ***Identity Provider for Machines*** extends the benefits of dynamic machine identity verification — a foundational element of Zero Trust — to OT environments. The platform brings the assurances provided by concepts like fine-grained access control, multi-factor authentication (MFA) and scheduled access to the realm of manufacturing protocols used in OT environments.

Corsha and the AFSC are taking a 'Crawl – Walk – Run' strategy to implementing Zero Trust on the shop floor. The first integration completed at Warner Robins AFB involved bringing Corsha's entire platform into the air-gapped enclave of a legacy robotic controller to demonstrate Corsha's ability to provide identity and access control, even in front of legacy equipment.

Top-line goals included:

- A no-code integration, meaning no modification to the controller or client
- Fine-grained access control even MFA for OT protocols
- The ability to stream real-time data like backups and telemetry to data repositories

The AFSC + Corsha team had ambitious goals for the integration to gauge whether the Corsha platform could secure authentication to a typical legacy manufacturing machine on the shop floor and support secure real-time streaming of data from the robotic controller.



Corsha's authenticator application was also installed on client devices and used to create identities on the platform and pin devices to the gateway. The platform then watches traffic, manages identities, and allows or denies access in real time. To complete secure login, the platform generates one-time user codes, like those sent to users via text in human MFA, that cannot be reused if they fall into the wrong hands.

Key success drivers included:

A Drop In ATO'd Solution — even for legacy systems

The AFSC specified that the Corsha solution be able to connect to industrial robotic equipment without requiring OEM technology or controller vendors to modify equipment. “Having to bring in third-party vendors to update protocols or add new connectivity options would present a clear impediment to widespread adoption,” says Wayne Ayer, SES, Director of Engineering & Technical Management - Director of the AFSC Software Directorate at AFSC. “Corsha proposed an easy, drop-in security overlay that gives us a flexible and widely applicable solution.”

Zero Trust Extended to non-human connections

Non-person Entities are a key focus of the DoD ZT Execution Roadmap, especially in OT environments where most traffic occurs between machines rather than involving human interaction. With the increasing reliance on data, automation, and AI, this trend is expected to continue growing. To counter the rising threat of attacks by adversaries impersonating machines, AFSC is collaborating with Corsha to expand protections like MFA and regulated access, typically reserved for humans, to automated connections on the shop floor.

Secure real-time streaming of data

Due to their standalone nature, pulling data from manufacturing equipment has traditionally been a very manual, fragmented, irregular process. Depot-level operators have devised tedious workarounds to connectivity like plugging laptops into controllers to load new programs, patch systems, and download screenshots of data onto disks or USB drives.

The team would then physically walk drives and laptops across the shop floor connecting individually to each enclave, collect data manually, and then return to an IT network at their desk to connect to digital engineering systems to plug in and transfer data. Besides being time-inefficient, this ad hoc “sneaker-netting” increases the risk of data loss, insider threats, and misconfigurations. Last but not least, it fails to comply with evolving mandates for data protection and connecting to equipment on production floors.

Corsha integration enables real-time secure data movement from an OT controller to a data repository unlocking capabilities for AFSC like predictive analytics and digital twins.

Secure remote and third-party access

Government facilities practice world-class physical security, but digitization means more workers, vendors, and technicians seeking to access systems remotely — even those housed within air-gapped environments. The Corsha solution needed to enable secure authentication both remotely and onsite to minimize risk from insider threats and human error.

Safeguard performance

Uptime is everything in manufacturing and other OT environments. With even microseconds of latency able to delay delivery, AFSC needed to measure the impact of the Corsha platform on productivity beforehand. The first integration confirmed imperceptible impact from Corsha’s added authentication and access control checks.

Strong authentication avoids risk

- Supply chain attacks
- Downtime and operational disruptions
- Data Loss and intellectual property theft
- Regulatory violations and legal consequences
- Financial losses

“So, how is it going?”

The initial integration met the AFSC’s primary goal — proving the platform could pin access to OT systems from only trusted machines — and did it quickly. Once the government granted Corsha the authority to conduct testing on manufacturing floors, the team deployed the solution to production equipment and executed the integration in less than two weeks.

The exercise included simulating real-world attempts to hack into systems. “Corsha demonstrated that legitimate entities could use their authenticator to log in easily while malicious actors were unable to connect,” says Iyer. “The platform managed non-human identities dynamically and enabled secure automated movement of data to/from shop floor machines and digital engineering systems for resilient information-sharing in real time.”

Corsha demonstrated through its initial integration the high assurances needed for AFSC to network OT and IT systems together. Now Corsha is working with AFSC strategic and technical leadership to connect multiple enclaves and demonstrate a larger data sharing initiative within the Robins robotics complex. With Corsha in place, the promise of secure data-sharing across network domains unlocks the potential of automation and industry 4.0.

A heightened state of security

The solution aligns with goals for adopting Zero Trust set forth by CISA, NIST, and MITRE ATT&CK. Along with keeping threat actors out, the Corsha platform delivers powerful improvements in security operations:

- Secure access control to industrial systems
- Overall reduction in security incidents and vulnerabilities
- Secure automated data streaming from OT to IT
- Secure automated remote patching and system updates
- Regulated access enabled onsite for selected vendor equipment
- Audit capabilities tied into alerting workflows

And, no impact on performance. Corsha’s platform successfully integrates with the production enclave without having any perceptible impact to production operations. Throughout testing, the solution generated mere milliseconds of latency, well within the parameters of real-time operations.

Corsha unlocks OT Automation and Industry 4.0

Corsha’s Zero Trust Platform creates the industry’s first dynamic, fully automated MFA for non-human users. The platform secures data movement workflows within and beyond OT and IT network boundaries that require continuous verification, easy monitoring, and pinpoint control. Corsha delivers an easy drop-in solution for modern cyber controls to be seamlessly retrofitted into Industrial IOT enclaves with no modifications required to untrusted machines.

Real-time data for faster decision-making

With Corsha securing connections between systems, the AFSC engineering team gains reliable, real-time access to data that helps optimize digital engineering workflows. Insights generated by disparate OT systems can be aggregated in one place and used to inform collective, real-time decisions around production planning, predictive maintenance, data security, supply chain, and overall efficiency.

Higher ROI

Digital communication to and from the shop floor cuts down on the number of people that routinely must walk back and forth to capture and transfer data. Secure remote access also eliminates costs associated with flying in vendor technicians to patch or troubleshoot systems. The Corsha approach secures remote access down to Purdue Model level 1 devices.

Innovation promotes collaboration

While the scope of the demonstration did not include updating OT machines, AFSC experts wanted to know whether solutions could be tailored to support highly specialized equipment and protocols. Corsha added support for vendor-specific manufacturing protocols used to communicate with a widely used robotic arm. Then Corsha turned to Dell Technologies and leveraged their zero trust collaborations collaborated to leverage Dell’s 3200 Edge Gateways as a commercial “off the shelf” hardware solution for Corsha’s ruggedized Proxy.

Cleared for Takeoff

Corsha has an active IL4 ATO with AFSC Warner Robins and is bringing capabilities like Big Data Analytics, advanced robotic model sharing, and AR/VR securely to the shop floor. Next steps for the Warner Robbins center include identifying and connecting more robotic systems to the Corsha platform and extending coverage to a wider array of clients and protocols. Securing access to a typical legacy manufacturing device moves the Sustainment Center one step closer to its ultimate goal for IT/OT convergence: allowing machines on and outside production enclaves to share data across network boundaries, and eventually
to the cloud.

Choosing Corsha's scalable, drop-in solution for securing access to manufacturing OT marks a critical milestone in turning Zero Trust cybersecurity from formidable obstacle to powerful agent of change. Learn more here

Corsha™