Simplesense®

Case Study: Air Force Installation Resilience Operations Command & Control (IROC) Program

Fully operational at the Air Force Installation of the Future, Tyndall AFB, across 125+ buildings and six control systems for both CE and SF squadrons

aws PARTNER Public Sector

Simplesense's Cyber Physical Infrastructure (CPI) is fully operational today as part of the IROC program. IROC protects Operational Technology / Control Systems (OT/CS) in 125+ buildings for both Civil Engineering (CE) and Security Forces (SF) squadrons and has an ongoing Approval to Operate (ATO) with continuous monitoring of all buildings and control systems. IROC fuses relevant OT/CS data in Team Awareness Kit (TAK) dashboards, combining CE, SF, and network data in one pane of glass by leveraging cloud-based data infrastructure.

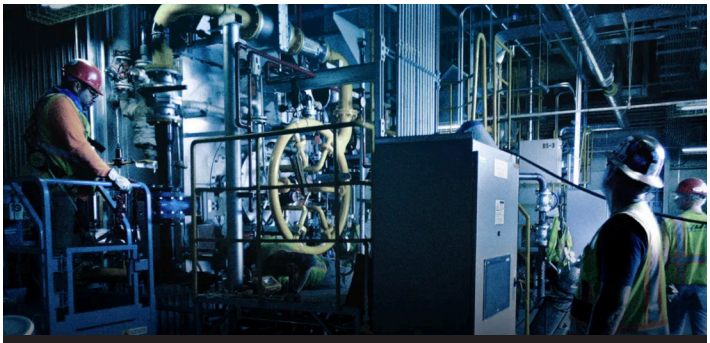
The following capabilities are fully operational within the IROC ATO boundary:

- Emergency operations and building status dashboards for mobile and command center users
- Honeywell Vindicator Intrusion Detection System (IDS) and Access Control System (ACS)
- Siemens Desigo Building Automation, Fire, Mass Notification, and Gunshot Detection
- Nozomi Guardian OT network monitoring
- Schneider power meters

Ongoing ATO with Continuous Monitoring

The IROC program obtained the first ongoing ATO for an Air Force industrial control system, made possible through the Air Force A4 Authorization and Assessment process that the Air Force Chief Information Officer recognizes as a Fast Track ATO. The IROC ATO is the first cloud-connected OT/CS system in the Air Force and was jointly authorized by both CE and SF authorizing teams without conditions:

- Moderate-High-High CIA rating for inclusion of the most sensitive unclassified systems
- Agile ATO iteration process, authorizing new capabilities into the IROC ATO every 3-6 months depending on complexity, relative to 18-24 months through a traditional ATO process
- ATO architected by authorizing team for rapid deployment to new installations



Rapidly authorizing and deploying proven commercial cybersecurity solutions while unlocking siloed data from OT/CS

1 year development, 6 month install
First Fast Track ATO for cloud-connected OT

Reduced operator workload
Ensured mission readiness
Empowered and enabled C2
Rapidly adopted new technologies
Leveraged commercial best practices

Standards Based, DoD Compliant

Simplesense CPI implements the following standards and reference architectures:

- DoD Zero Trust Reference Architecture
- MOSAICS/Control System Cybersecurity Design Reference Architecture
- NIST 800-53: Security and Privacy Controls for Information Systems and Organizations
- NIST 800-82r3: Guide to OT Security
- Unified Facilities Criteria 4 010 6: Cybersecurity of Facility-Related Control Systems
- Unified Facilities Guide Specifications 25 05 11: Cybersecurity for Facility-Related Control Systems

Agile Process

Simplesense's agile, iterative process gave the development of the IROC ATO a major advantage. Instead of fixing a roadmap from the start of the project, Simplesense interviewed over 100 authorizing officials (AOs), security controls assessors (SCAs), Information System Security Managers (ISSMs), system engineers, and requirements holders to continually modify the scope of each of 15 iterations over 3 years to fit the needs of the project.

Phil Hatch
President, Government Solutions
718-618-4939 / hello@simplesense.io

Demonstrated Outcomes

The IROC program set out to solve three problems:
1. Delivering data to the right users at the right time
2. Securing OT/CS from attack, and
3. Building a future-ready system of systems that will rapidly adapt to new threats and capabilities.

Reduced Operator Workload:
- Centralized ATO management and cyber response ensure rapid response to threats. Continuous monitoring services use automation to push patches weekly and scan systems daily.
- With IROC, control system operators no longer manage the IT infrastructure of a control system. IROC manages hardware servers and maintains operating systems, enabling OT/CS operators to focus on the control system itself instead of IT.
- Migrating services to the Cloud Enclave instead of maintaining redundant on-premises hardware and software reduces workload significantly.

Ensured Mission Readiness with Cybersecurity
- IROC decreased response times to threats with automated threat detection and automated, continuous monitoring of OT/CS versus the previous standard: infrequent, manual scans.
- Zero Trust principles reduce the attack surface for OT/CS to the bare minimum, protecting the most vulnerable equipment and using Machine Learning in Nozomi to detect anomalies.
- IROC segments control system traffic, keeping CE and SF systems isolated from each other while further segmenting IDS traffic from secure spaces from IDS traffic, meeting ICD 705 requirements.

Empowered and Enabled Command & Control
- Emergency response: IROC provides real-time data from control systems and external sources, such as local 911 services, ingesting and streaming data in near real-time. IROC leverages TAK as the primary COP for consumption of data.
- Maintenance: With IROC, the installation is able to deliver data to commercial Fault Detection and Diagnostics (FDD), Condition-based Maintenance (CbM), and other future AI/ML analytics tools, leveraging the same data infrastructure.

Rapidly Adopted New Technologies
- Through 6 iterations of its ATO, IROC proved the ability to rapidly integrate and authorize new OT/CS and data sources in 3-6 months compared to 18-24 months through a traditional ATO process.
- For future installations, the IROC ATO architecture leverages inheritance from other ATOs, including cloud providers such as AWS GovCloud, to power a 3 month ATO iteration cycle.

Leveraged Commercial Best Practices
- IROC deploys new switches, firewalls, gateways, and servers using infrastructure as code instead of manual configuration, reducing human error, increasing uptime, and increasing scalability.
- Relying on the cloud instead of on-premises servers reduces costs, increases speed to scale, enables rapid integration of new capabilities, and increases availability and reliability.
- DevSecOps, baked into the entire IROC development lifecycle, increases uptime and security by catching potential vulnerabilities early when the cost to mitigate is low.