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 160+ buildings and six control systems with a production contract underway to expand to five additional Air Force, Space Force, and Army installations.

Simplesense's Installation Resilience Platform™ is fully operational today as part of the Air Force IROC program. IROC protects Operational Technology / Control Systems (OT/CS) in 160+ 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, meeting the latest compliance requirements. IROC fuses relevant OT/CS data on-site and in the cloud in customizable dashboards, combining cross-functinoal data into a single pane of glass.

aws PARTNER Public Sector

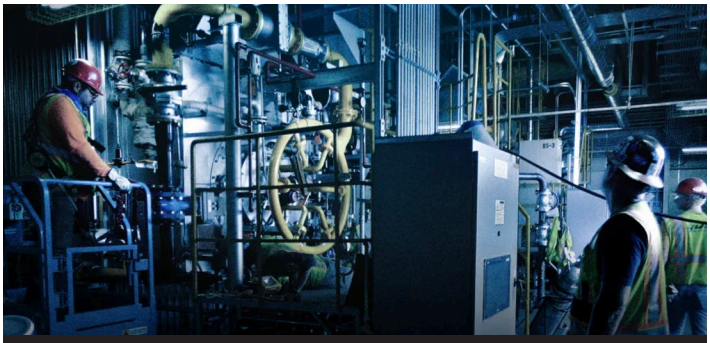
The following capabilities are fully operational in IROC:

- 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
- Splunk Security Information Event Mgmt (SIEM)
- Teleport zero trust remote access

Ongoing ATO with Continuous Monitoring

IROC obtained the first ongoing ATO for a cloud-connected Air Force industrial control system and was jointly authorized by both CE and SF authorizing officials without conditions:

- Moderate-High-High Confidentiality, Integrity, and Availability (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 relative to a traditinoal 18-24 month process
- ATO architected for rapid deployment to new installations



Decrease Downtime, Increase Resilience
Empowering operators to rapidly adapt and respond with clarity

Operating across 1 Air Force Base, 160+ buildings, 7,000+ sensors, 2,300+ devices

Reduced operator workload 1+ hrs/day
Reduced troubleshooting dispatches by 75%
Improved efficiency with automated reports
Reduced on-site compliance paperwork
Reduced critical outages by 95%
Rapidly adopted new software in 3 months
Ensured mission readiness

Standards Based, DoD Compliant

Simplesense's technology platform 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 led to rapid deployment of commercial technology in months instead of years. Instead of fixing a roadmap from the start of the project, Simplesense interviewed over 100 authorizing officials, 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, Chief Strategy Officer
303-242-7718 / phil@simplesense.io

Demonstrated Outcomes

The IROC program set out to solve three problems:

1. Secure OT/CS from attack,
2. Deliver data to the right users at the right time, &
3. Build 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 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

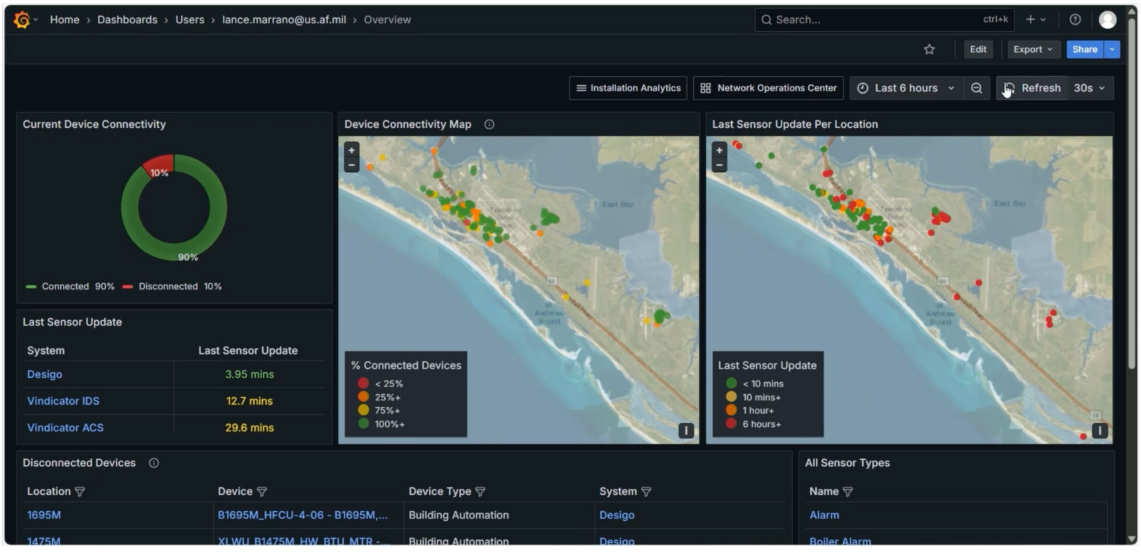
- Emergency response: IROC provides real-time data from control systems and external sources, such as local 911 services, ingesting and streaming data in near real-time. IROC leverages TAK as the primary COP for consumption of data.
- Maintenance: With IROC, the installation is able to deliver data to 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 16 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.



Simplesense's Installation Resilience Platform enables real-time data from multiple control systems accessible via Application Programming Interface (API) and viewable in a single pane of glass. This screenshot shows data from building automation, networking, fire alarm, and security alarm systems in a customizable dashboard.