Carnegie Mellon University
Software Engineering Institute

# ZERO TRUST INDUSTRY DAYS 2024 SCENARIO: SECLUDED SEMICONDUCTORS, INC.

*Rhonda Brown*

February 2024



## Organization

Secluded Semiconductors, Inc. has established a manufacturing facility on an island 1,000 miles from the continental United States (U.S.). At this facility, chips are manufactured, tested, and shipped to customers to incorporate into their electronic products. The company researches, develops, and designs chips on the island and at the company's U.S. mainland headquarters. Secluded Semiconductors, Inc. operates its semiconductor-fabrication process seven days a week, 24 hours a day and depends on having high-quality electrical power, an adequate water supply, and raw materials used in the manufacturing process.

## Personnel

Secluded Semiconductors, Inc. employs about 1,000 personnel who reside and work on the island. Of these, 20 are involved in information technology (IT) support, 50 are in clerical and logistic support, 30 are executives and managers, 500 work directly in chip manufacturing, and the remaining 400 work in a variety of city services (e.g., transportation, water, emergency medical services, education) that support the island.

## Suppliers

The island seaport serves as a shipping port for receiving raw materials (e.g., silicone, germanium, copper, other critical minerals). The island airport also serves as a shipping port and provides transportation for personnel to travel to and from the island. Secluded Semiconductors, Inc. is keenly concerned about inventory control to ensure that adequate raw materials arrive to meet the current chip-fabrication capacity and enable it to sustain market demand.

## Power

The electrical power for the facility and its supporting infrastructure on the island is sourced from both a large-scale solar power plant located on the island and from offshore wind turbines, which are tuned to accommodate fluctuations in energy production. Standby diesel generators provide an emergency backup power source.

## OT & IIoT

The facility relies on a mix of operational technology (OT) and Industrial Internet of Things (IIoT) applications. Three systems, which were developed in the 2015 time frame, are integrated into the fabrication plant and are run by highly specialized personnel:

- The first system uses clean room robotic technology to control the fabrication process environment to minimize contamination.
- The second system supports the production of silicon wafers, which are the thin slices of semiconductor that form the base of personal computer (PC) chips before they are fabricated.
- The third system is the Supervisory Control and Data Acquisition (SCADA) system for monitoring equipment status and the fabrication process.

Smart sensors, actuators, and cameras are connected via the Internet to industrial applications. IIoT applications are used for inventory control, quality control, automated testing, and packaging. Terabytes of data from the entire manufacturing process are collected from thousands of sensors on connected machines, stored in a data lake on the cloud, and analyzed with software tools that optimize and streamline production processes.

## Infrastructure

The island's infrastructure aims to enhance operational efficiency by integrating manufacturing with smart city technologies. The integrated system dynamically balances residential and manufacturing power needs against available power levels. Residential smart meters and other sensors help to determine the optimal use of available resources.

The island uses hybrid cloud services. A private cloud is hosted in the manufacturing facility's on-premises data center that supports chip fabrication, which must meet the high availability requirements of manufacturing workloads. Intellectual property that supports the company's strategic advantage, including chip architectural design and trade secret ingredients in photolithography processes, are stored within the organization's premises. This data center also supports human resources, corporate email, internal web services, and backup activity. The manufacturing facility uses

a centralized identity, credential, and access management (ICAM) solution, which is located off the island.

A second data center, located in the continental U.S. at the company's headquarters, provides continuity of operations planning (COOP) for the organization's main data center. The manufacturing facility can be run from the second data center, and there is remote access to it.

Public cloud services support order placement, shipping logistics, and accounting as well as Internet activity in other businesses, homes, and public spaces (e.g., social media activity, online banking, shopping, streaming services, and social media activity).

Internet connectivity to the island is supplied by three different satellite networks that provide the high level of resilience required since inclement weather may cause outages. The island has cellular and Wi-Fi coverage with 5G capabilities. Satellite dishes, which are installed on homes, receive signals via modems and Wi-Fi routers to power the Internet devices in homes, businesses, and public spaces.

## Challenge

A hurricane passes by the island that knocks out the satellite communications and could reduce the power grid capabilities for up to three days. How would your zero trust approach support continued operations for the manufacturing facility?

## Goals

The following are Secluded Semiconductors, Inc.'s goals related to its security and resilience:

1. The *Advanced* level of the Cybersecurity and Infrastructure Security Agency's (CISA's) *Zero Trust Maturity Model* is achieved within one year [CISA 2023].
2. The *Optimal* level of CISA's *Zero Trust Maturity Model* is achieved within two years and is confirmed via an assessment [CISA 2023].
3. The zero trust implementation is resilient enough to identify threats, even if it is in a degraded mode.
4. Policy changes can be implemented and operational within 30 minutes.
5. All logging and monitoring information can be obtained through application programming interfaces (APIs).
6. An integrated security solution supports securing all users in all locations consistently. Users are permitted and able to work on the manufacturing process remotely.
7. In the event of a disaster, chip manufacturing and business COOP is successfully operational within 12 hours.
8. Zero trust can be applied to chip manufacturing and the rest of the island's capabilities.
9. Cybersecurity spending does not exceed $3 million over the next two years.

## Questions

Please answer the following questions based on all the threats and goals identified to inform the presentation of your recommended implementation:

1. What mitigations would reduce the resulting security/resilience risks and threats associated with the island infrastructure?
2. What concerns do legacy systems create, and how would the legacy systems be addressed to support the zero trust strategy?
3. What challenges arise with OT and IIoT systems when considering a zero trust implementation? How do you resolve those challenges?
4. In a highly connected system like a smart city, how do you handle threats and vulnerabilities with a zero trust implementation without impacting overall functionality?
5. How does zero trust help address the accessibility and availability required of a manufacturing environment?
6. What factors must be considered when managing disasters with a zero trust implementation?
7. In the event of a loss of connectivity with cloud services, how do you manage identity and access management (IAM)?

# References


### [CISA 2023]

Cybersecurity and Infrastructure Security Agency (CISA). *Zero Trust Maturity Model, Version 2.0*. CISA. April 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

## Legal Markings



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.



DM24-0160

## Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

**Phone**: 412/268.5800 | 888.201.4479
**Web**: www.sei.cmu.edu
**Email**: info@sei.cmu.edu