


Ch-8: Securing IOT

- 
- ▶ A Brief History of OT Security
 - ▶ Common Challenges in OT Security
 - ▶ How IT and OT Security Practices and Systems Vary
 - ▶ Formal Risk Analysis Structures: OCTAVE and FAIR
 - ▶ The Phased Application of Security in an Operational Environment

A Brief History of OT Security

► Introduction

- Differentiating assumptions vs. realities in industrial cybersecurity
- Cybersecurity incidents in OT environments have physical consequences
- Focus on official sources rather than media reports

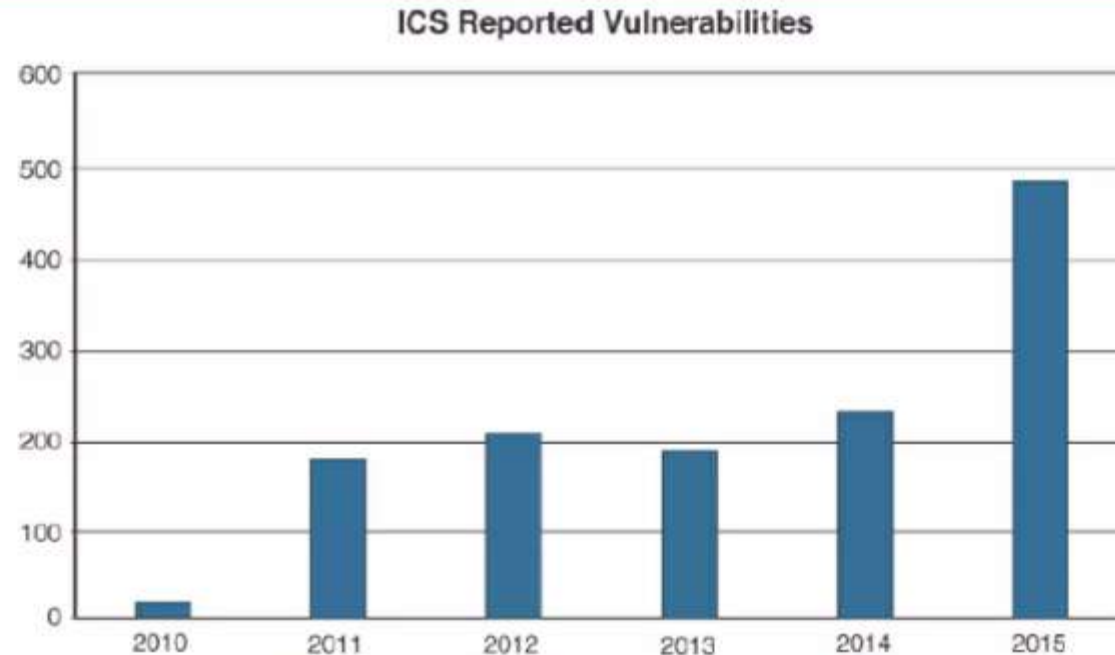
A Brief History of OT Security

▶ Real-World Cybersecurity Incidents

- ▶ **Stuxnet Malware (Iran):** Damaged uranium enrichment systems
- ▶ **German Smelter Attack:** Cyberattack caused furnace damage
- ▶ **Maroochy Shire (Australia, 2000):** Sewage system hack released 800,000 liters of sewage
- ▶ **Ukraine Power Grid Attack (2015):** Caused hours-long outage, affecting thousand

A Brief History of OT Security

A Brief History of OT Security:

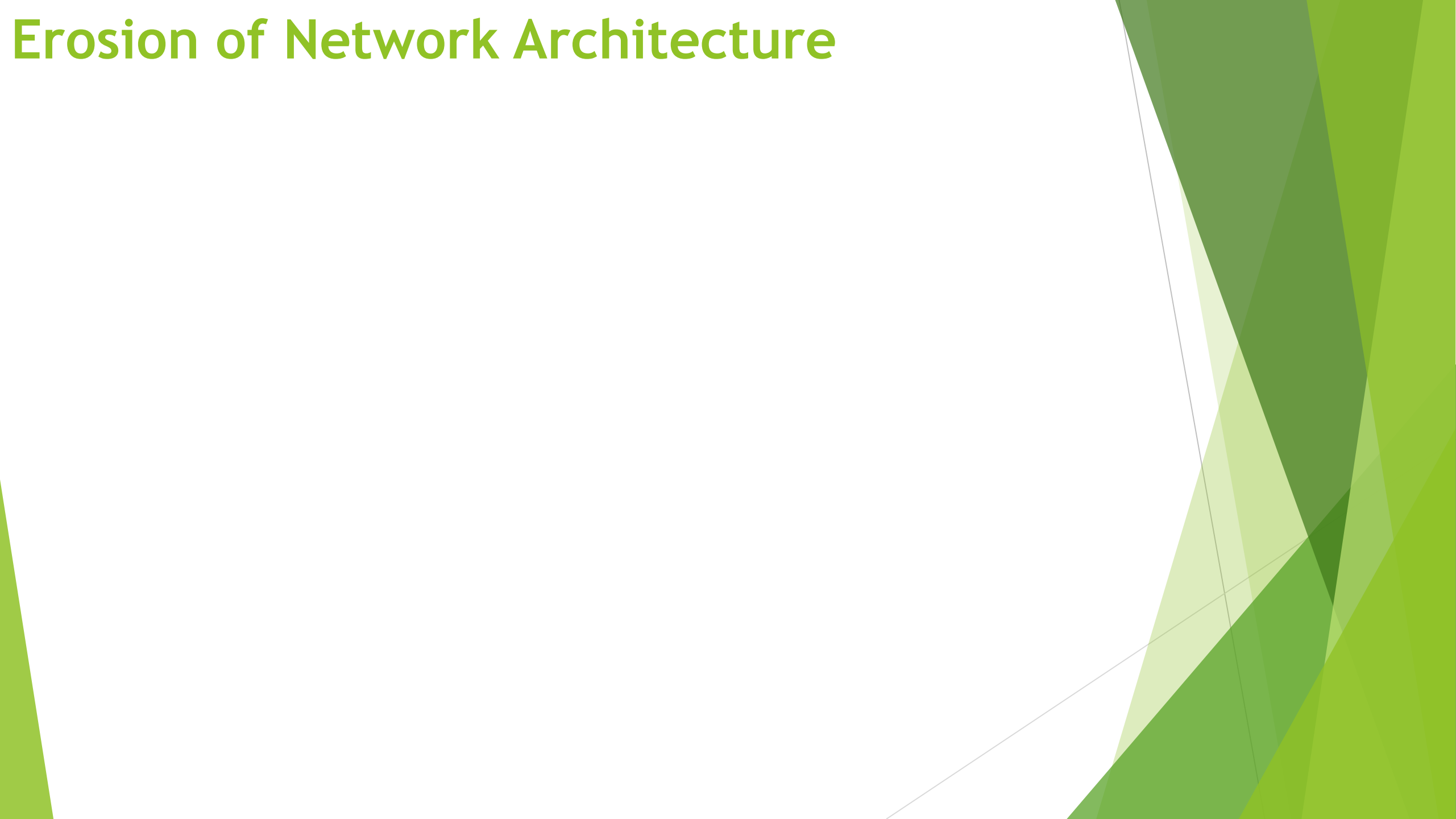


History of Vulnerability Disclosures in Industrial Control Systems Since 2010 (US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) <https://ics-cert.us-cert.gov>).

Common Challenges in OT security

- ▶ Erosion of Network Architecture
- ▶ Pervasive Legacy Systems
- ▶ Insecure Operational Protocols
- ▶ Modbus
- ▶ DNP3 (Distributed Network Protocol)
- ▶ ICCP (Inter-Control Center Communications Protocol)
- ▶ OPC (OLE for Process Control)
- ▶ International Electrotechnical Commission (IEC) Protocols
- ▶ Other Protocols
- ▶ Device Insecurity
- ▶ Dependence on External Vendors
- ▶ Security Knowledge 256

Erosion of Network Architecture



Erosion of Network Architecture

Erosion of Network Architecture:

- Two of the major challenges in securing industrial environments have been **initial design and ongoing maintenance**.
- The initial design **challenges arose from the concept that networks were safe due to physical separation from the enterprise with minimal or no connectivity to the outside world, and the assumption that attackers lacked sufficient knowledge to carry out security attacks**

Erosion of Network Architecture

- The challenge, and the biggest threat to network security, is **standards and best practices either being misunderstood or the network being poorly maintained.**
- In fact, from a **security design perspective**, it is better to know that communication paths are **insecure than to not know the actual communication paths.**
- This kind of organic growth has led to **miscalculations of expanding networks** and the introduction of **wireless communication in a standalone fashion**, without consideration of the impact to the original security design.

Pervasive Legacy Systems

Common Challenges in OT Security: Pervasive Legacy Systems:

- Due to the static nature and **long lifecycles of equipment** in industrial environments, many operational systems may be **deemed legacy systems**.
- For example, in a **power utility environment**, it is not uncommon to have **racks of old mechanical equipment** still operating alongside **modern intelligent electronic devices (IEDs)**.
- From a security perspective, this is **potentially dangerous** as many devices may have **historical vulnerabilities or weaknesses** that have not been **patched and updated**, or it may be that patches are not even available due to the **age of the equipment**.

Pervasive Legacy Systems

Common Challenges in OT Security: Pervasive Legacy Systems:

- communication methods and protocols may be **generations old** and must be interoperable with the **oldest operating entity in the communications path**.
- This includes **switches, routers, firewalls, wireless access points, servers, remote access systems, patch management, and network management tools**.
- All of these may have exploitable **vulnerabilities and must be protected**.

Insecure Operational Protocols

- Industrial protocols, such as **supervisory control and data acquisition(SCADA)** particularly the older variants, suffer from common security issues.
- Three examples of this are a **frequent lack of authentication** between communication endpoints, **no means of securing and protecting** data at rest or in motion, and **insufficient granularity of control** to properly specify recipients or avoid default broadcast approaches.

Modbus

- Modbus is commonly found in many industries, such as **utilities and manufacturing environments, and has multiple variants** (for example, serial,TCP/IP).
- It was created by the first **programmable logic controller (PLC)** vendor, **Modicon**, and has been in use since the **1970s**.
- It is one of the most widely used protocols in industrial deployments, and its development is governed by the **Modbus Organization**.

Modbus

- **Authentication of communicating endpoints** was not a default operation because it would allow an inappropriate source to **send improper commands** to the recipient.
- For example, for a message to reach its destination, nothing more than the proper **Modbus address and function call (code)** is necessary.
- Some older and serial-based versions of **Modbus communicate via broadcast**.
- The ability to curb the **broadcast function** does not exist in some versions.

- DNP3 is found in **multiple deployment scenarios** and industries.
- It is common in utilities and is also found in **discrete and continuous process** systems. Like many other **ICS/SCADA protocols**, it was intended for serial communication between **controllers and simple IEDs**.
- In the case of DNP3, participants **allow for unsolicited responses**, which could trigger an undesired response.

and protocols may be...

DNP3 (Distributed Network Protocol):

- The missing security element here is the ability to **establish trust** in the system's state and thus the ability **to trust the veracity of the information** being presented.
- This is akin to the **security flaws presented by Gratuitous ARP messages** in Ethernet networks, which has been addressed by **Dynamic ARP Inspection (DAI)** in modern Ethernet switches.

How IT and OT Security Practices and Systems Vary

Feature	IT Security	OT Security
Focus	Data Confidentiality	System Availability & Safety
Main Concern	Data breaches & cyberattacks	Physical disruptions & system failures
Patching & Updates	Frequent updates	Limited updates due to uptime requirements
Access Control	Open & flexible	Restricted & controlled
Communication	Open protocols & internet-based	Proprietary & real-time systems