CUI-CON

CMMC Considerations for OT Environments

What are we talking about?

- More acronyms, what is OT?
- CMMC scoping guide
- Basic cybersecurity safeguards for OT environments
- What are “Risk-based security policies, procedures, and practices”?

What are we talking about?

- More acronyms, what is OT?
- CMMC scoping guide
- Basic cybersecurity safeguards for OT environments
- What are “Risk-based security policies, procedures, and practices”?

What are we talking about?

- More acronyms, what is OT?
- **CMMC scoping guide**
- Basic cybersecurity safeguards for OT environments
- What are “Risk-based security policies, procedures, and practices”?

What are we talking about?

- More acronyms, what is OT?
- CMMC scoping guide
- **Basic cybersecurity safeguards for OT environments**
- What are “Risk-based security policies, procedures, and practices”?

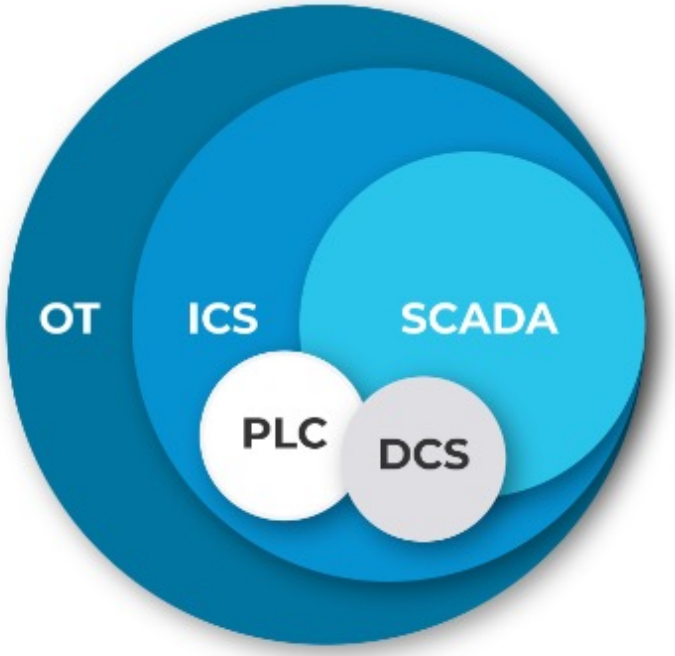
What are we talking about?

- More acronyms, what is OT?
- CMMC scoping guide
- Basic cybersecurity safeguards for OT environments
- What are “Risk-based security policies, procedures, and practices”?

...with the right combination of letters...

- OT – Operational Technology
  - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

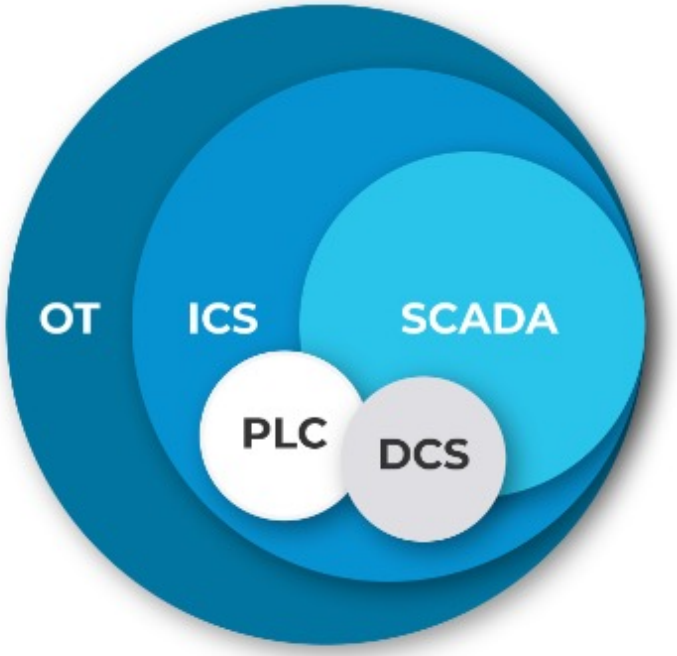
- ICS – Industrial Control Systems
  - PLC - Programmable Logic Controllers
  - DCS - Distributed Control System
- SCADA - Supervisory Control and Data Acquisition



...with the right combination of letters...

- **OT – Operational Technology**
  - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

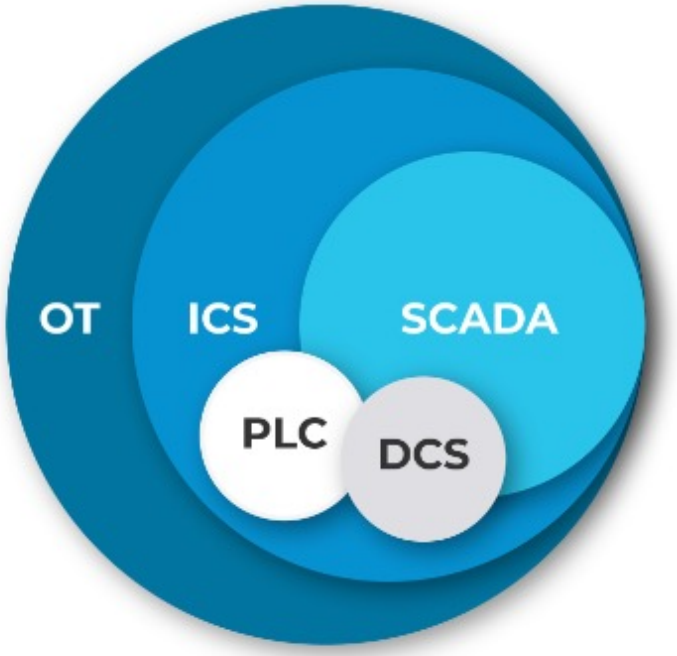
- ICS – Industrial Control Systems
  - PLC - Programmable Logic Controllers
  - DCS - Distributed Control System
- SCADA - Supervisory Control and Data Acquisition



...with the right combination of letters...

- OT – Operational Technology
  - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

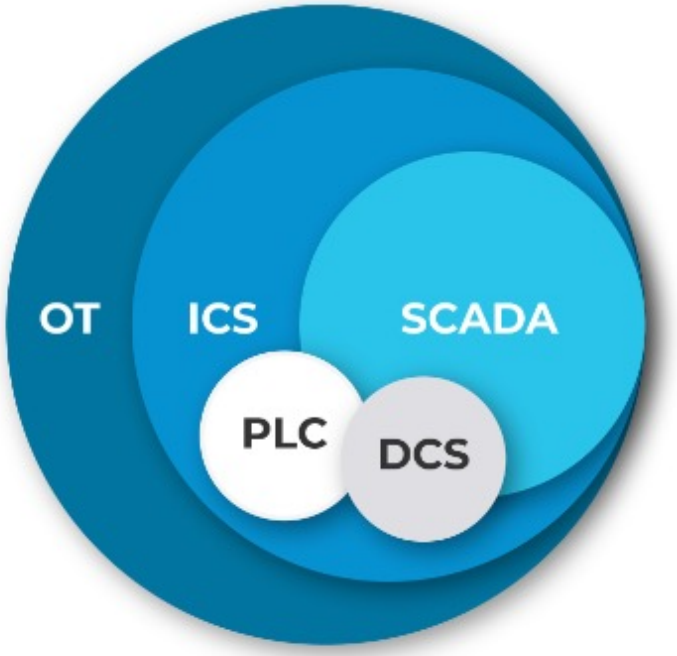
- **ICS – Industrial Control Systems**
  - PLC - Programmable Logic Controllers
  - DCS - Distributed Control System
- SCADA - Supervisory Control and Data Acquisition



...with the right combination of letters...

- OT – Operational Technology
  - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

- ICS – Industrial Control Systems
  - PLC - Programmable Logic Controllers
  - DCS - Distributed Control System
- **SCADA - Supervisory Control and Data Acquisition**



CMMC L2 Scoping Guide

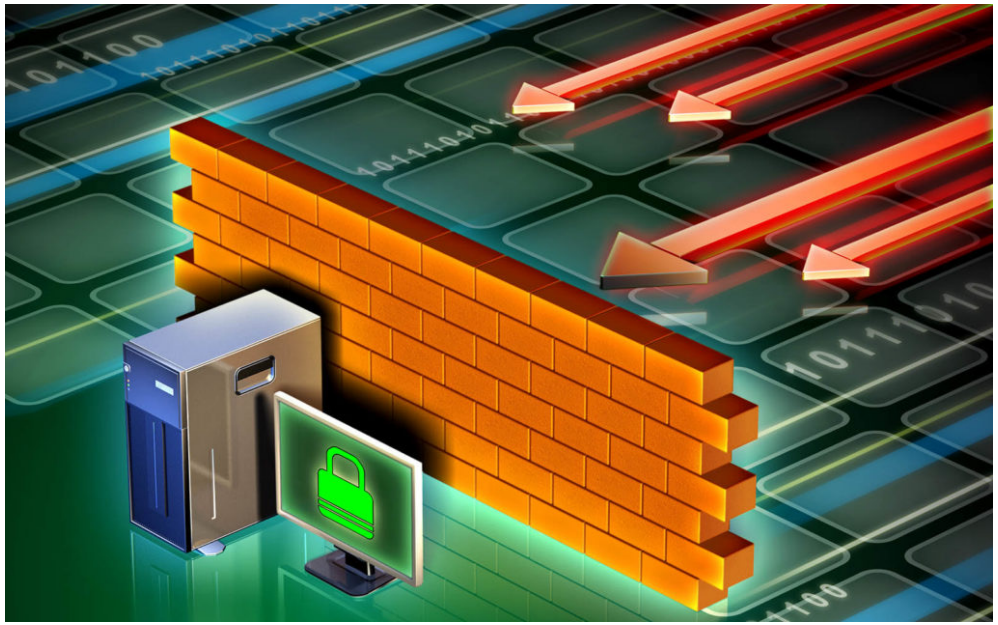
- Defines asset categories and protection requirements for those assets
  - CUI Assets
  - Security Protection Assets
  - Contractor Risk Managed Assets
  - Specialized Assets
  - Out of Scope

CUI Assets

- Assets that process, store, or transmit CUI
  - Document in Asset Inventory
  - Document in SSP
  - Document in Network Diagram
  - Will be assessed against CMMC practices/800-171 controls

Security Protection Assets

- Assets that provide security functions to the assessment scope
  - Document in Asset Inventory
  - Document in SSP
  - Document in Network Diagram
  - Will be assessed against CMMC practices/800-171 controls

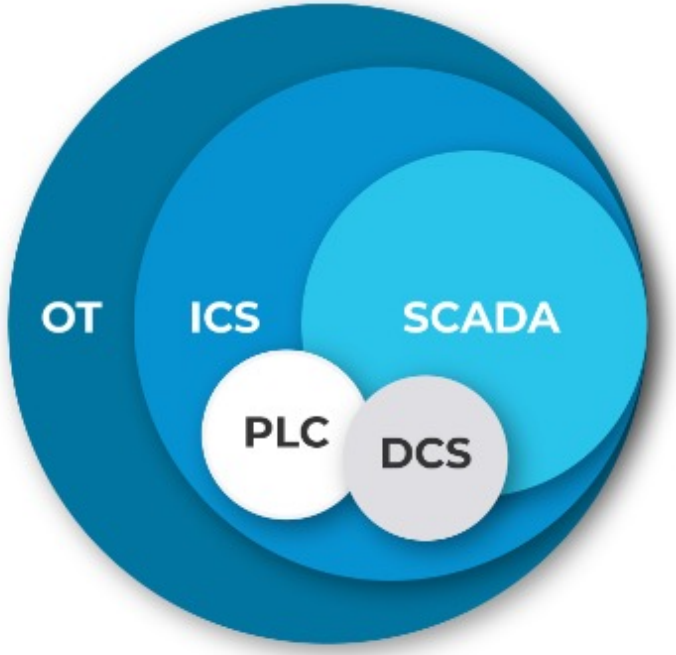


Contractor Risk Managed Assets

- Assets that are within the boundary but **shouldn't** be processing, storing, or transmitting CUI
  - Document in Asset Inventory
  - Document in SSP
  - Document in Network Diagram
  - Manage in accordance with defined policies and procedures

Specialized Assets

- Assets that **may** or may not process, store, or transmit CUI
- At a **minimum**, the contractor is required to:
  - Document in Asset Inventory
  - Document in SSP
  - Document in Network Diagram
  - Manage in accordance with defined policies and procedures
  - Not assessed against CMMC practices/NIST 800-171 controls
- A Certified Assessor will review the SSP to verify that specialized assets are managed using the contractor's risk-based information security policy, procedures, and practices and accounted for within the contractor's Assessment Scope

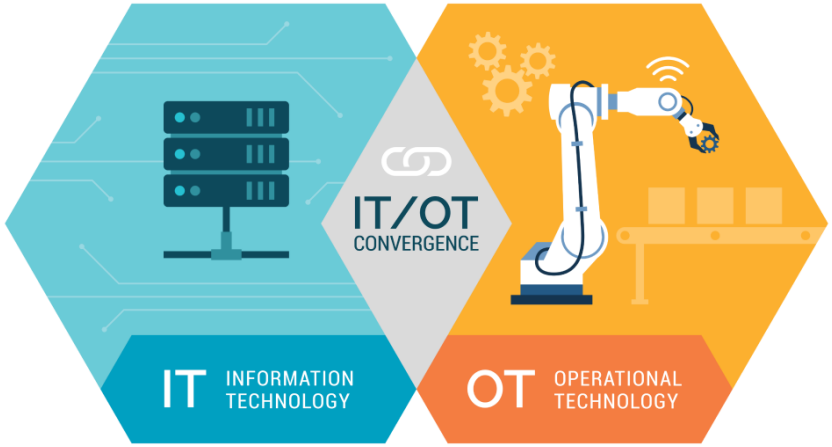


Specialized Assets

- OT is considered a “Specialized Asset” in the CMMC Scoping Guide and is defined as follows:
  - OT is used in manufacturing systems, industrial control systems (ICS), or supervisory control and data acquisition (SCADA) systems. OT may include programmable logic controllers (PLCs), computerized numerical control (CNC) devices, machine controllers, fabricators, assemblers, and machining.

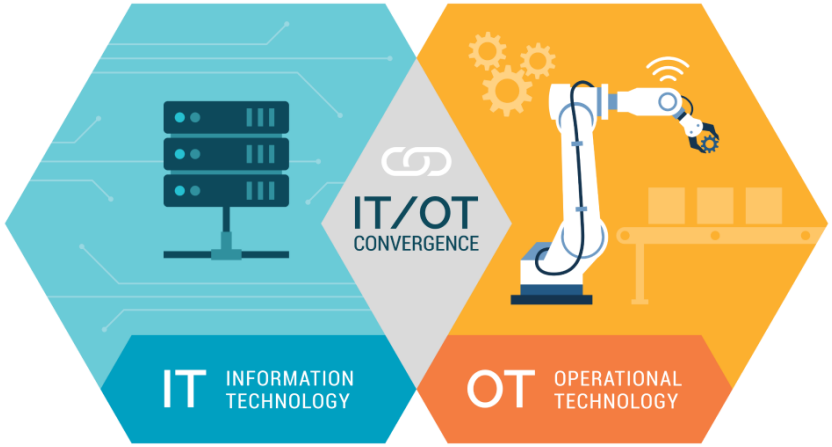
Segmenting OT Assets

- Separation Techniques
  - Logical Separation – Firewalls and VLANs
    - OT assets should be segmented from IT assets using a robust ruleset to enforce data flows
    - Data flows should be identified and documented in a diagram and in the SSP
    - Special care should be taken to document interconnections between environments
  - Physical Separation – Locks, Badge Access, Gates
    - The shop floor should be physically separated where possible from the rest of the environment
    - Only authorized and trained personnel should have access to the shop floor



Defense in Depth

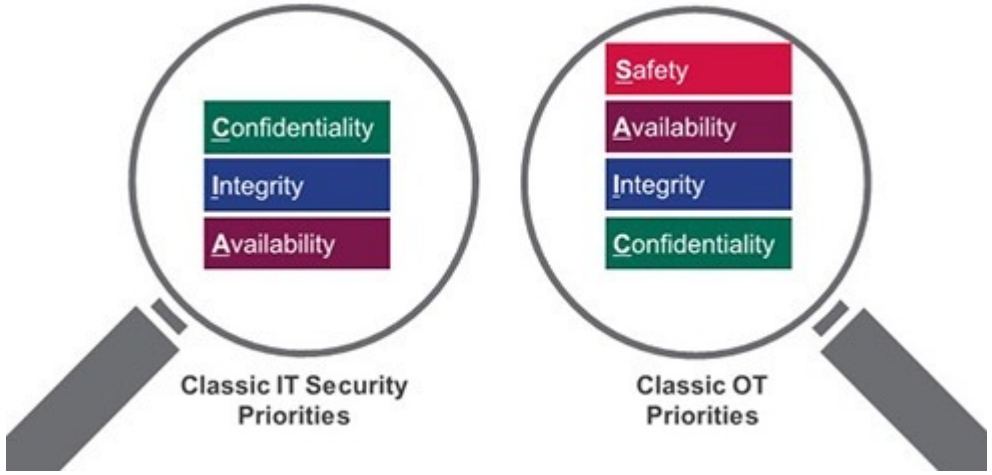
- The use of layered people, processes, and technology to minimize the impact of a single control failure
  - Governance – Have a plan and strategy
  - Physical – Reducing the risk of accidental or intentional loss by controlling the environment
  - Network Security – Segmenting access to the OT environment
  - Logging – Capturing what is happening in the environment and creating audit trails
  - Monitoring – Combining data to identify any problems in the environment
  - Hardware Security
  - Software Security



Different Security Priorities for OT

While IT environments are concerned with Confidentiality, Integrity, and Availability, OT environments, OT environments prioritize Safety, Availability, and Integrity over Confidentiality

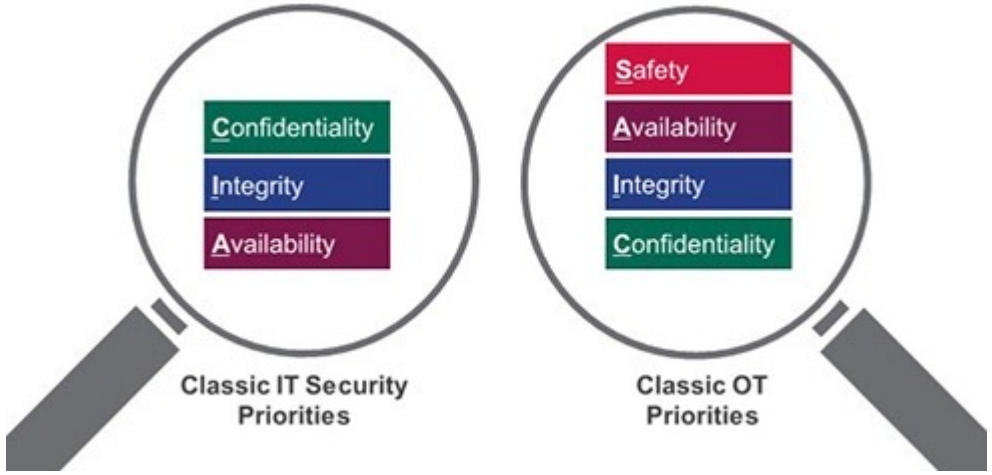
- Safety – Ensuring that processes are carried out in a manner that protects the operator
- Availability – Minimizing downtime
- Integrity – Delivering expected results
- Confidentiality – Preventing the unintended leak of valuable information



Different Security Priorities for OT

While IT environments are concerned with Confidentiality, Integrity, and Availability, OT environments, OT environments prioritize Safety, Availability, and Integrity over Confidentiality

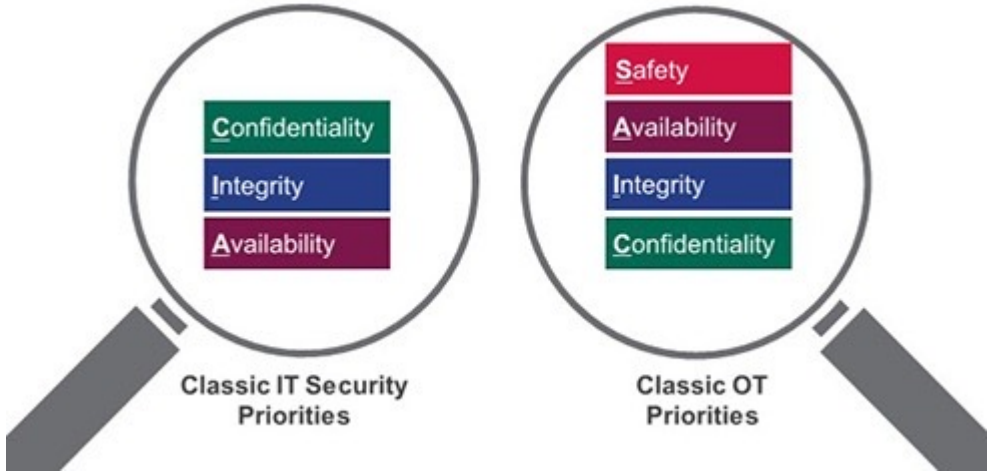
- **Safety – Ensuring that processes are carried out in a manner that protects the operator**
- Availability – Minimizing downtime
- Integrity – Delivering expected results
- Confidentiality – Preventing the unintended leak of valuable information



Different Security Priorities for OT

While IT environments are concerned with Confidentiality, Integrity, and Availability, OT environments, OT environments prioritize Safety, Availability, and Integrity over Confidentiality

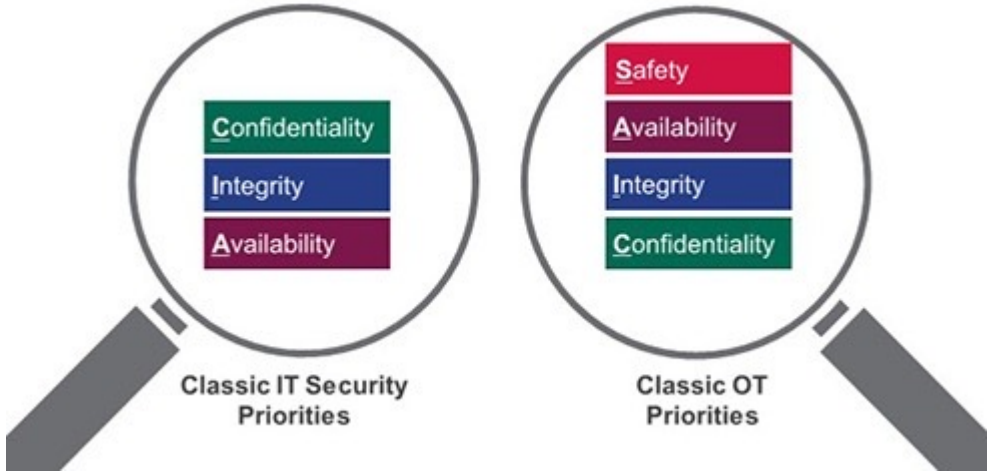
- Safety – Ensuring that processes are carried out in a manner that protects the operator
- **Availability – Minimizing downtime**
- Integrity – Delivering expected results
- Confidentiality – Preventing the unintended leak of valuable information



Different Security Priorities for OT

While IT environments are concerned with Confidentiality, Integrity, and Availability, OT environments, OT environments prioritize Safety, Availability, and Integrity over Confidentiality

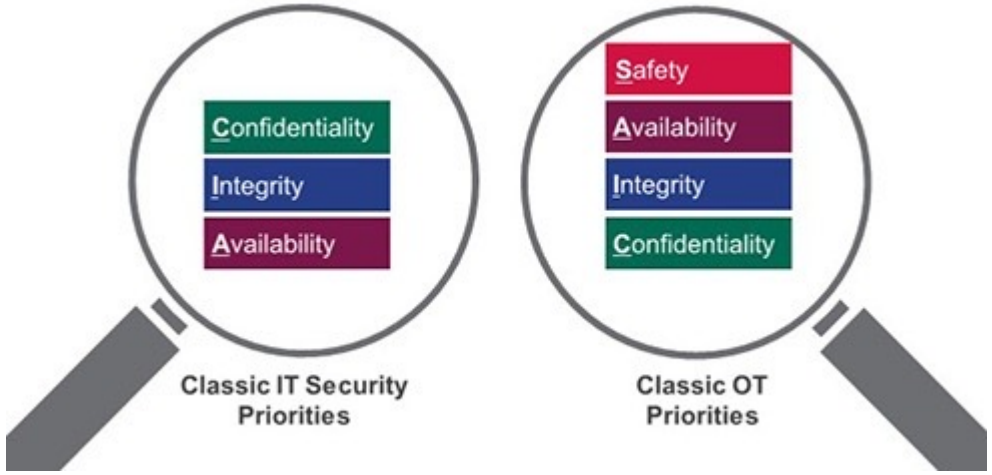
- Safety – Ensuring that processes are carried out in a manner that protects the operator
- Availability – Minimizing downtime
- **Integrity – Delivering expected results**
- Confidentiality – Preventing the unintended leak of valuable information



Different Security Priorities for OT

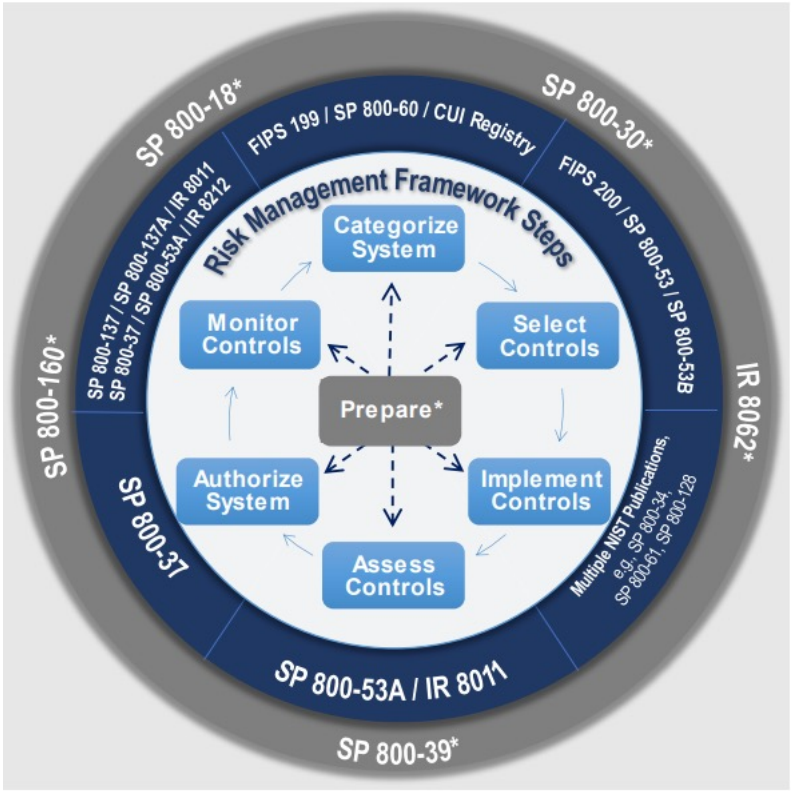
While IT environments are concerned with Confidentiality, Integrity, and Availability, OT environments, OT environments prioritize Safety, Availability, and Integrity over Confidentiality

- Safety – Ensuring that processes are carried out in a manner that protects the operator
- Availability – Minimizing downtime
- Integrity – Delivering expected results
- **Confidentiality – Preventing the unintended leak of valuable information**



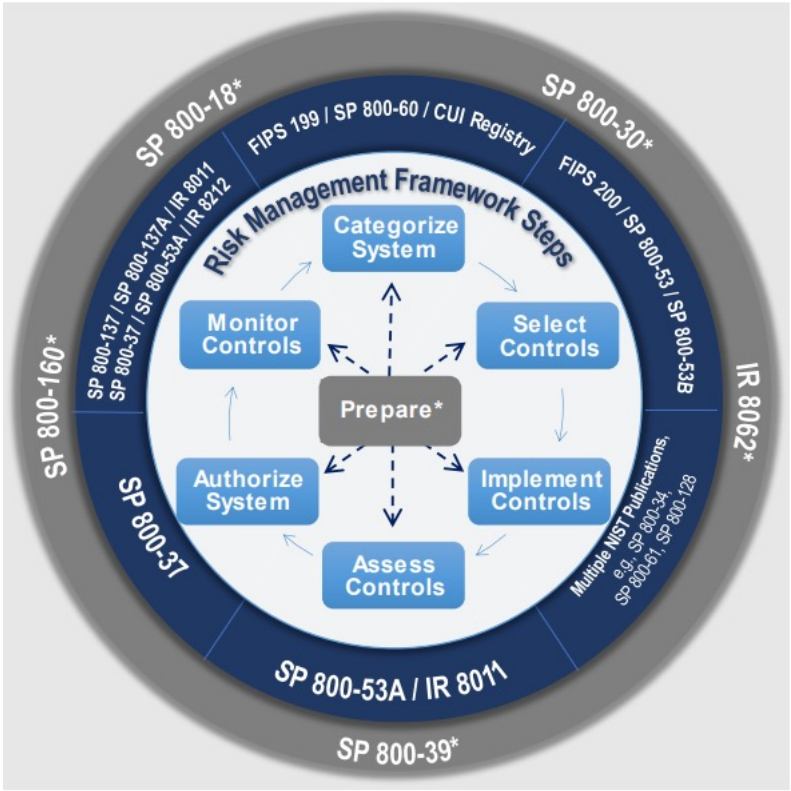
NIST 800-82

- Guide to Operational Technology (OT) Security
  - Application of NIST RMF (Risk Management Framework) to OT environments (people, processes, technology)
    - Prepare
    - Categorize
    - Select Controls
    - Implement Controls
    - Test Controls
    - Monitor Controls



Securing the Environment and Developing Assurance

- Identify roles and stakeholders
- Document your strategy for managing risk within the environment
- Identify risks within the environment and select appropriate controls to manage risk
- Document how controls will be implemented in your governance documents (policies and procedures)
- Implement the controls
- Assess and continuously monitor controls



Core Controls

- Maintain Asset Inventory
- Mapping Data Flows and Environment
- Identity Management and Access Control
- Logical Access Control
- Physical Access Control
- Segmentation
- Awareness and Training
- Data Security
- Least Functionality
- Change Management
- Incident Response
- Maintenance

Core Controls cont.

- Logging
- Media Protection
- Personnel Security
- Remote Access/Third Party Access
- Patch Management
- Time Synchronization
- Event Management and Anomaly Detection
- Continuous Monitoring
  - Malicious Code
  - Event and User level monitoring
  - Network Monitoring
  - Vulnerability Scanning

Policies and Procedures

- Should be based on a common framework
  - NIST 800-53
  - Secure Controls Framework (SCF)
  - No need to reinvent the wheel

- Govern OT policies in the same manner as IT policies
  - Senior leadership ownership
  - Regular reviews
  - User education on cybersecurity responsiblities

- Procedures should be delegated to relevant stakeholders
  - Get stakeholder buy-in
  - SMEs can turn policy statements into operating procedures

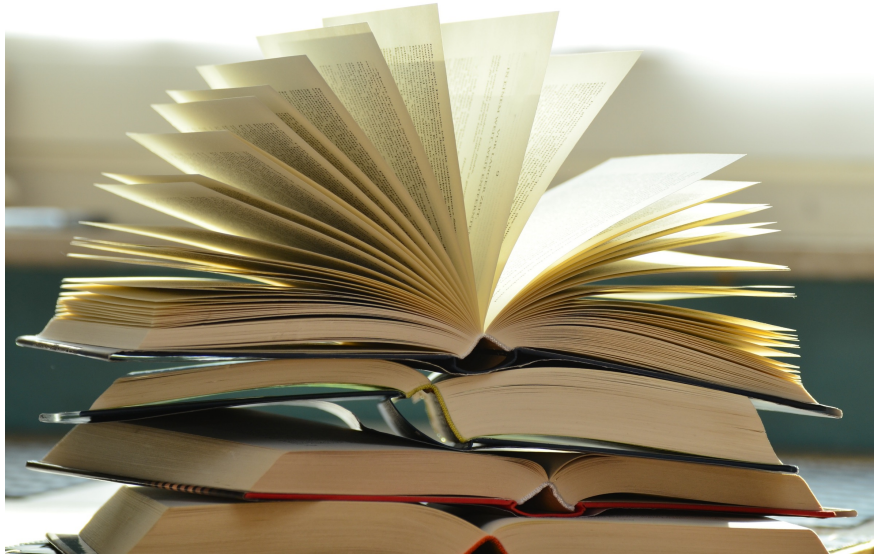
Business Case for OT cybersecurity investment

- Increasing scrutiny of OT environments by regulatory agencies
- Senior leadership visibility on the business impact of failure scenarios
  - Application of BCP/DR (Business Continuity Planning and Disaster Recovery) principles to create business case for OT CAPEX through tech refresh or additional compensating controls
- Roadmap for identifying and remediating risks within the OT environment
- Working with Operational Risk Management functions to quantify failure scenarios
- Evaluating and communicating cybersecurity posture through maturity based assessments

What to expect

- “Risk based policies and procedures” are a stop-gap to more prescriptive requirements
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) being more broadly applied in the energy sector
- Moving away from “just air gap it” and compensating controls as cost prohibitive detriments to efficiency
- More malicious code/firmware attacks by state actors taking advantage of immature OT security posture

Bedtime Reading



- MITRE ATT&CK ICS Techniques
  - https://attack.mitre.org/techniques/ics/
- NIST 800-82r3 – Guide to OT Security
  - https://csrc.nist.gov/pubs/sp/800/82/r3/final
- CMMC Level 2 Scoping Guide
  - https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf
- SCF (Secure Controls Framework) Integrated Controls Management Model
  - https://securecontrolsframework.com/integrated-controls-management/