PROJECT
ENG
PRO

CYBER SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

By Project ENG PRO

FR 7 – Resource Availability

- FR1 – Identification, authentication and access control
- FR2 – Use Control
- FR3 – System Integrity
- FR4 – Data Confidentiality
- FR5 – Restrict Data Flow
- FR6 – Timely response to event
- FR7 – Resource Availability

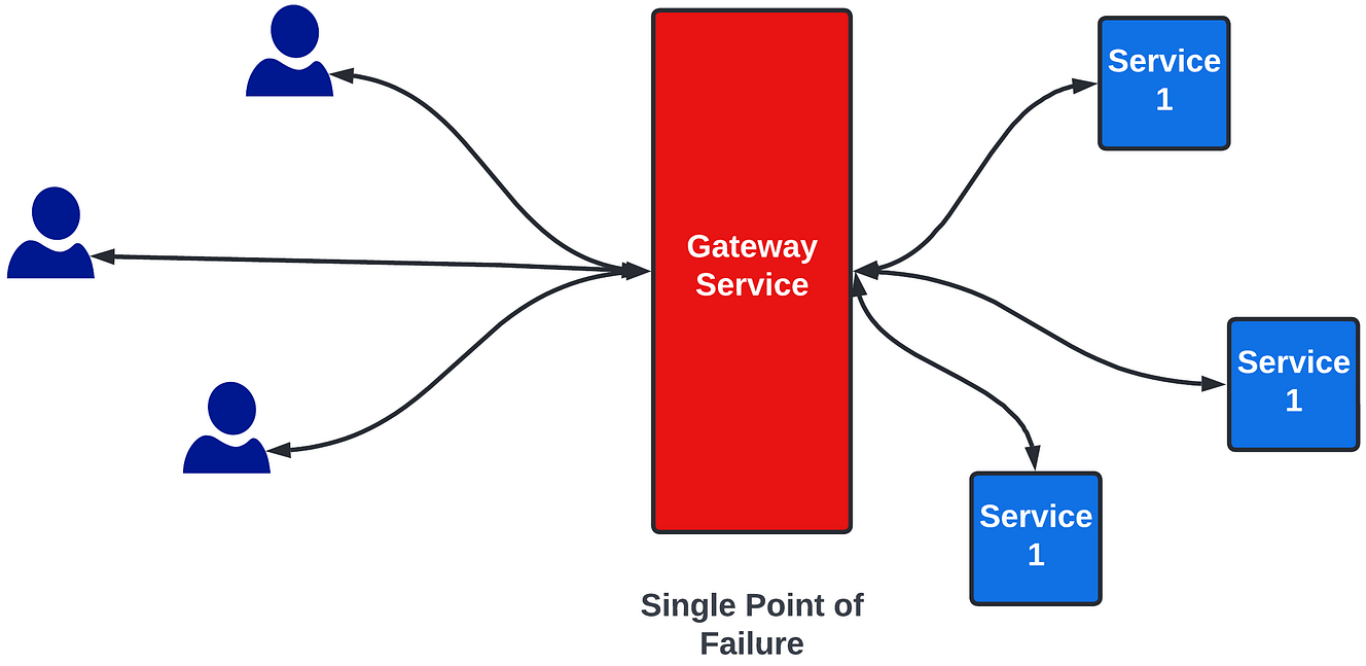
Resource Availability

It is crucial to have a robust monitoring system in place that can report the current list of installed components and their associated properties.

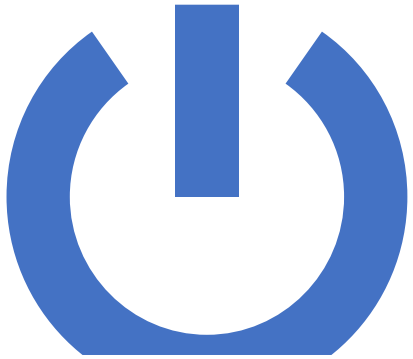
Resource Availability

It's essential to address the concept of avoiding single points of failure and instead enhancing redundancy and fault tolerance.

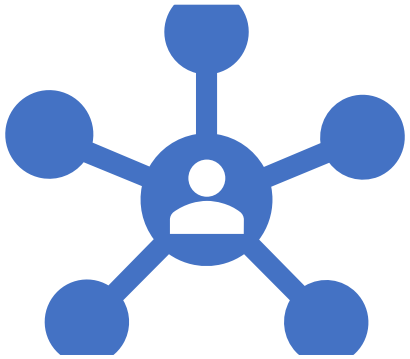
It's crucial to integrate security throughout the entire environment. Conduct a thorough evaluation to identify potential points of failure.



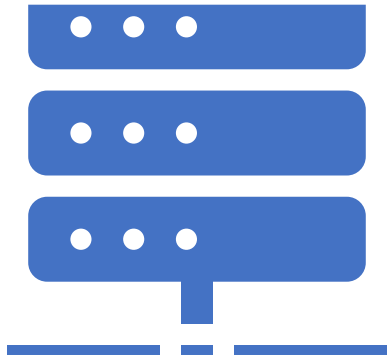
Single Points of Failure



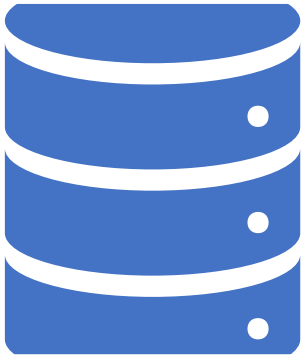
Power Supply



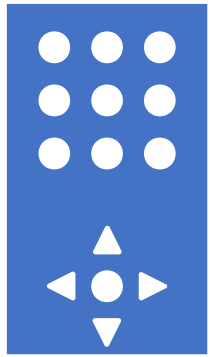
Network Link



Server RAID Configuration



Data Backups



Control System Components

SINGLE POINT OF FAILURE MITIGATION

RISK ASSESSMENT

PINPOINT EXPOSURE

COST VS. IMPACT ANALYSIS

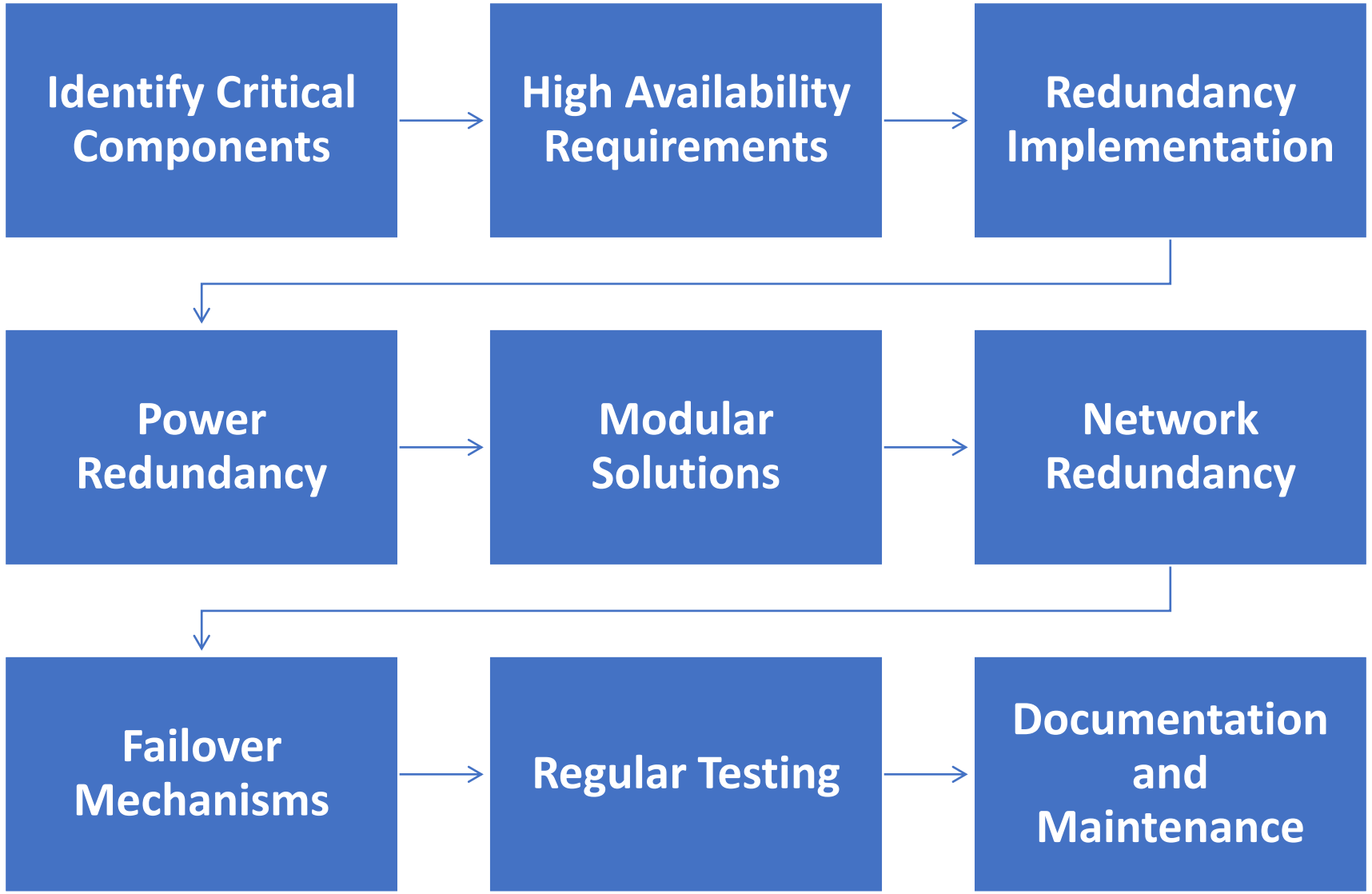
PRIORITIZE CRITICAL POINTS

IMPLEMENTATION OF SOLUTIONS

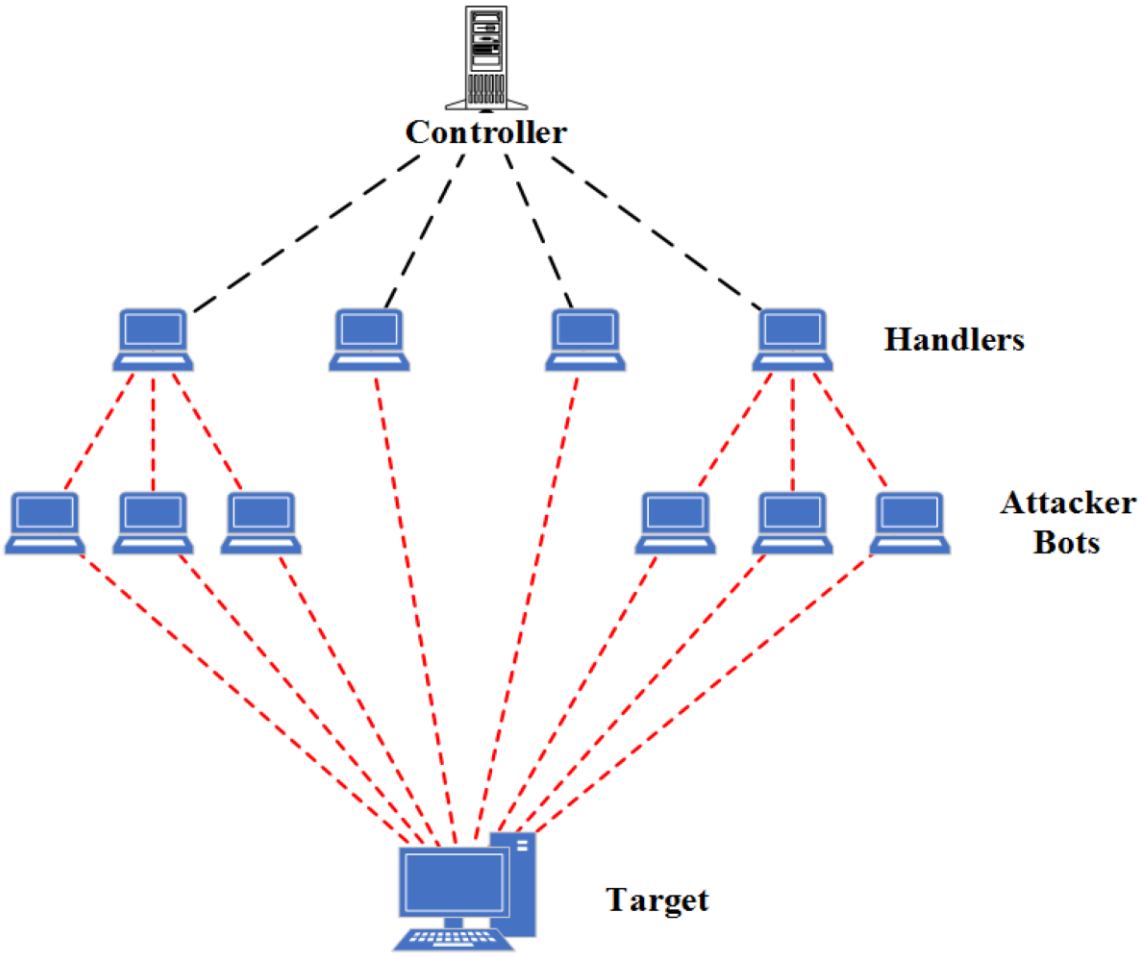
TESTING AND VALIDATION

CONTINUOUS MONITORING

Redundancy and Fault Tolerance



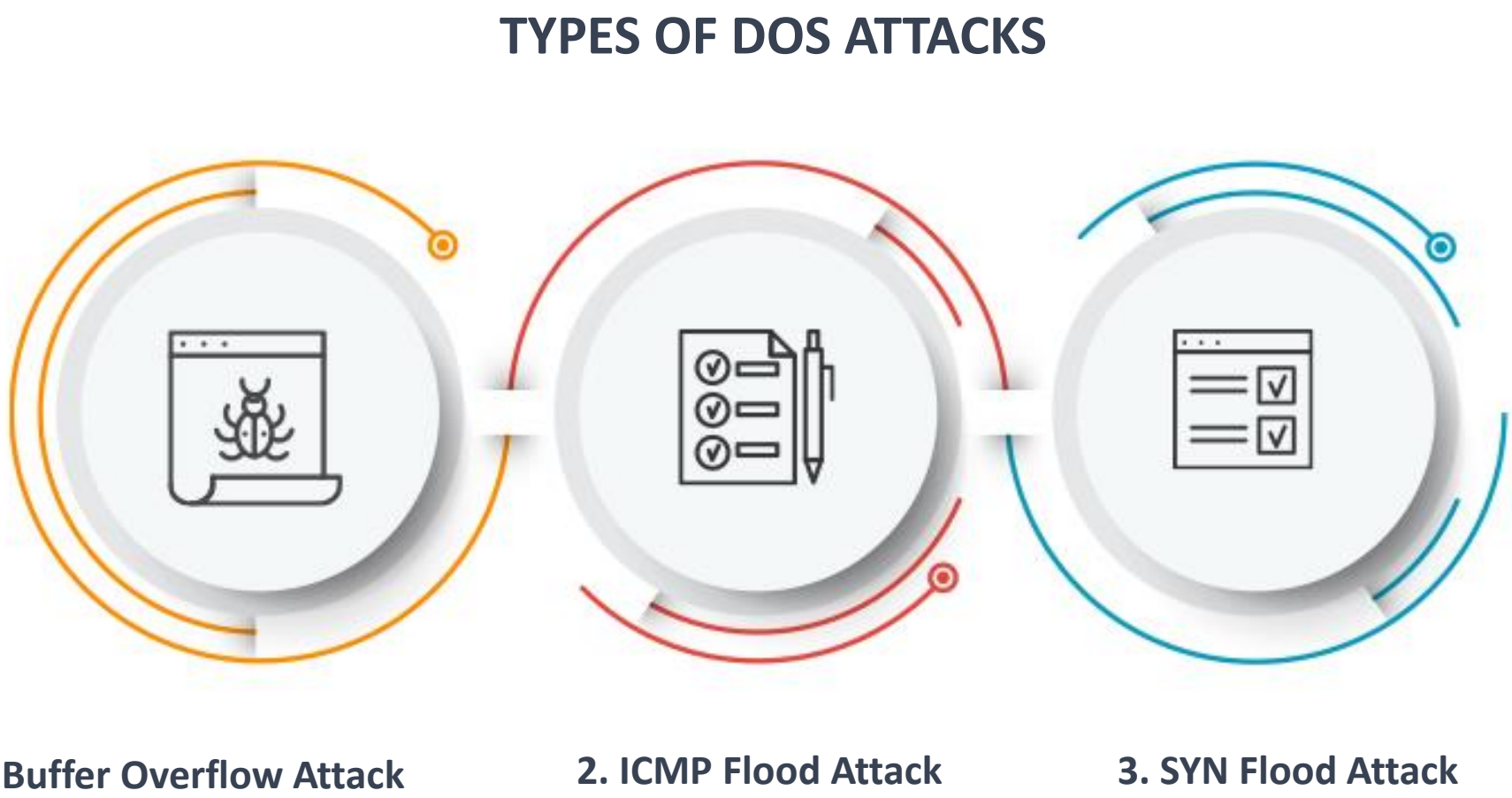
Graceful failure



Denial of Service Attack

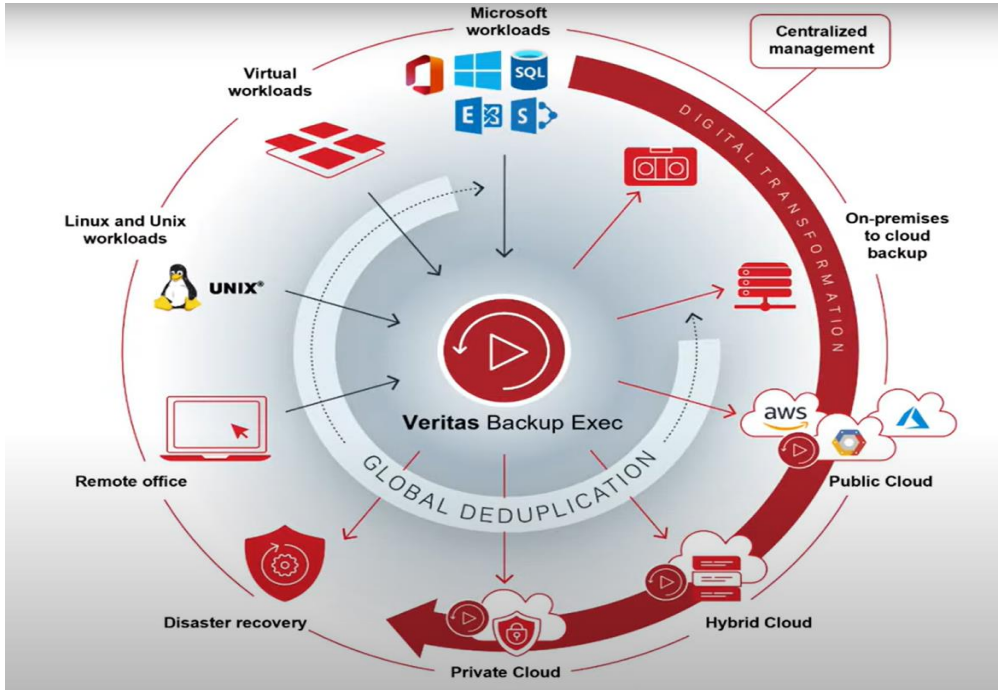
A DoS attack aims to make a system or network inaccessible to its intended users. Attackers achieve this by flooding the target with excessive traffic, overwhelming its resources and causing service disruptions.

Denial of Service Attack



Control System Backup

- Regular backups for latest PLC and app versions.
- Quick data restoration within RTO.
- Centralized backup systems for speed.
- Validate and test backup process.
- Use solutions like Acronis, Veritas, vendor tools.
- Vendor-specific solutions for automation.
- Reliable backups minimize downtime.



Wrap Up