Nugroho Prananto Utomo

Senior Consultant
DNV

Control System Architecture: From Flat Network to Zero Trust

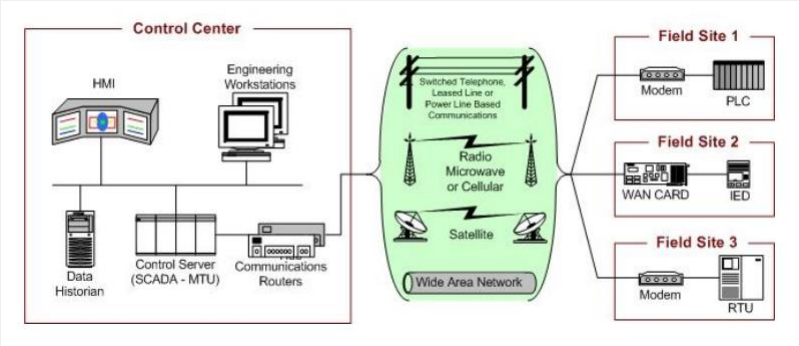
Control System Architecture: From Flat Network to Zero Trust

Energy Innovation 2021

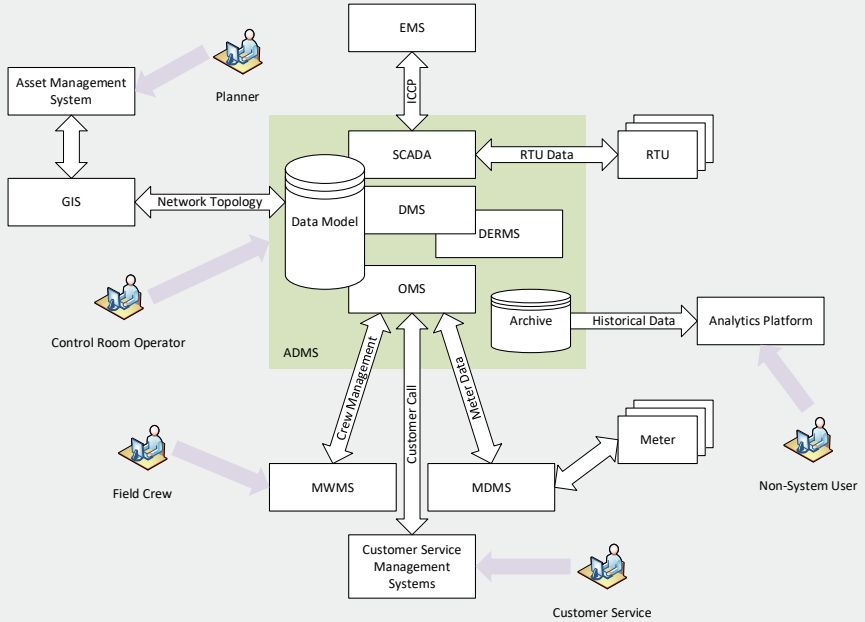
Nugroho Prananto Utomo

23 July 2021

Control System Network Evolution



- Reference: NIST 800-82

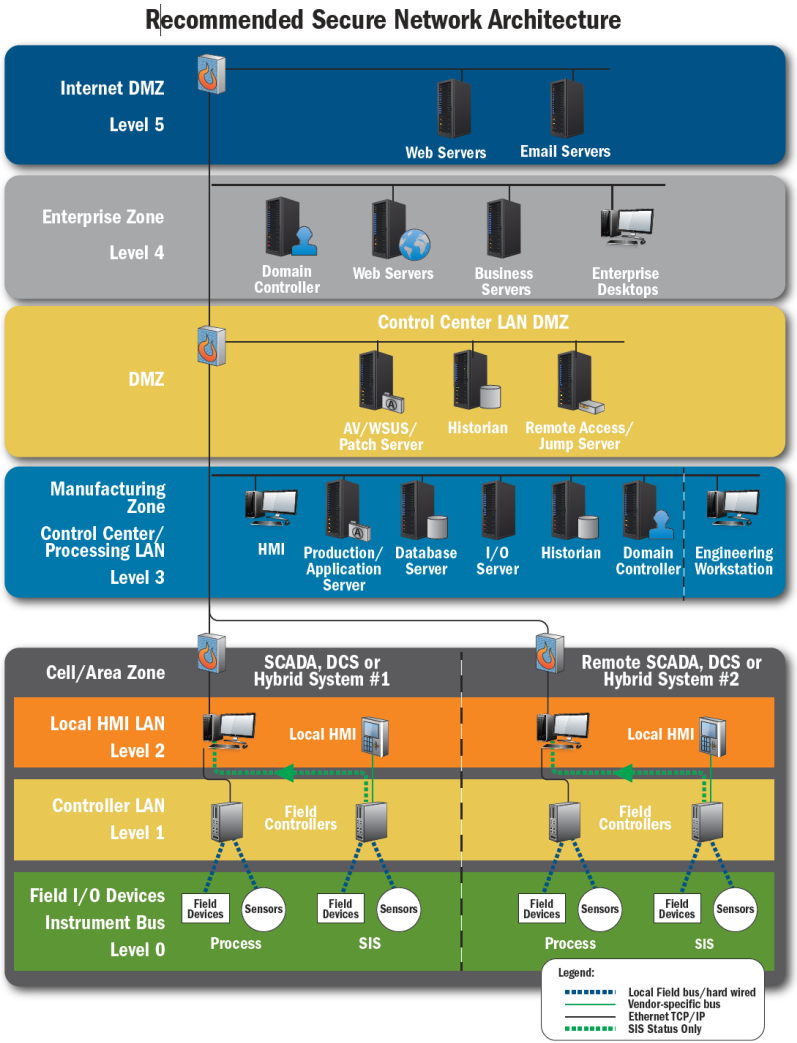


- Advance Distribution Management System (ADMS) conceptual design

Securing Control System Network

Purdue Enterprise Reference Architecture

IEC 62443 Zones and Conduits



- Recommended secure network architecture from DHS ICS-CERT Défense-in-Depth Recommended Practice

Conduit Devices between Zones

- Next-Generation Firewall
  - Application layer firewall
  - Packet inspection and control
- Unidirectional Gateway
  - Only support specific protocol

- **Challenges:**
  - Increasing number of required remote connection that required as part of Control System business process, e.g:
    - Field Crew access via public internet
    - IoT penetration that can help to gather more data
  - Increasing number of IT-based system integration, makes the “advance” conduit design more complicated

- *“Hard and crunchy on the outside, soft and chewy in the middle”*

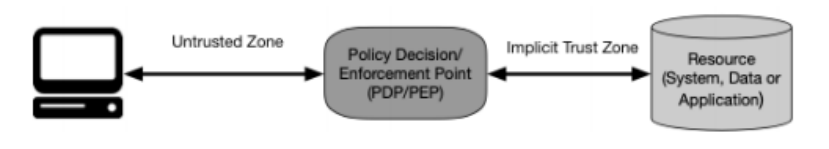
Zero Trust Architecture

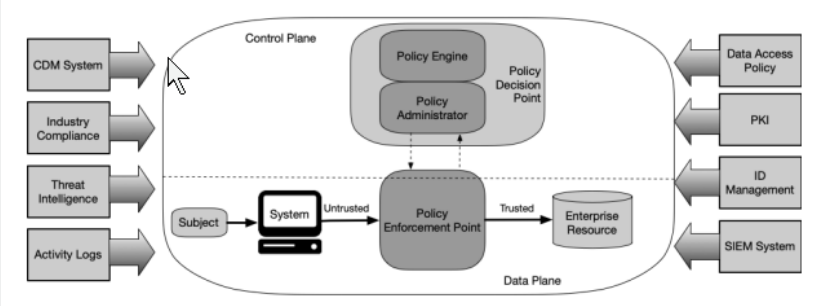
“A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries”

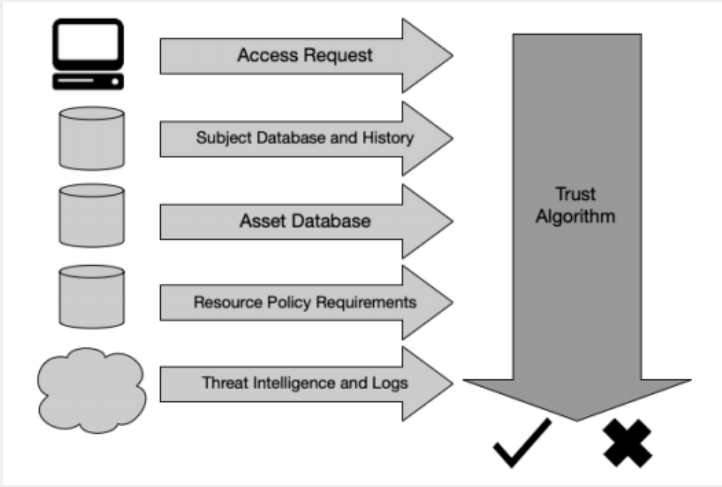
- US Executive Order on Improving the Nation’s Cybersecurity (May 2021)

- All data sources and computing power are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

Zero Trust Architecture
NIST SP 800-207







- Zero Trust Logical Component
- Trust Algorithm Input

Zero Trust Architecture

- Benefit
  - Eliminates implicit trust
    - Improve the scalability of the system and integration
  - Provide real-time assessment to determine access
    - Improve the security and limit the “lateral” attack

- Challenges
  - Introducing ZTA to a Perimeter-Based Architected Network will need additional efforts to identify assets, subjects, data flows and workflow

Nugroho Prananto Utomo

nugroho.prananto@dnv.com
+65 9771 9081

www.dnv.com