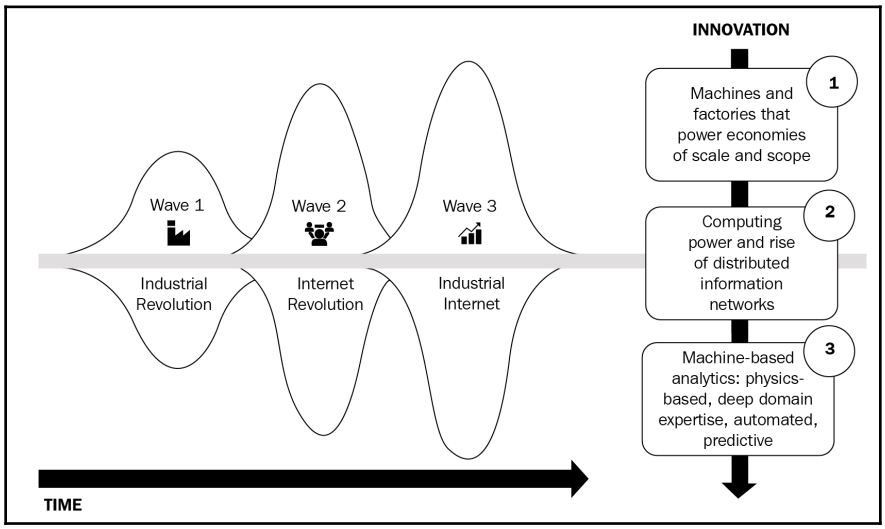
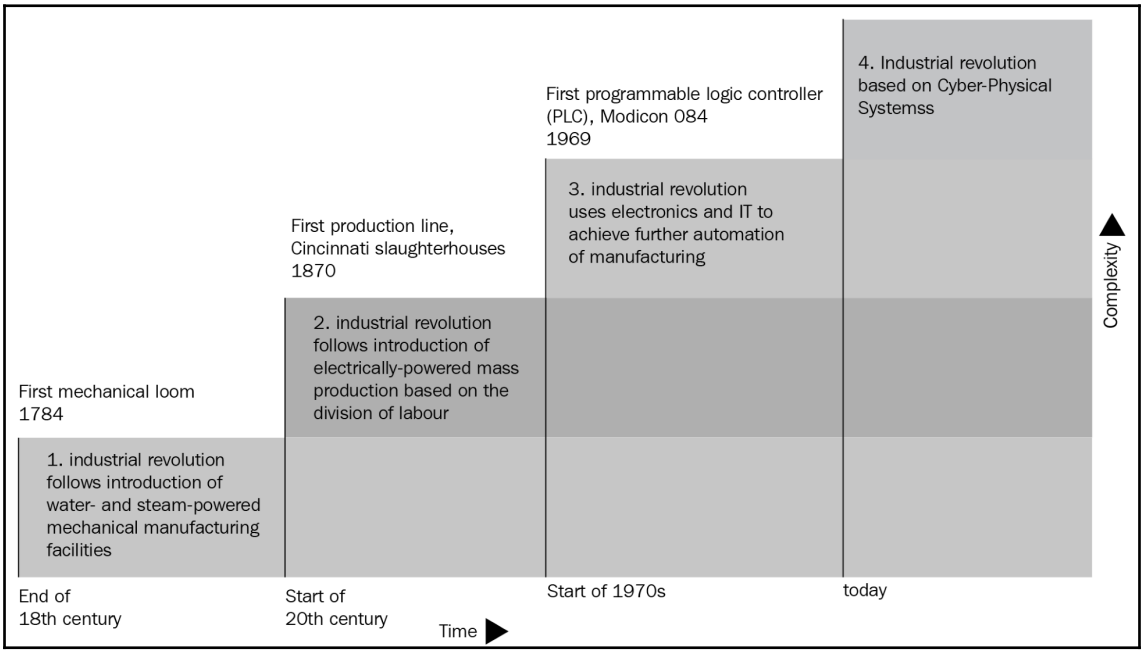
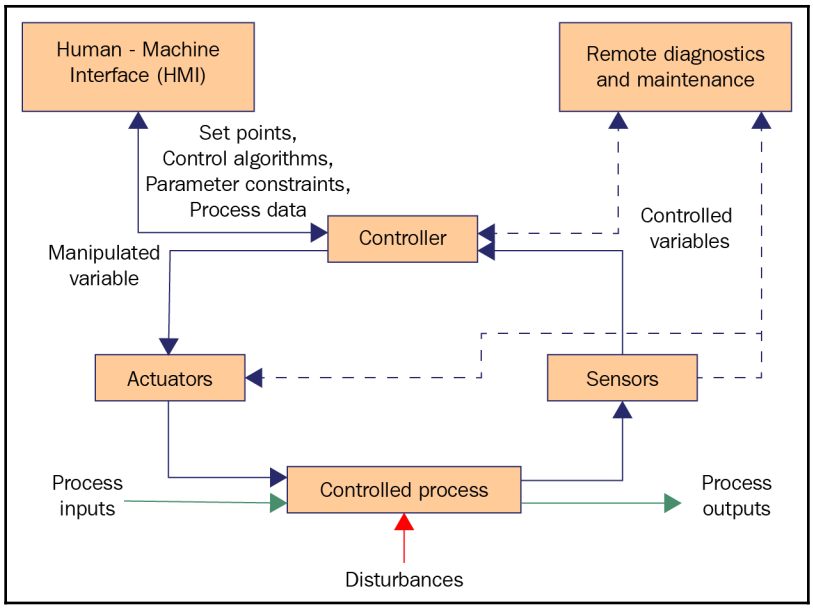
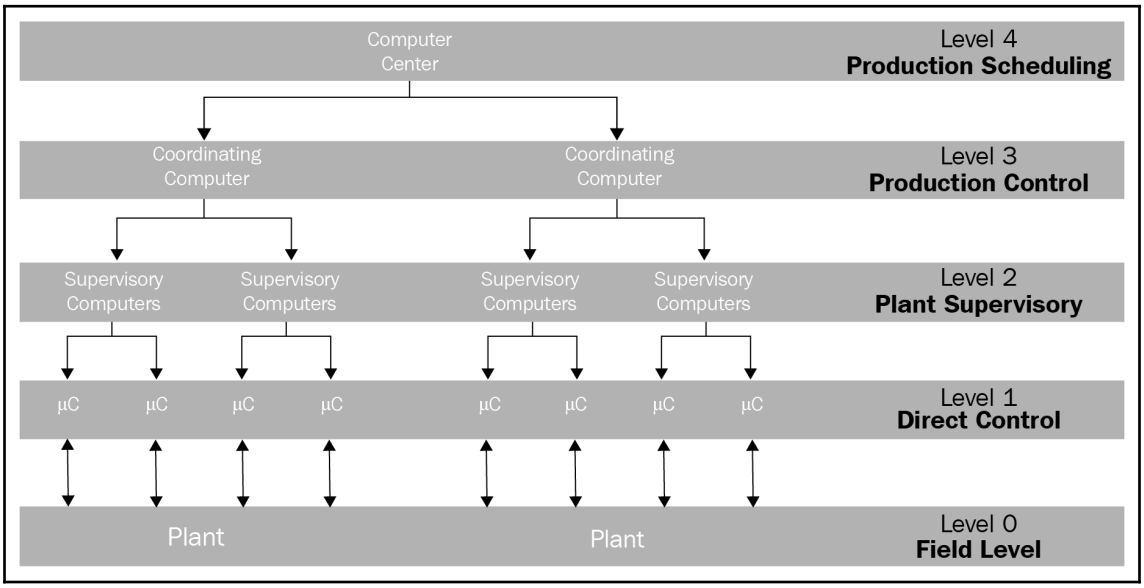
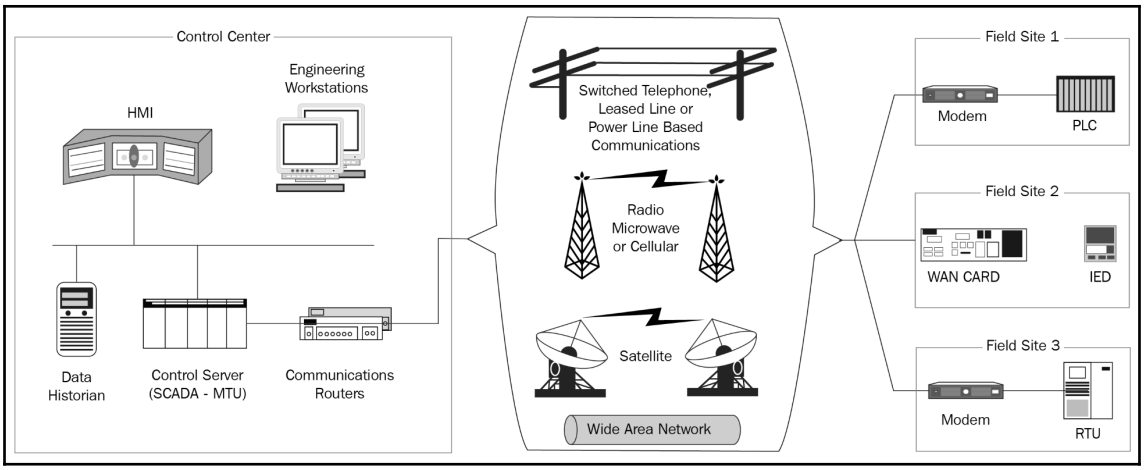
Chapter 01: An Unprecedented Opportunity at Stake

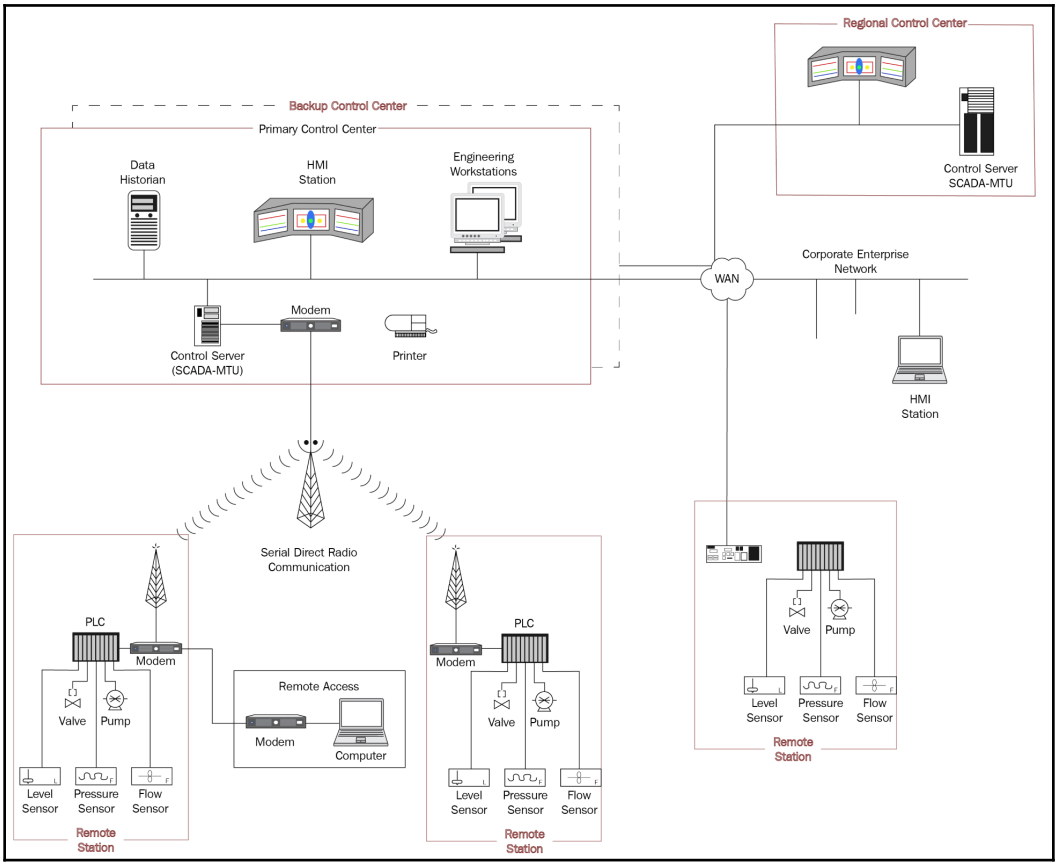


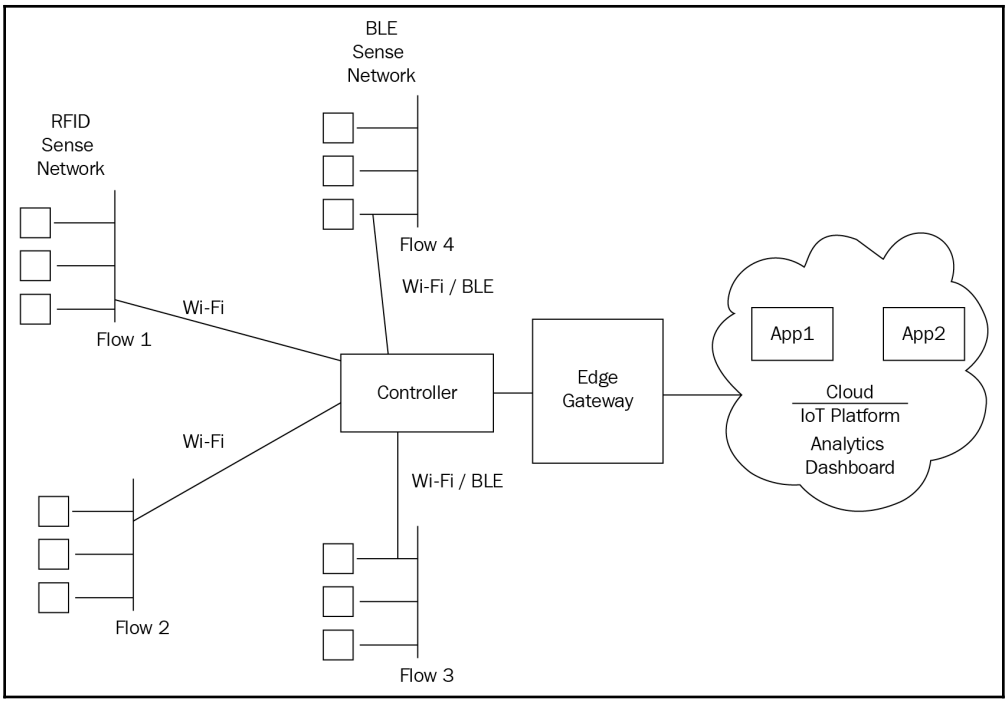


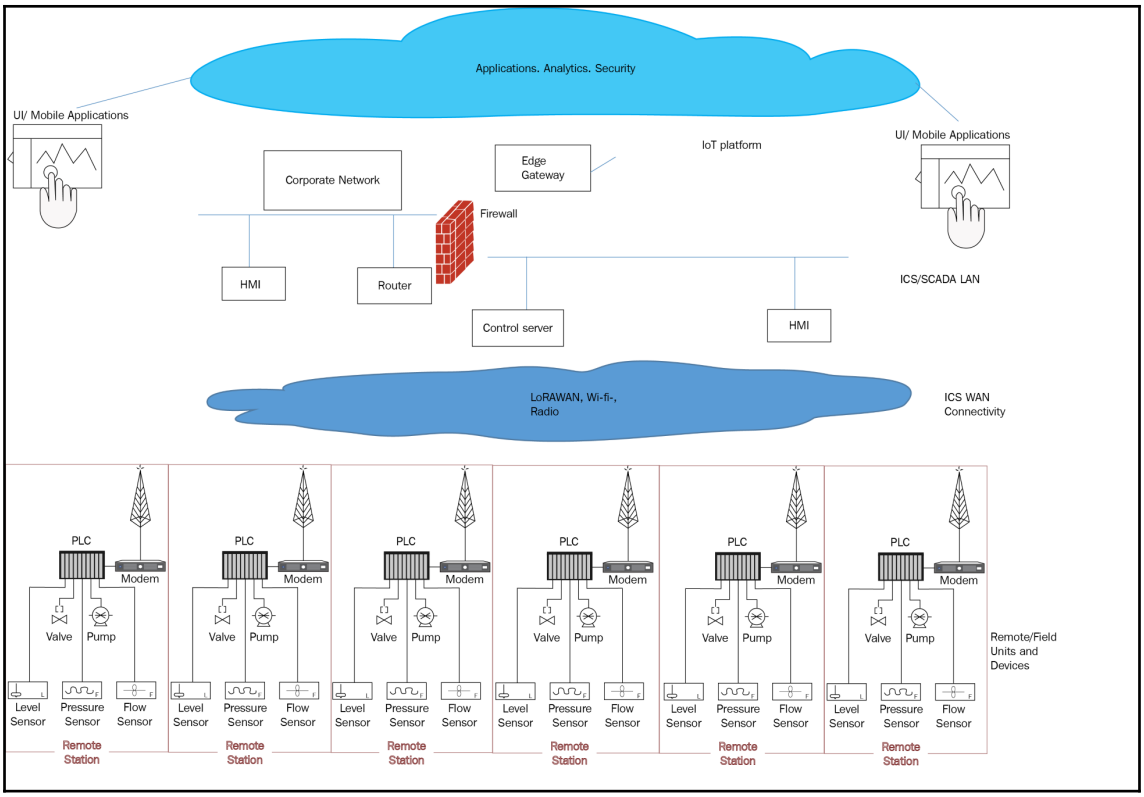

Human - Machine Interface (HMI)
Remote diagnostics and maintenance
Set points,
Control algorithms,
Parameter constraints,
Process data
Controller
Controlled variables
Manipulated variable
Actuators
Sensors
Process inputs
Controlled process
Process outputs
Disturbances

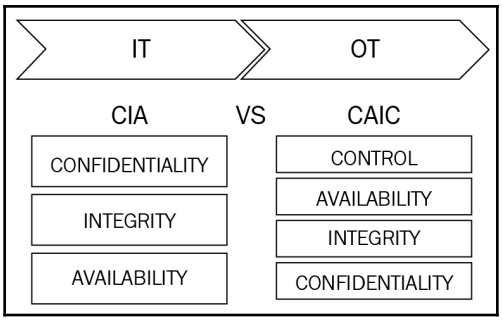

Computer Center
Level 4
Production Scheduling
Coordinating Computer
Coordinating Computer
Level 3
Production Control
Supervisory Computers
Supervisory Computers
Supervisory Computers
Supervisory Computers
Level 2
Plant Supervisory
µC
µC
µC
µC
µC
µC
µC
µC
Level 1
Direct Control
Plant
Plant
Level 0
Field Level

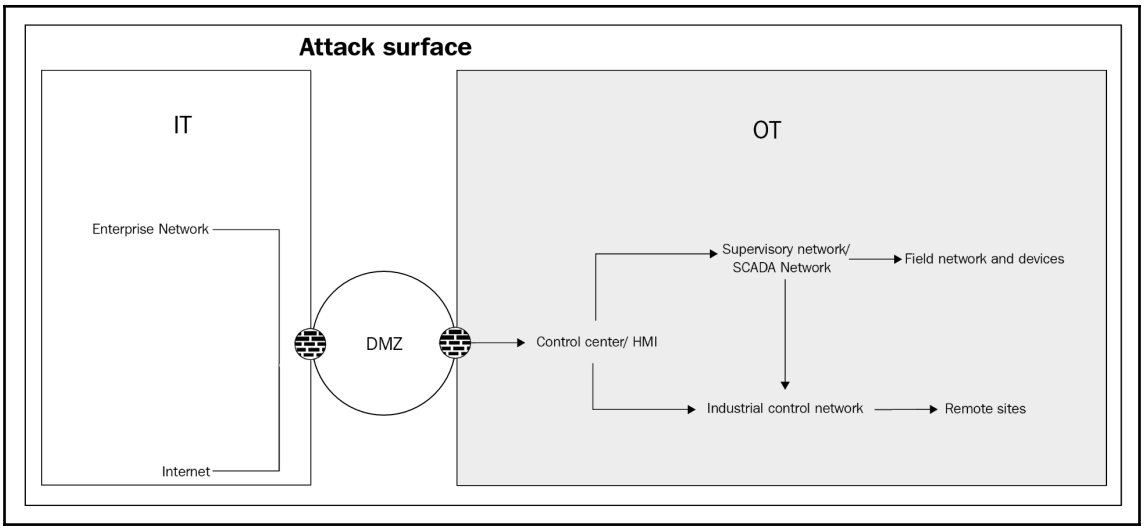

Control Center
Engineering Workstations
HMI
Data Historian
Control Server (SCADA - MTU)
Communications Routers
Switched Telephone, Leased Line or Power Line Based Communications
Radio Microwave or Cellular
Satellite
Wide Area Network
Field Site 1
Modem
PLC
Field Site 2
WAN CARD
IED
Field Site 3
Modem
RTU

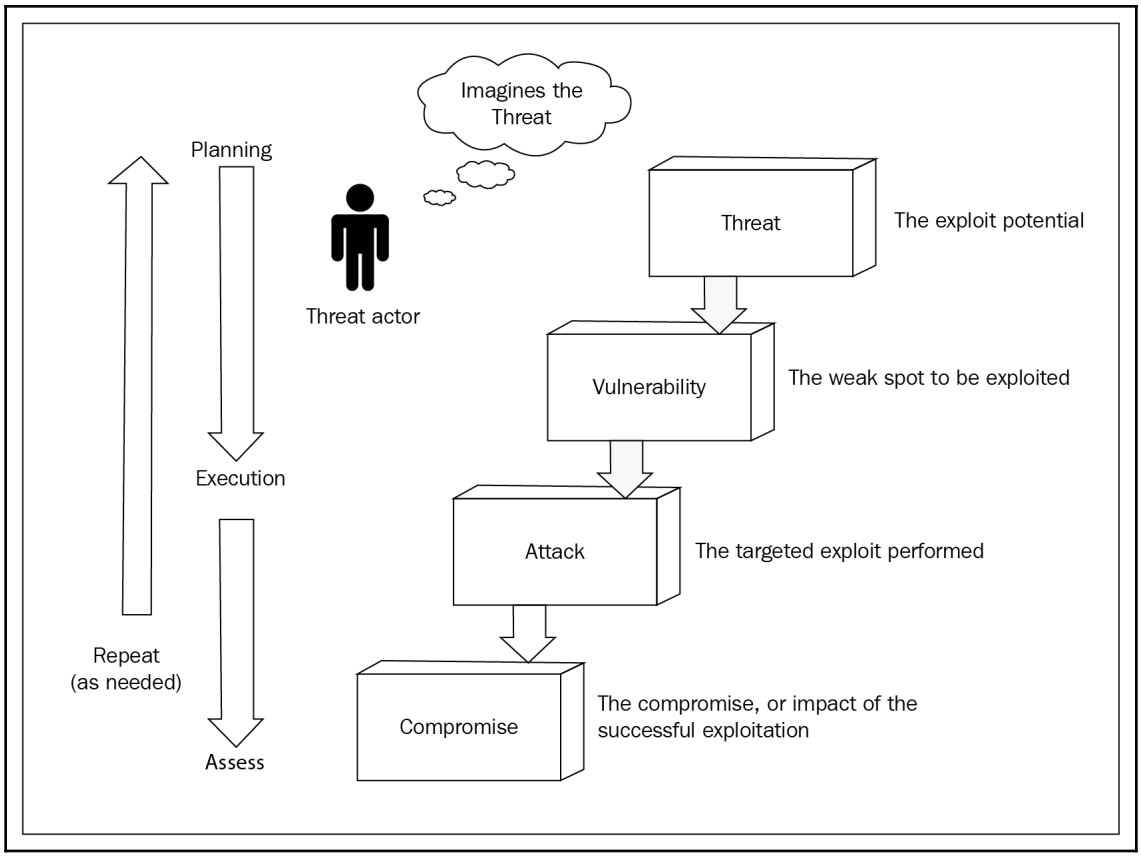

Regional Control Center
Control Server SCADA-MTU
Backup Control Center
Primary Control Center
Data Historian
HMI Station
Engineering Workstations
Modem
Control Server (SCADA-MTU)
Printer
WAN
Corporate Enterprise Network
HMI Station
Serial Direct Radio Communication
PLC
Modem
Valve
Pump
Level Sensor
Pressure Sensor
Flow Sensor
Remote Station
Remote Access
Modem
Computer
Remote Station
Valve
Pump
Level Sensor
Pressure Sensor
Flow Sensor
Remote Station

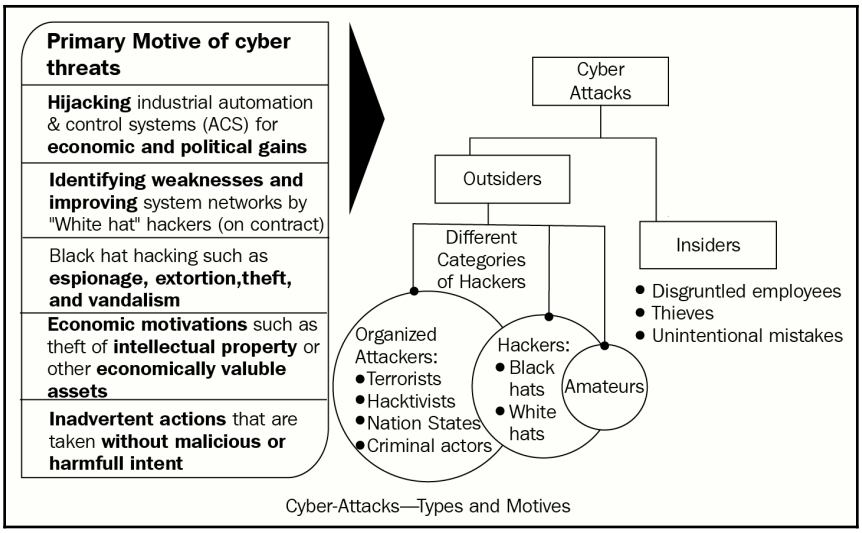

BLE
Sense
Network
RFID
Sense
Network
Flow 4
Wi-Fi / BLE
Wi-Fi
Flow 1
Controller
Edge
Gateway
App1
App2
Cloud
IoT Platform
Analytics
Dashboard
Wi-Fi
Wi-Fi / BLE
Flow 2
Flow 3


Applications. Analytics. Security
UI/ Mobile Applications
IoT platform
UI/ Mobile Applications
Corporate Network
Edge Gateway
Firewall
HMI
Router
Control server
HMI
ICS/SCADA LAN
LoRAWAN, Wi-fi-, Radio
ICS WAN Connectivity
PLC
Modem
Valve
Pump
Level Sensor
Pressure Sensor
Flow Sensor
Remote Station
Remote/Field Units and Devices

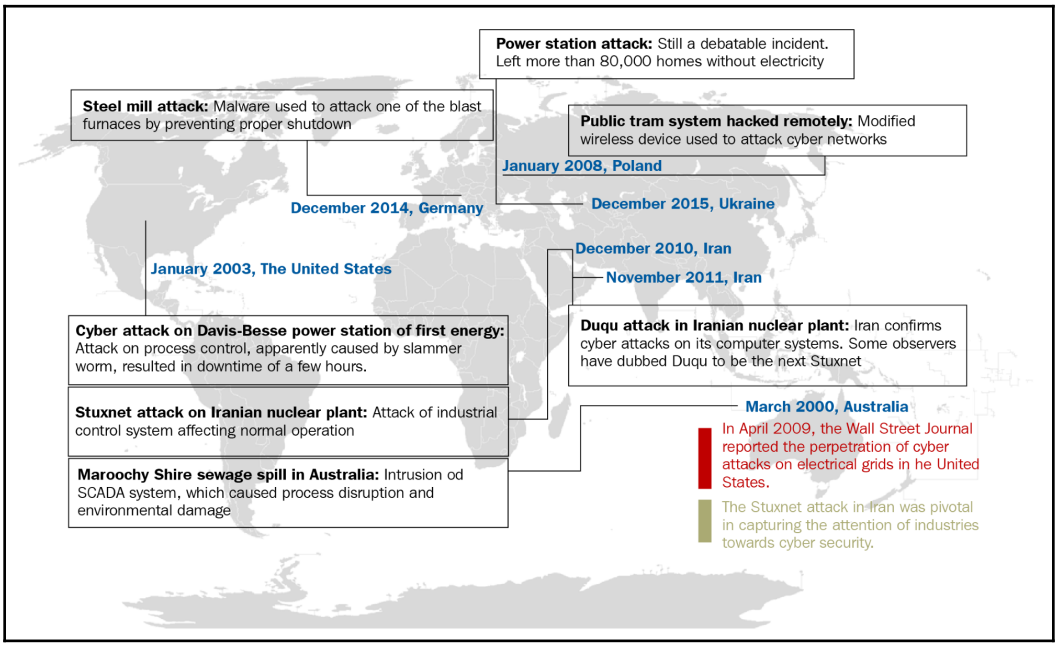

IT
OT
CIA
VS
CAIC
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
CONTROL
AVAILABILITY
INTEGRITY
CONFIDENTIALITY


Attack surface
IT
OT
Enterprise Network
Internet
DMZ
Control center/ HMI
Supervisory network/
SCADA Network
Field network and devices
Industrial control network
Remote sites

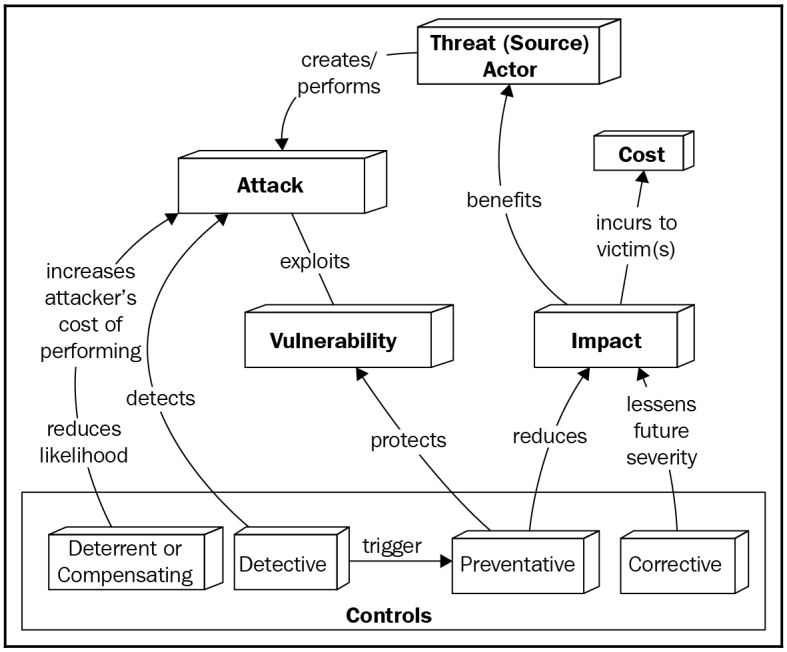

Imagines the Threat
Planning
Threat actor
Threat
The exploit potential
Vulnerability
The weak spot to be exploited
Execution
Attack
The targeted exploit performed
Repeat (as needed)
Compromise
The compromise, or impact of the successful exploitation
Assess

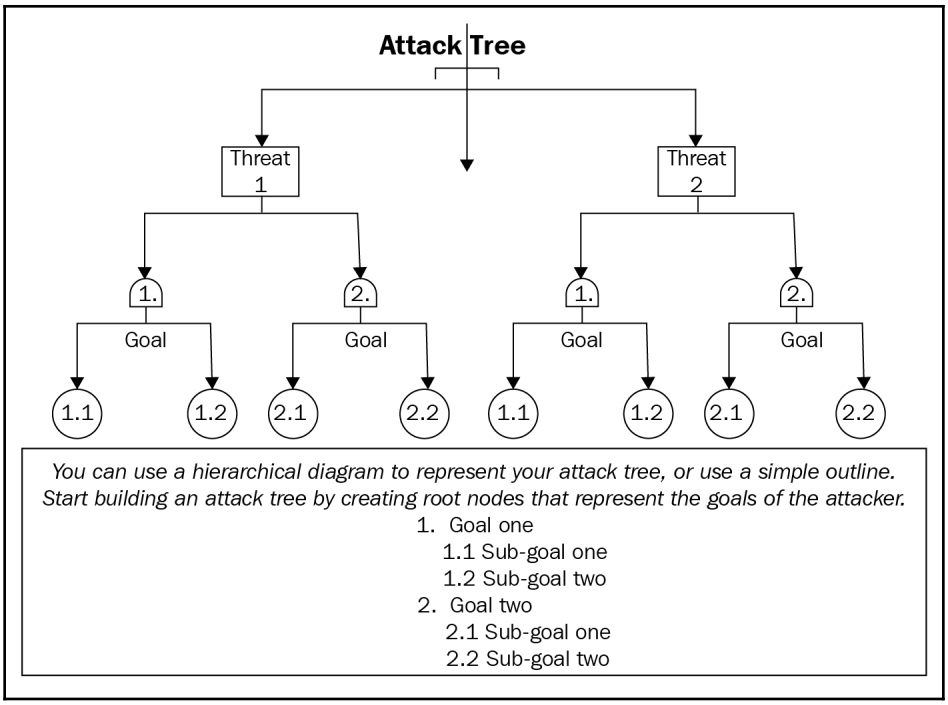


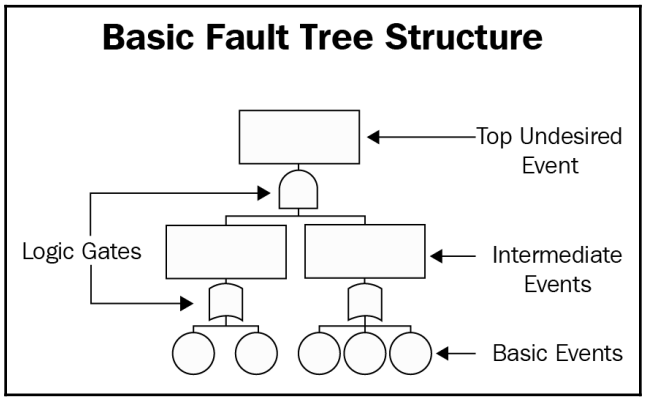
Cyber-Attacks—Types and Motives

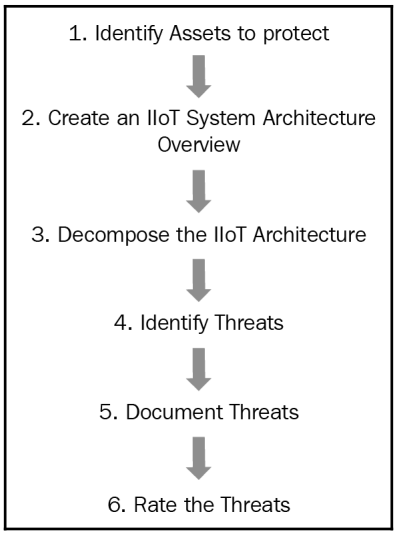


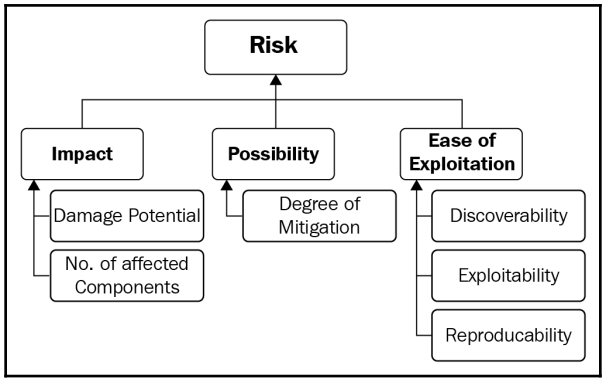
Chapter 02: Industrial IoT Dataflow and Security Architecture




Attack Tree
Threat 1
Threat 2
1.
2.
1.
2.
Goal
Goal
Goal
Goal
1.1
1.2
2.1
2.2
1.1
1.2
2.1
2.2
You can use a hierarchical diagram to represent your attack tree, or use a simple outline.
Start building an attack tree by creating root nodes that represent the goals of the attacker.
1. Goal one
1.1 Sub-goal one
1.2 Sub-goal two
2. Goal two
2.1 Sub-goal one
2.2 Sub-goal two


Basic Fault Tree Structure
Top Undesired Event
Logic Gates
Intermediate Events
Basic Events


1. Identify Assets to protect
2. Create an IIoT System Architecture Overview
3. Decompose the IIoT Architecture
4. Identify Threats
5. Document Threats
6. Rate the Threats


Risk
Impact
Possibility
Ease of Exploitation
Damage Potential
No. of affected Components
Degree of Mitigation
Discoverability
Exploitability
Reproducability

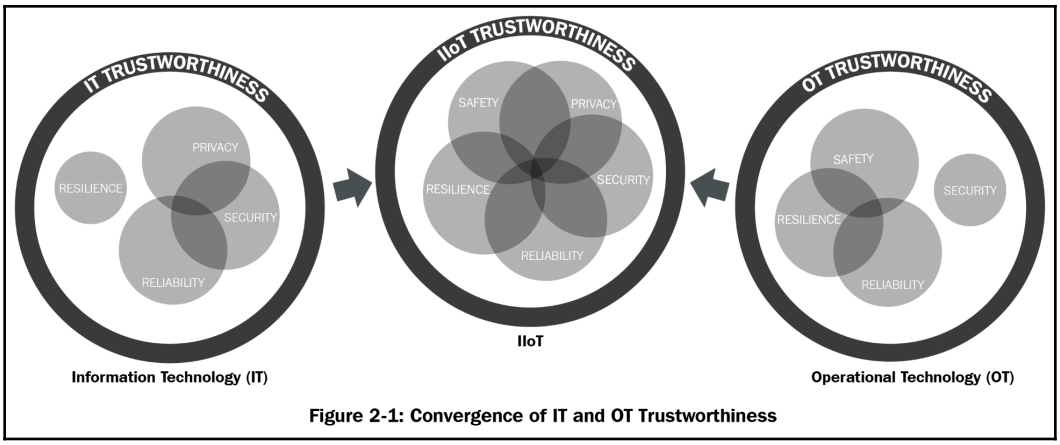
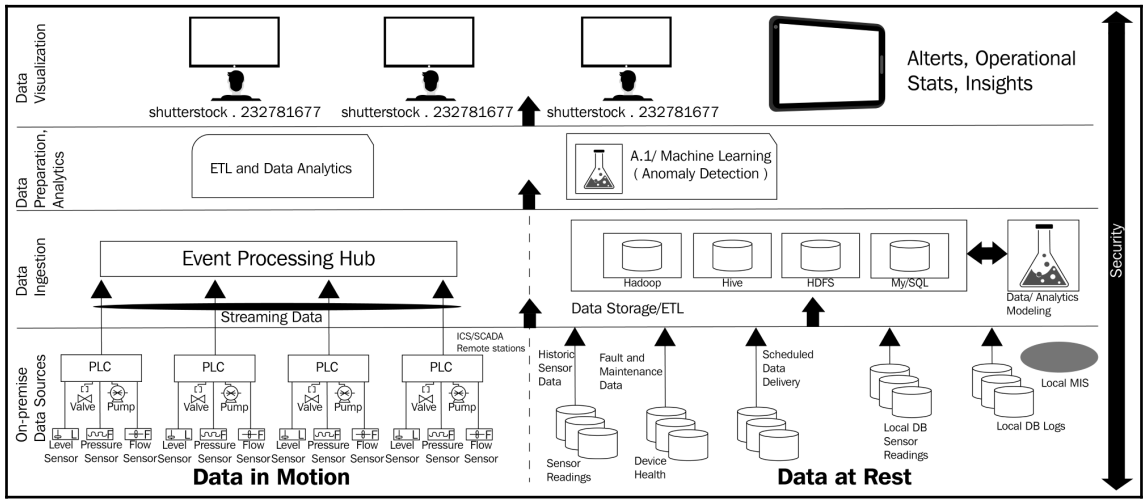
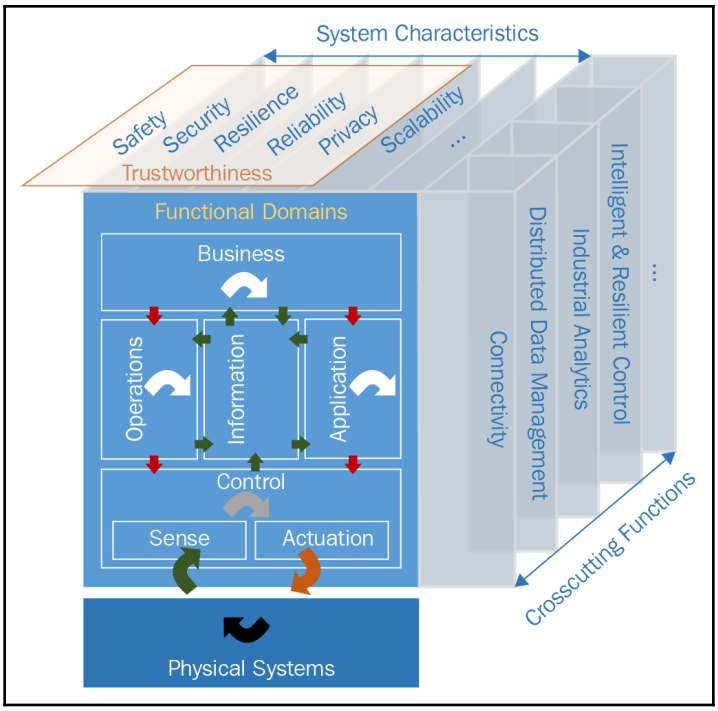
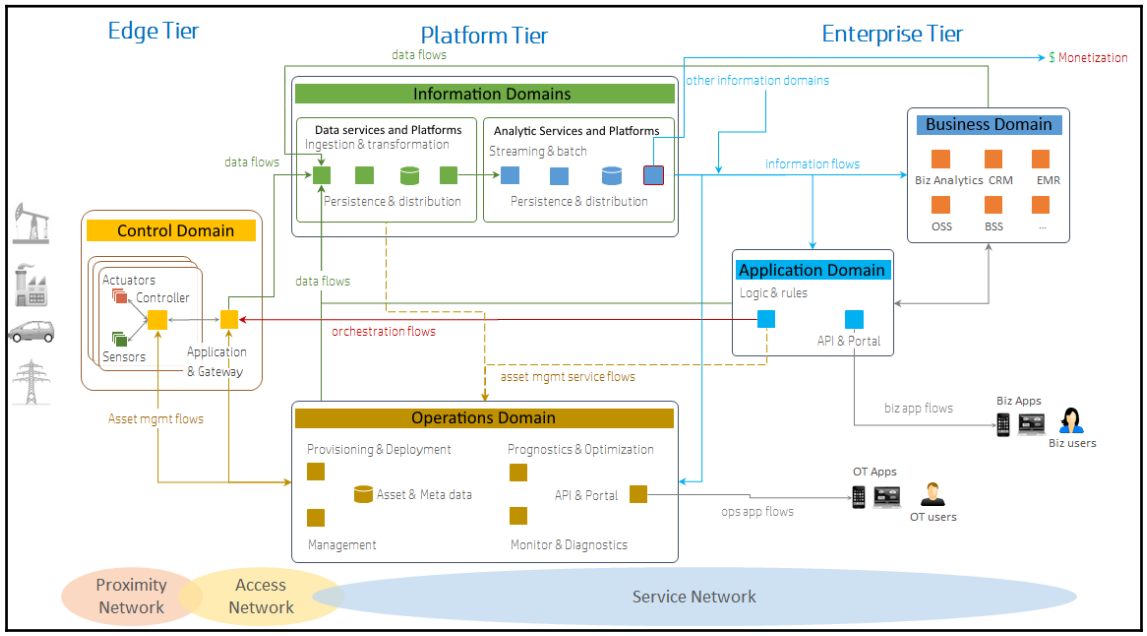
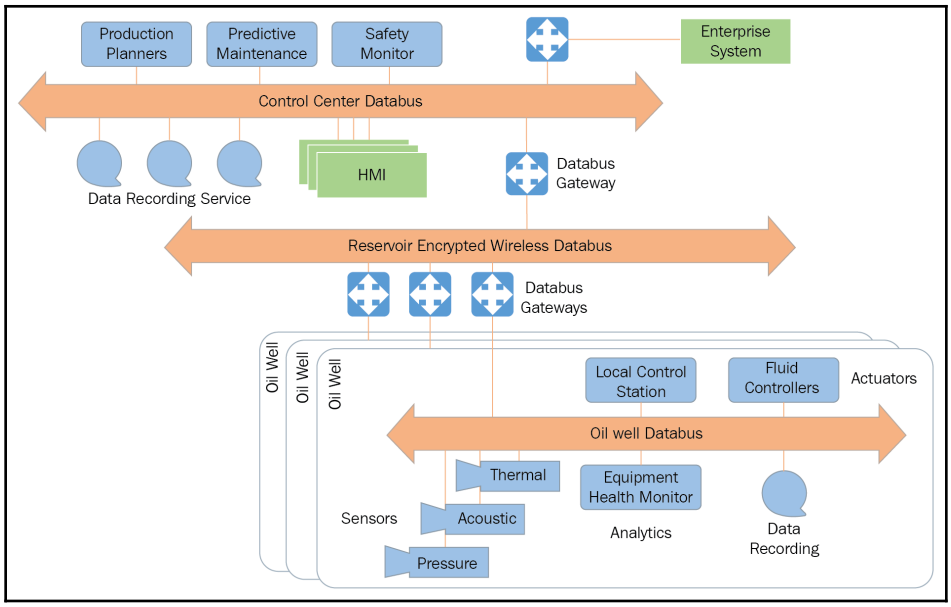


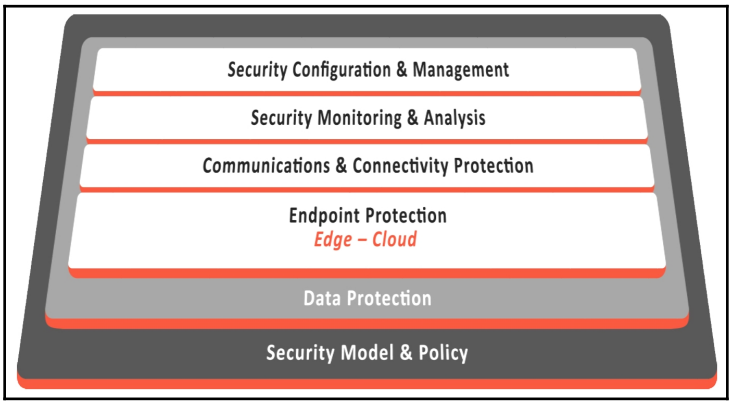
Figure 2-1: Convergence of IT and OT Trustworthiness

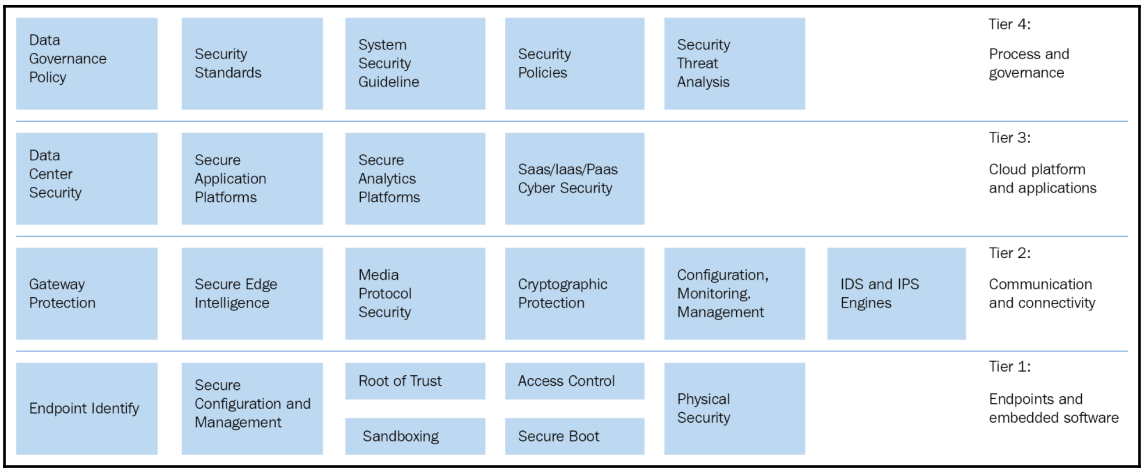



System Characteristics
Safety
Security
Resilience
Reliability
Privacy
Scalability
...
Trustworthiness
Functional Domains
Business
Operations
Information
Application
Control
Sense
Actuation
Physical Systems
Connectivity
Distributed Data Management
Industrial Analytics
Intelligent & Resilient Control
...
Crosscutting Functions

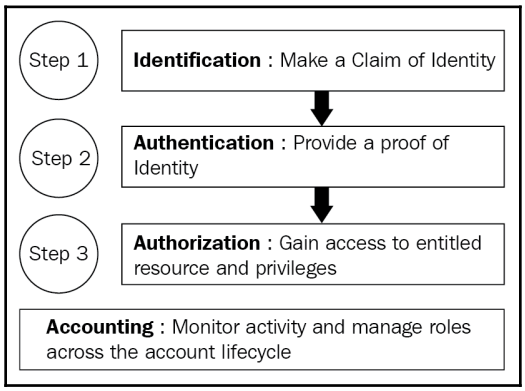

Edge Tier
Platform Tier
Enterprise Tier
data flows
$ Monetization
Information Domains
other information domains
Data services and Platforms
Ingestion & transformation
Analytic Services and Platforms
Streaming & batch
Persistence & distribution
Persistence & distribution
Business Domain
Biz Analytics
CRM
EMR
OSS
BSS
...
information flows
Control Domain
Actuators
Controller
Sensors
Application & Gateway
Application Domain
Logic & rules
API & Portal
orchestration flows
asset mgmt service flows
Asset mgmt flows
Operations Domain
Provisioning & Deployment
Prognostics & Optimization
Asset & Meta data
API & Portal
Management
Monitor & Diagnostics
biz app flows
Biz Apps
Biz users
OT Apps
OT users
ops app flows
Proximity Network
Access Network
Service Network

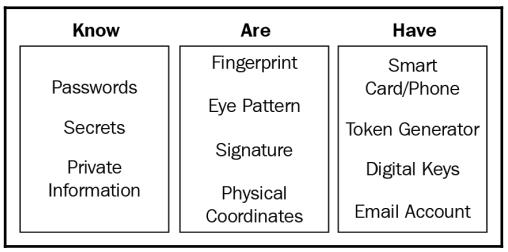

Production Planners
Predictive Maintenance
Safety Monitor
Enterprise System
Control Center Databus
Data Recording Service
HMI
Databus Gateway
Reservoir Encrypted Wireless Databus
Databus Gateways
Oil Well
Oil Well
Oil Well
Local Control Station
Fluid Controllers
Actuators
Oil well Databus
Thermal
Equipment Health Monitor
Sensors
Acoustic
Analytics
Data Recording
Pressure

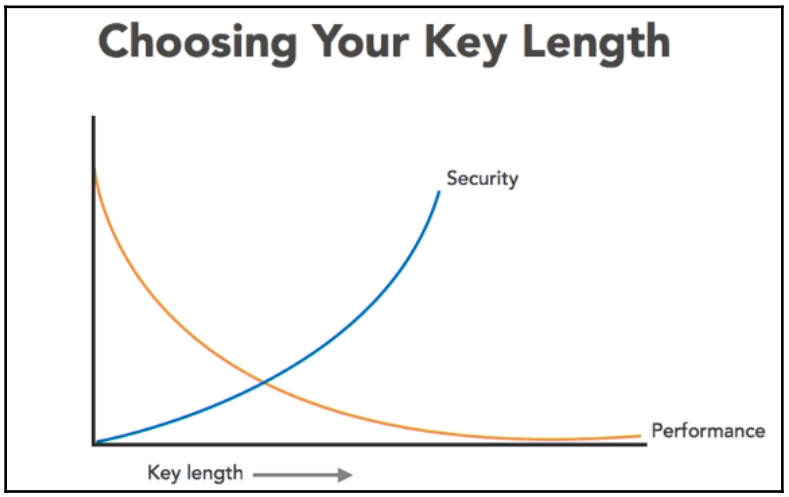

Security Configuration & Management
Security Monitoring & Analysis
Communications & Connectivity Protection
Endpoint Protection
Edge – Cloud
Data Protection
Security Model & Policy

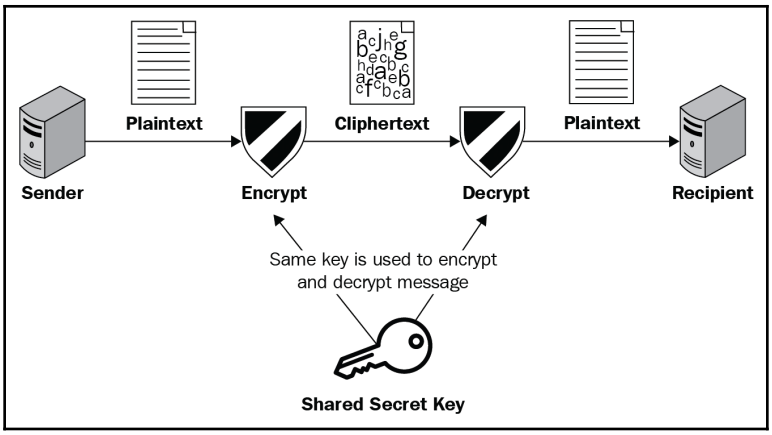

Data Governance Policy
Security Standards
System Security Guideline
Security Policies
Security Threat Analysis
Tier 4:
Process and governance
Data Center Security
Secure Application Platforms
Secure Analytics Platforms
Saas/Iaas/Paas Cyber Security
Tier 3:
Cloud platform and applications
Gateway Protection
Secure Edge Intelligence
Media Protocol Security
Cryptographic Protection
Configuration, Monitoring. Management
IDS and IPS Engines
Tier 2:
Communication and connectivity
Endpoint Identify
Secure Configuration and Management
Root of Trust
Sandboxing
Access Control
Secure Boot
Physical Security
Tier 1:
Endpoints and embedded software

Chapter 03: IIoT Identity and Access Management

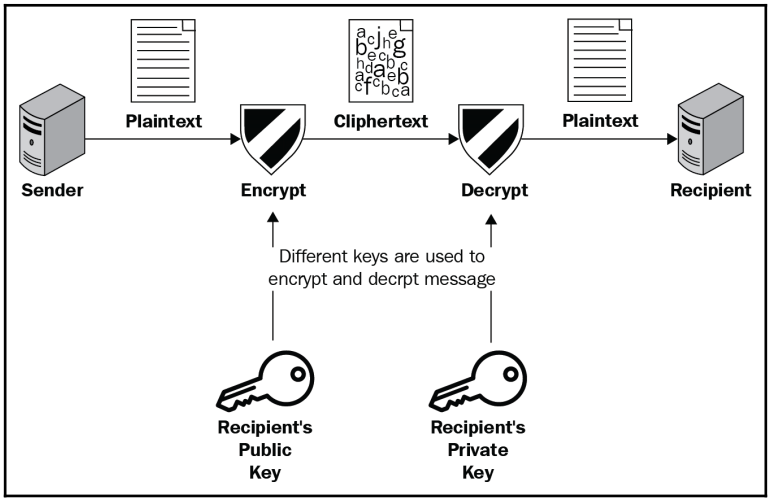


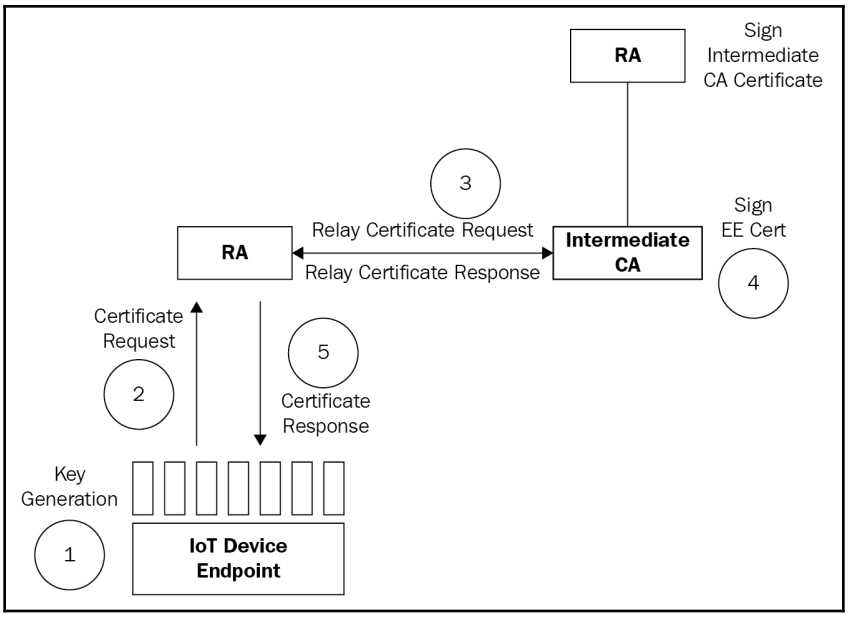


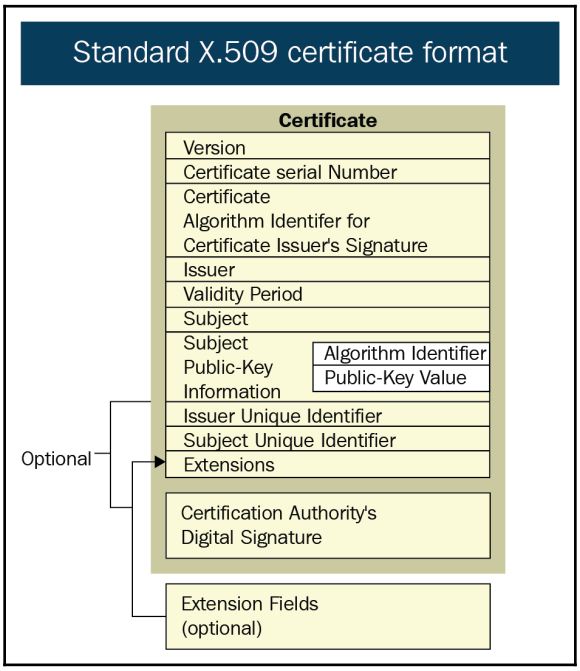


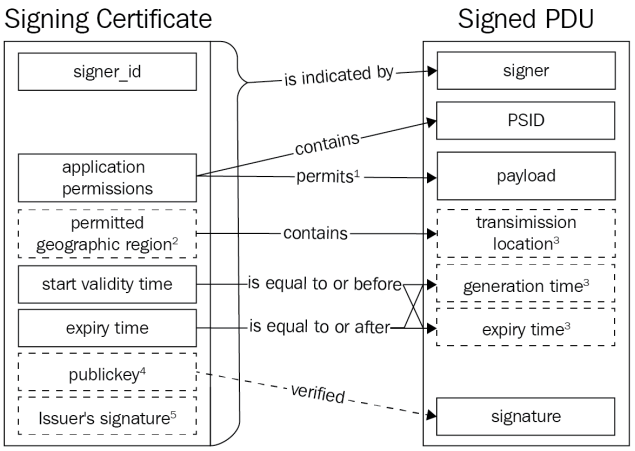


Group Size	Symmetric Keys
2	1
3	3
10	45
100	4950
1,000	499,500
10,000	49,995,000

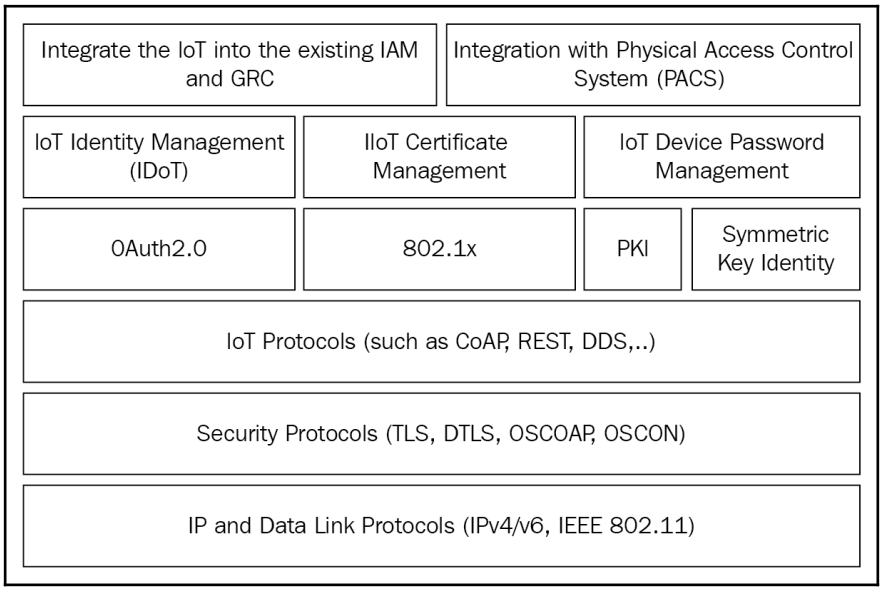



RA
Sign
Intermediate
CA Certificate
3
Relay Certificate Request
RA
Intermediate
CA
Relay Certificate Response
Sign
EE Cert
4
Certificate
Request
2
5
Certificate
Response
Key
Generation
1
IoT Device
Endpoint


Standard X.509 certificate format
Certificate
Version
Certificate serial Number
Certificate
Algorithm Identifer for
Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject
Public-Key
Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's
Digital Signature
Extension Fields
(optional)

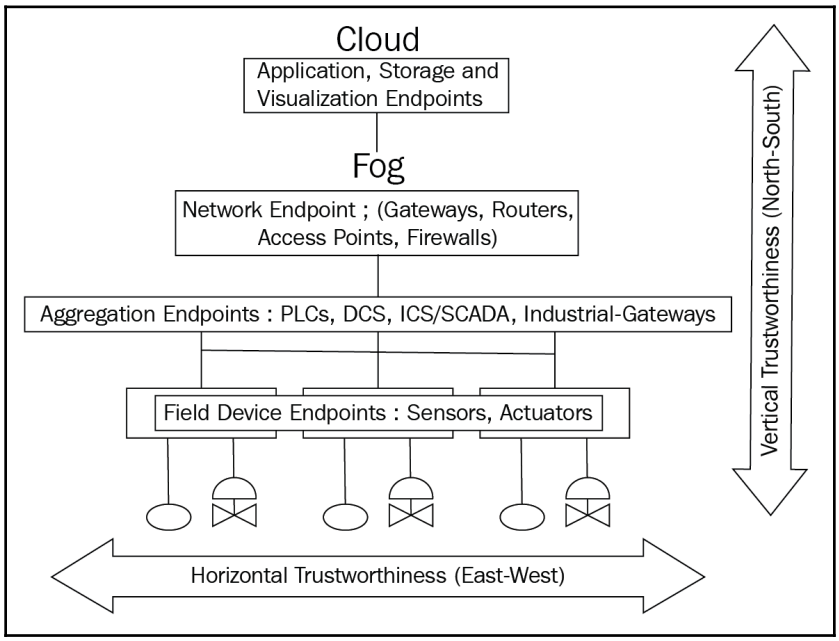


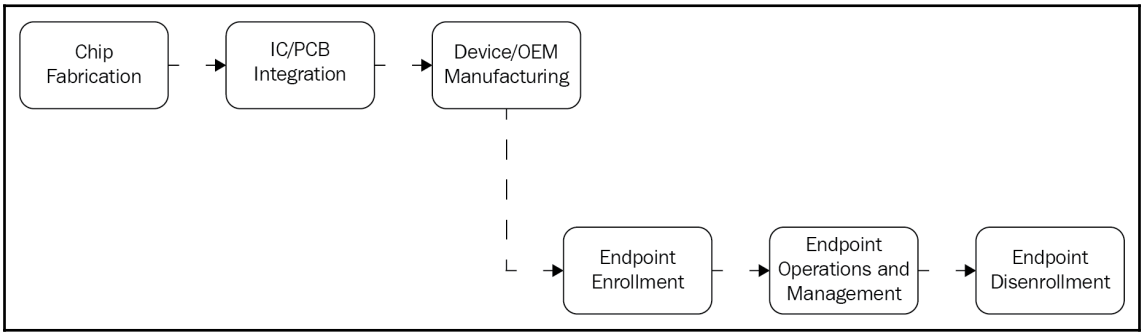
NOTES :
1. Determined using the PSIP and SSP. The process to determine whether the operational permissions permit the message payload is specified by the organization reserving the PSID and is out of scope for this standard.
2. Included per policy set by the appropriate authority for the region where the certificate is being used.
3. Optional. Inclusion od this data is as determined by the organization reserving the PSID. This data may be contained in the payload or within the security header fields.
4. For implicit certificates, the public key is derived rather than explicity stated within the certificate.
5. Not included in a implicit certificate.

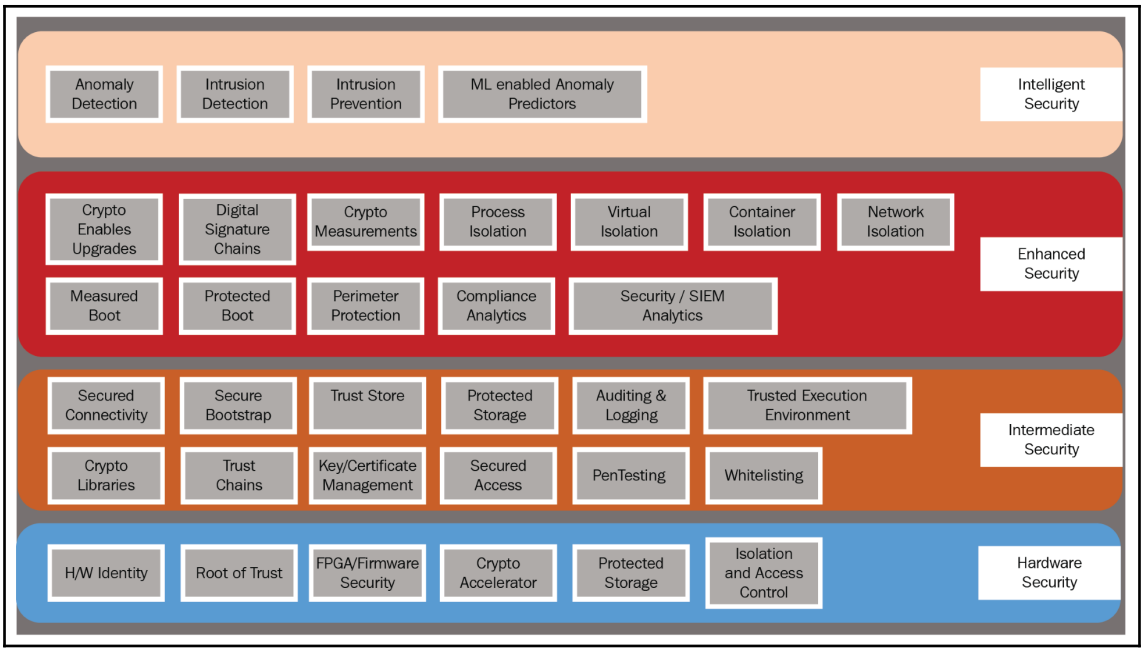


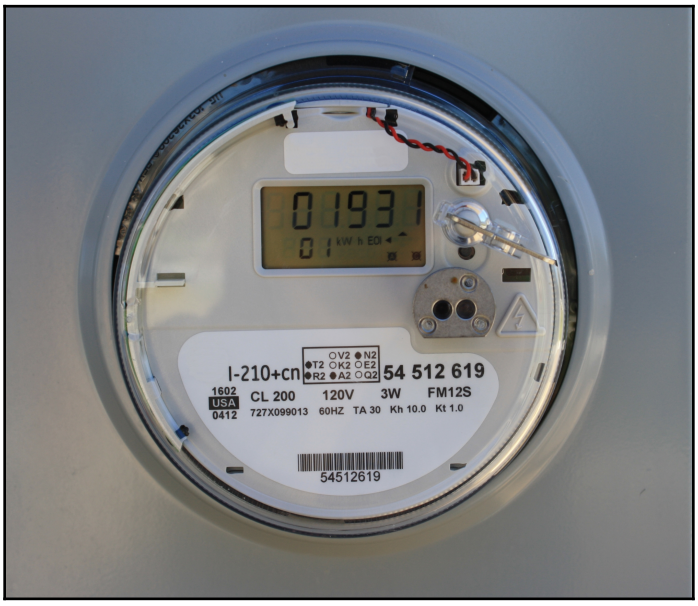
Capability	Yes/No; OR Assign Value
Confidentiality Authorized Access Only	
Integrity No Unauthorized Changes	
Authentication Proof of identity claims	
Nonrepudiation Verifiable Originator/Actor	
Cost/Key Crypto price performance	
Energy Consumption Battery/Power performance	
Memory Runtime memory consumption	
Processor Requirement CPU/Processor performance	

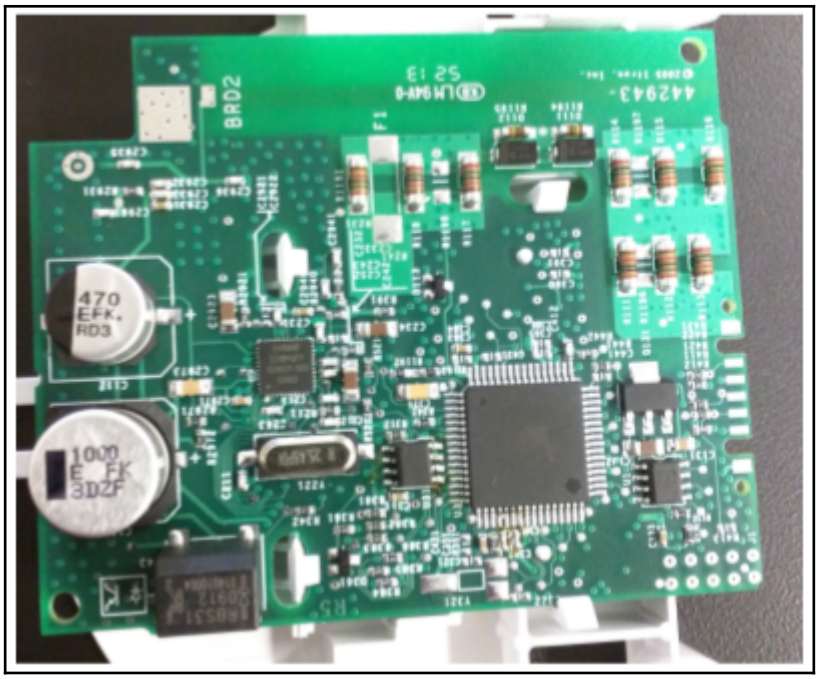
Chapter 04: Endpoint Security and Trustworthiness

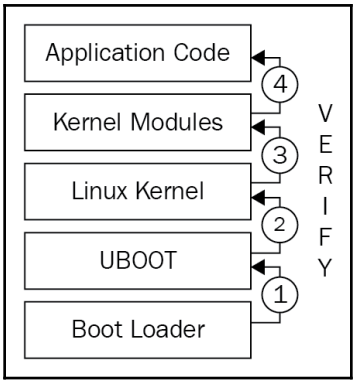


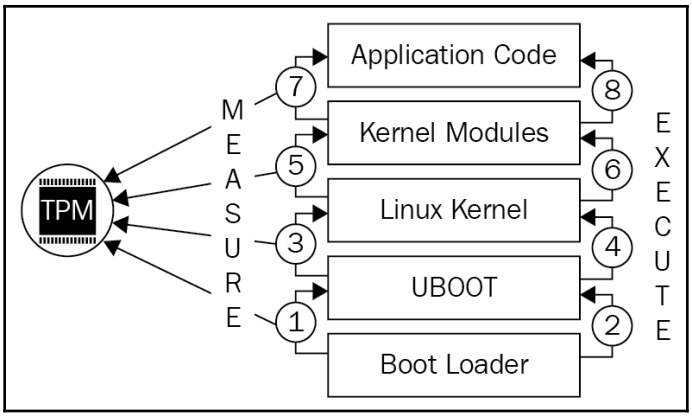


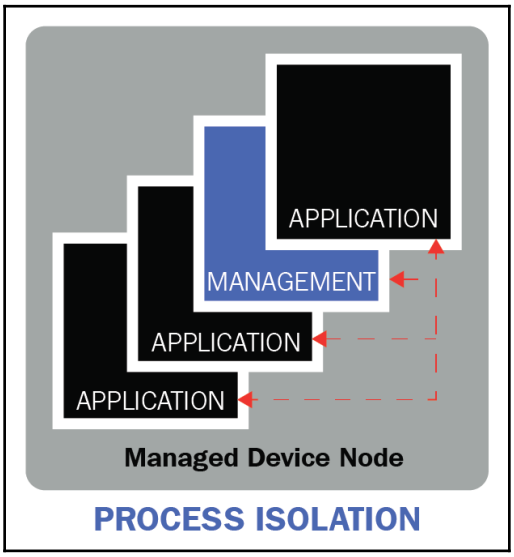

Anomaly Detection
Intrusion Detection
Intrusion Prevention
ML enabled Anomaly Predictors
Intelligent Security
Crypto Enables Upgrades
Digital Signature Chains
Crypto Measurements
Process Isolation
Virtual Isolation
Container Isolation
Network Isolation
Measured Boot
Protected Boot
Perimeter Protection
Compliance Analytics
Security / SIEM Analytics
Enhanced Security
Secured Connectivity
Secure Bootstrap
Trust Store
Protected Storage
Auditing & Logging
Trusted Execution Environment
Crypto Libraries
Trust Chains
Key/Certificate Management
Secured Access
PenTesting
Whitelisting
Intermediate Security
H/W Identity
Root of Trust
FPGA/Firmware Security
Crypto Accelerator
Protected Storage
Isolation and Access Control
Hardware Security

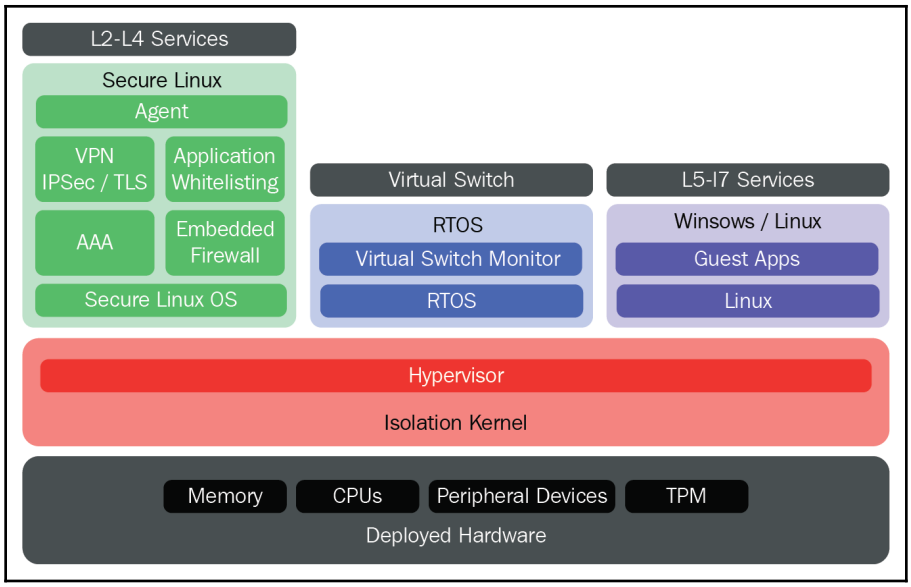

01931
I-210+cn
54 512 619
CL 200
120V
3W
FM12S
54512619




Application Code
Kernel Modules
Linux Kernel
UBOOT
Boot Loader
4
3
2
1
VERIFY

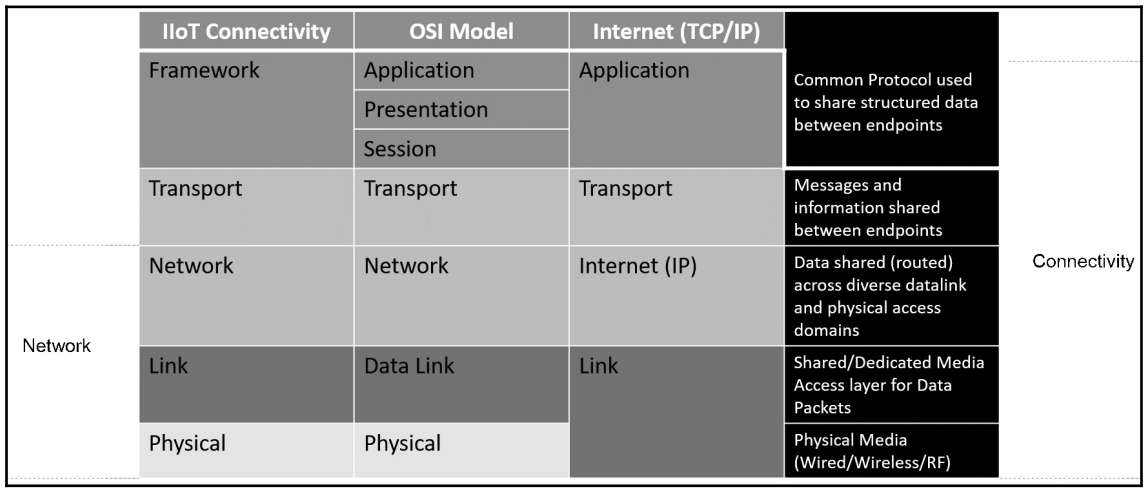

Application Code
Kernel Modules
Linux Kernel
UBOOT
Boot Loader
TPM
MEASURE
EXECUTE
1
2
3
4
5
6
7
8

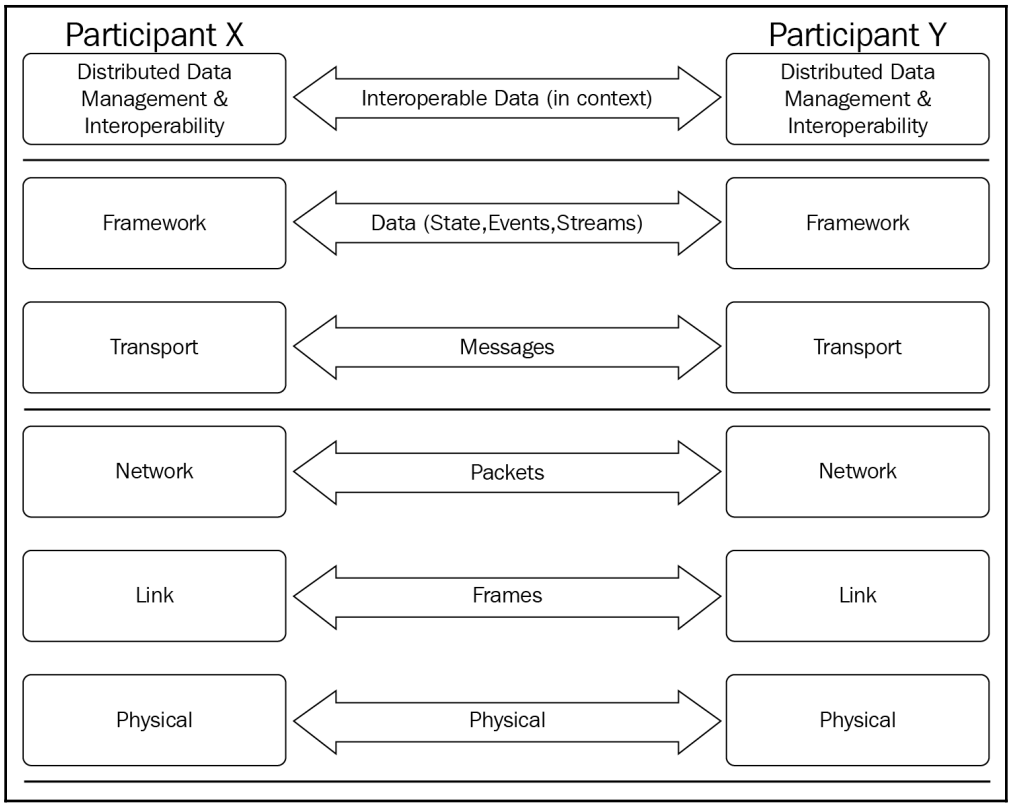

APPLICATION
MANAGEMENT
APPLICATION
APPLICATION
Managed Device Node
PROCESS ISOLATION

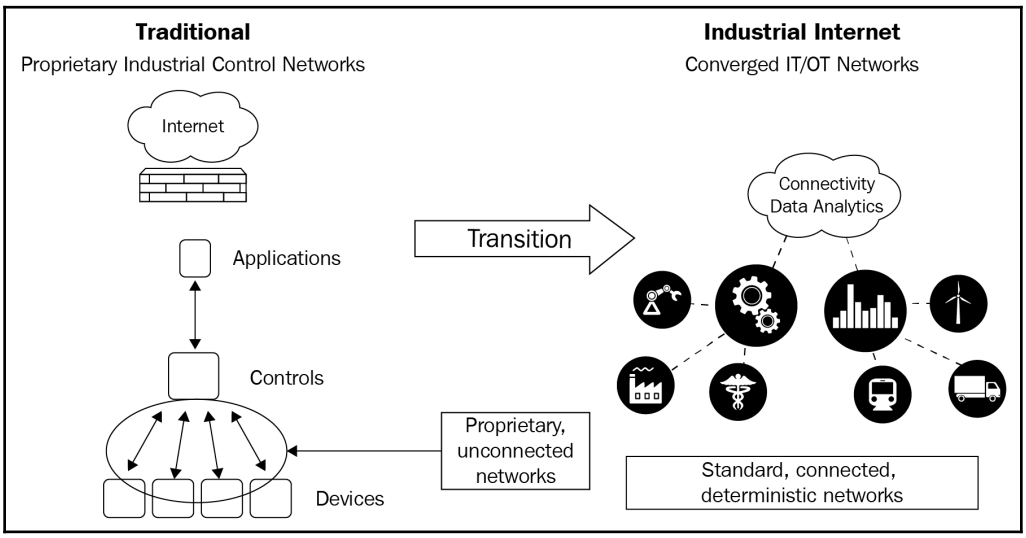


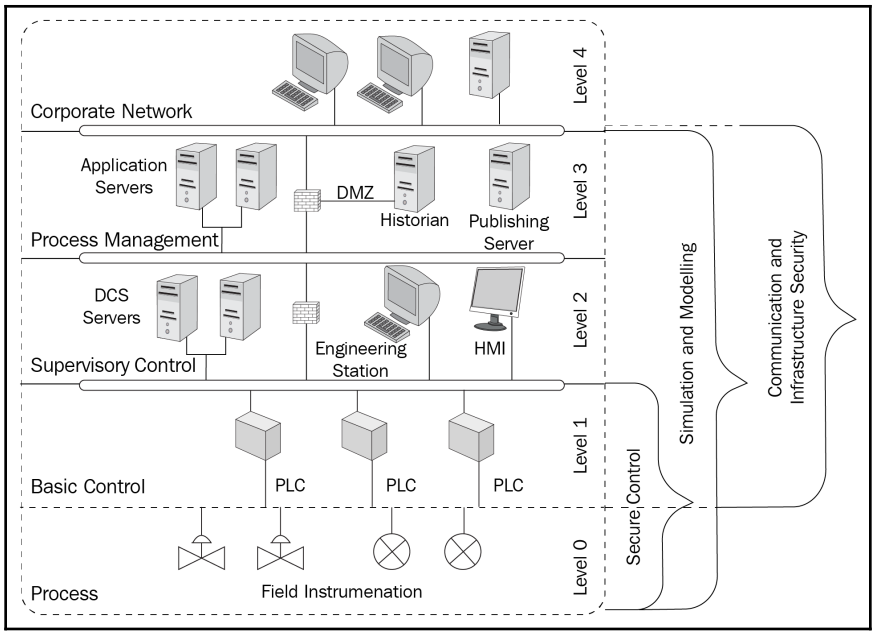
SECURITY CAPABILITY	INDUSTRY STANDARD
BOOT PROCESS INTEGRITY MEASUREMENT	NIST SP 800-155
ICS CYBERSECURITY STANDARDS	IEC 62443
SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS	NIST SP 800-53
INDUSTRIAL INTERNET SECURITY FRAMEWORK	IIC:PUB:G4:V1.0:PB:20160926
INDUSTRIE 4.0 STANDARD	Industries 4.0
IIC ENDPOINT SECURITY BEST PRACTICES	IIC:WHT:IN17:V1.6.3:ID:20180129
COMMON WEAKNESS ENUMERATION	CWE
SPECIFICATION ON SOFTWARE TAGGING	ISO/IEC 197702

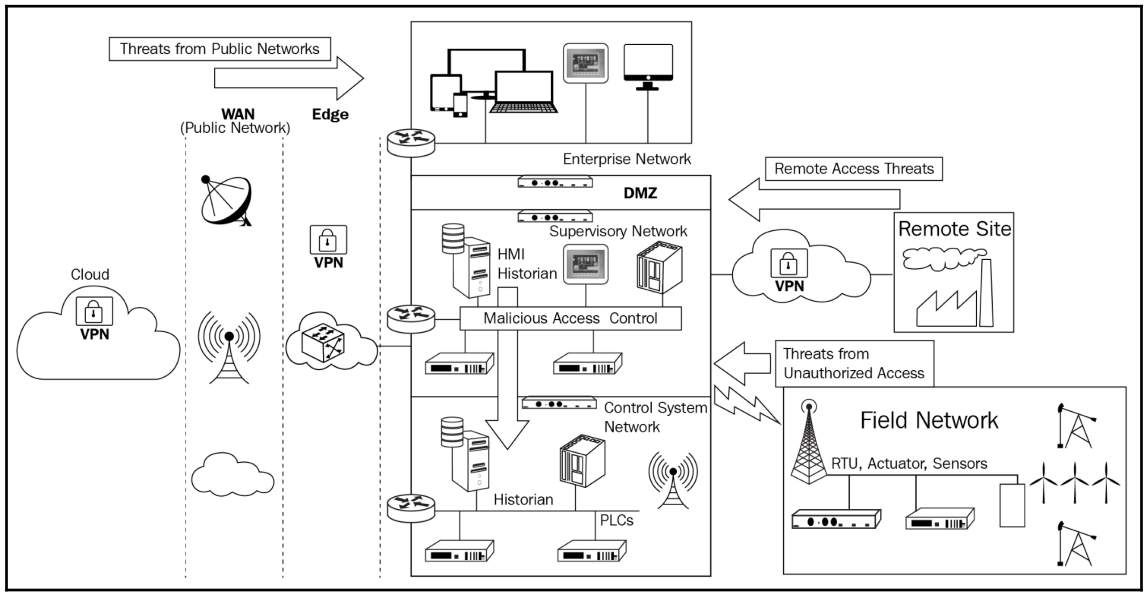
Chapter 05: Securing Connectivity and Communications

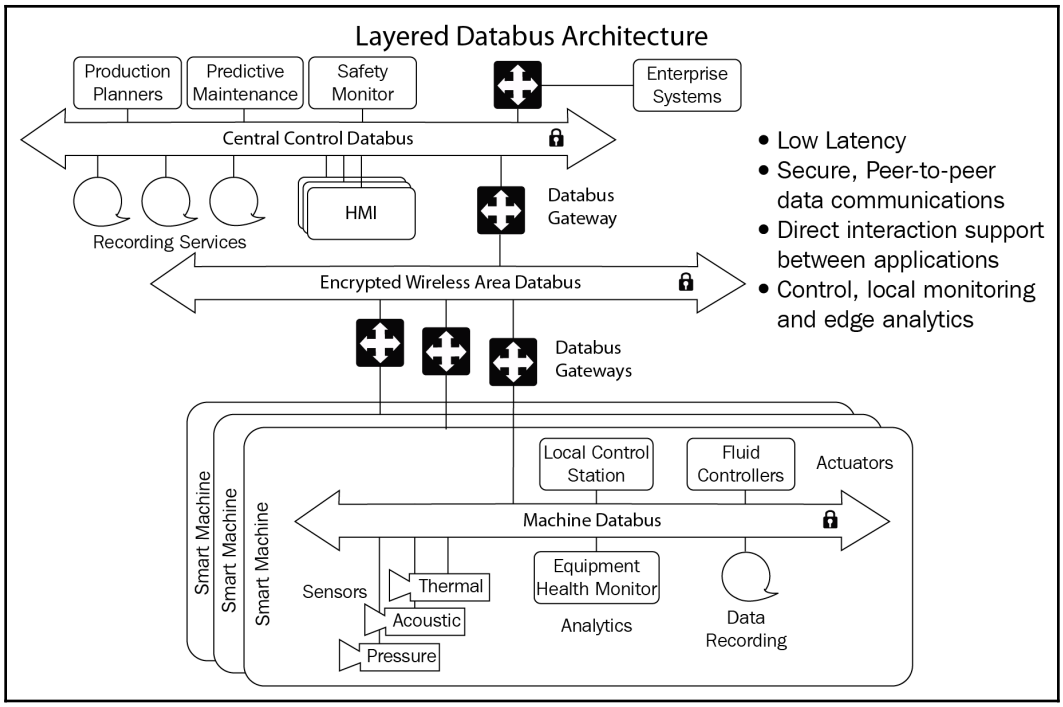


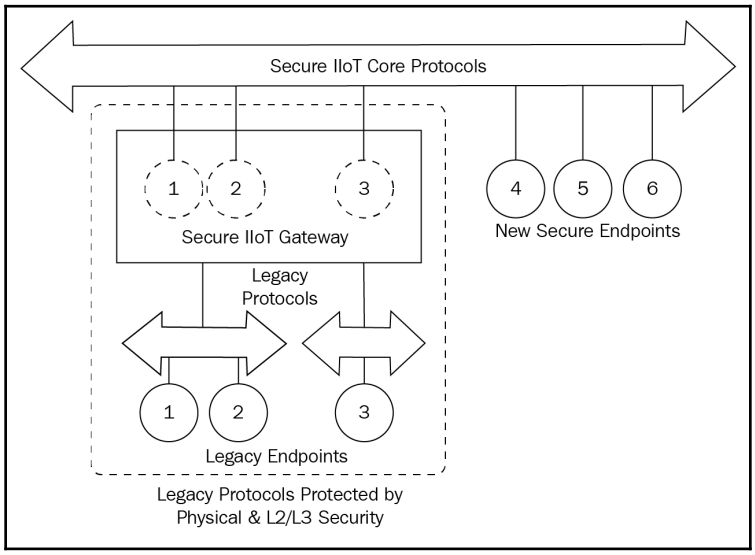

Participant X
Participant Y
Distributed Data Management & Interoperability
Interoperable Data (in context)
Distributed Data Management & Interoperability
Framework
Data (State,Events,Streams)
Framework
Transport
Messages
Transport
Network
Packets
Network
Link
Frames
Link
Physical
Physical
Physical

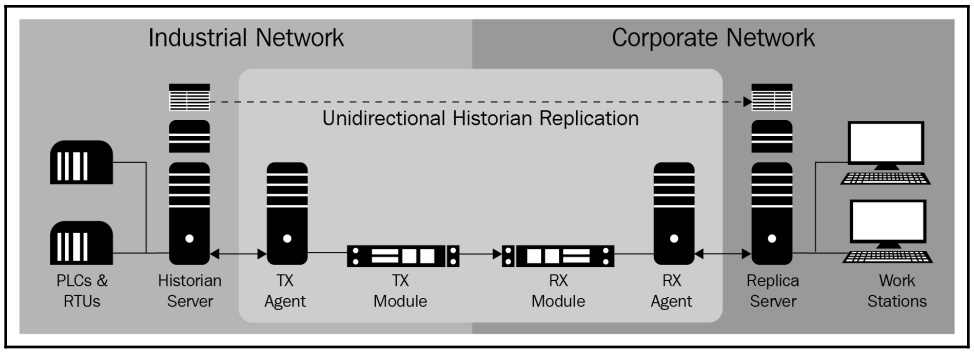

Traditional
Proprietary Industrial Control Networks
Industrial Internet
Converged IT/OT Networks
Internet
Applications
Controls
Devices
Transition
Connectivity
Data Analytics
Proprietary, unconnected networks
Standard, connected, deterministic networks

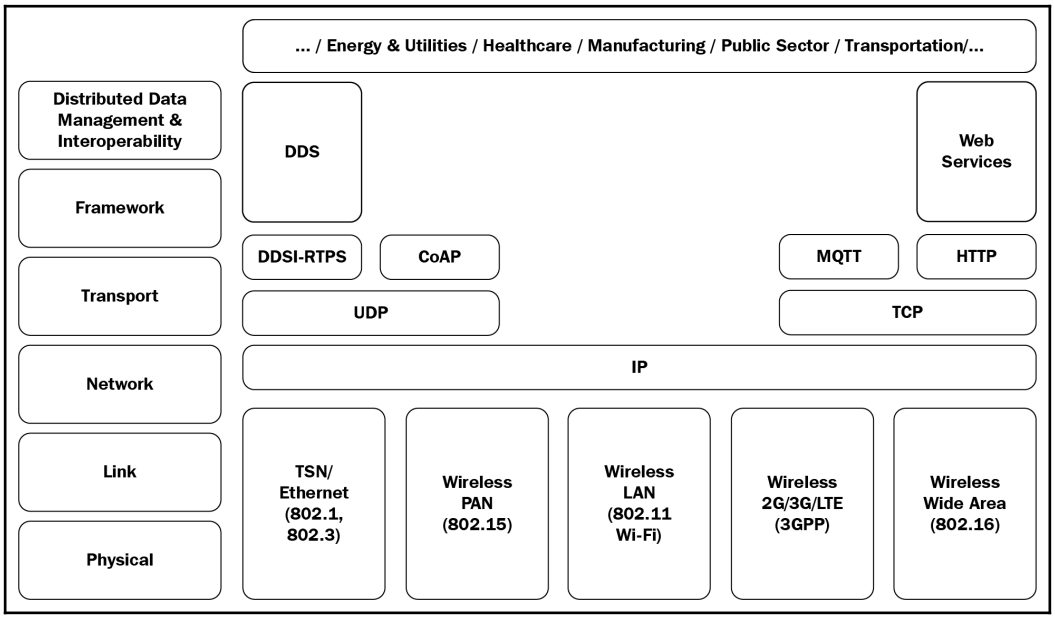

Corporate Network
Level 4
Application Servers
DMZ
Historian
Publishing Server
Process Management
Level 3
DCS Servers
Engineering Station
HMI
Supervisory Control
Level 2
Basic Control
PLC
PLC
PLC
Level 1
Process
Field Instrumenation
Level 0
Secure Control
Simulation and Modelling
Communication and Infrastructure Security


Threats from Public Networks
WAN
(Public Network)
Edge
Enterprise Network
Remote Access Threats
DMZ
Supervisory Network
HMI
Historian
Remote Site
VPN
Cloud
VPN
VPN
Malicious Access Control
Threats from Unauthorized Access
Control System Network
Field Network
RTU, Actuator, Sensors
Historian
PLCs


Layered Databus Architecture
Production Planners
Predictive Maintenance
Safety Monitor
Enterprise Systems
Central Control Databus
Recording Services
HMI
Databus Gateway
Encrypted Wireless Area Databus
Databus Gateways
• Low Latency
• Secure, Peer-to-peer data communications
• Direct interaction support between applications
• Control, local monitoring and edge analytics
Smart Machine
Smart Machine
Smart Machine
Local Control Station
Fluid Controllers
Actuators
Machine Databus
Sensors
Thermal
Acoustic
Pressure
Equipment Health Monitor
Analytics
Data Recording

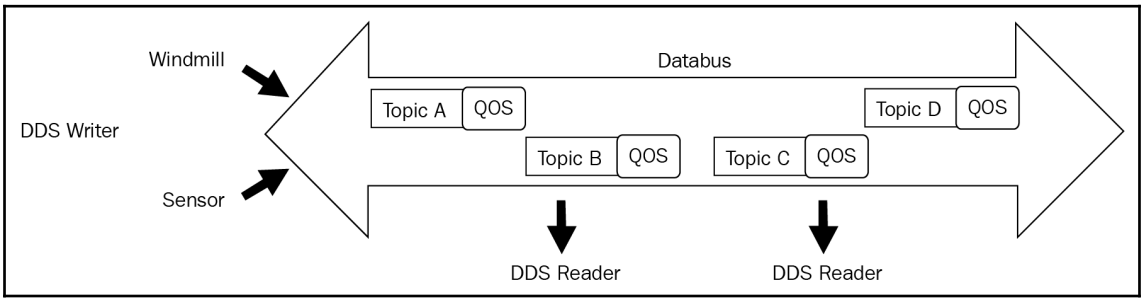

Secure IIoT Core Protocols
1
2
3
Secure IIoT Gateway
4
5
6
New Secure Endpoints
Legacy Protocols
1
2
3
Legacy Endpoints
Legacy Protocols Protected by Physical & L2/L3 Security

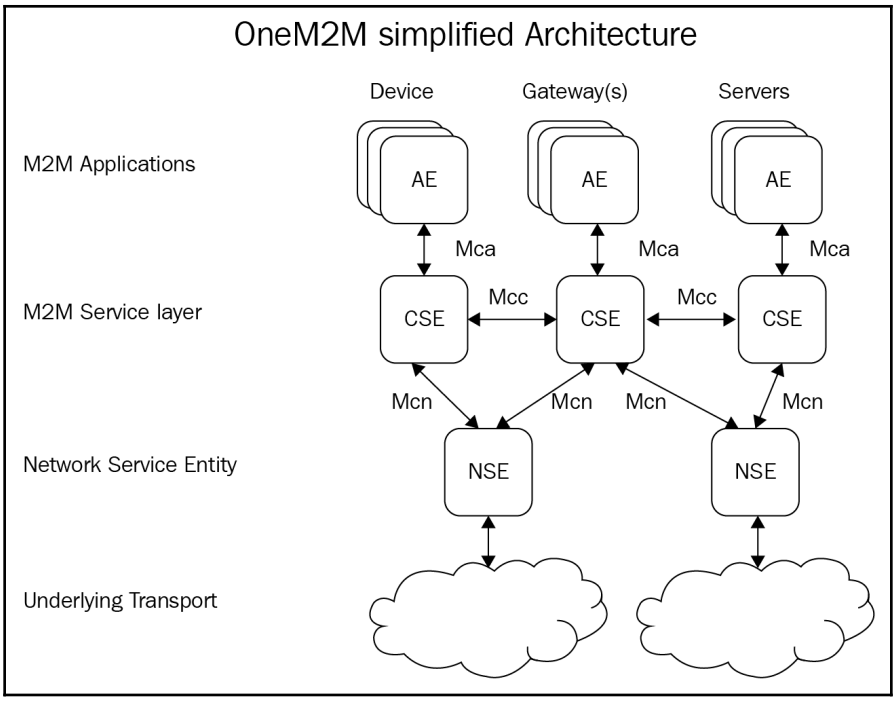

Industrial Network
Corporate Network
Unidirectional Historian Replication
PLCs & RTUs
Historian Server
TX Agent
TX Module
RX Module
RX Agent
Replica Server
Work Stations

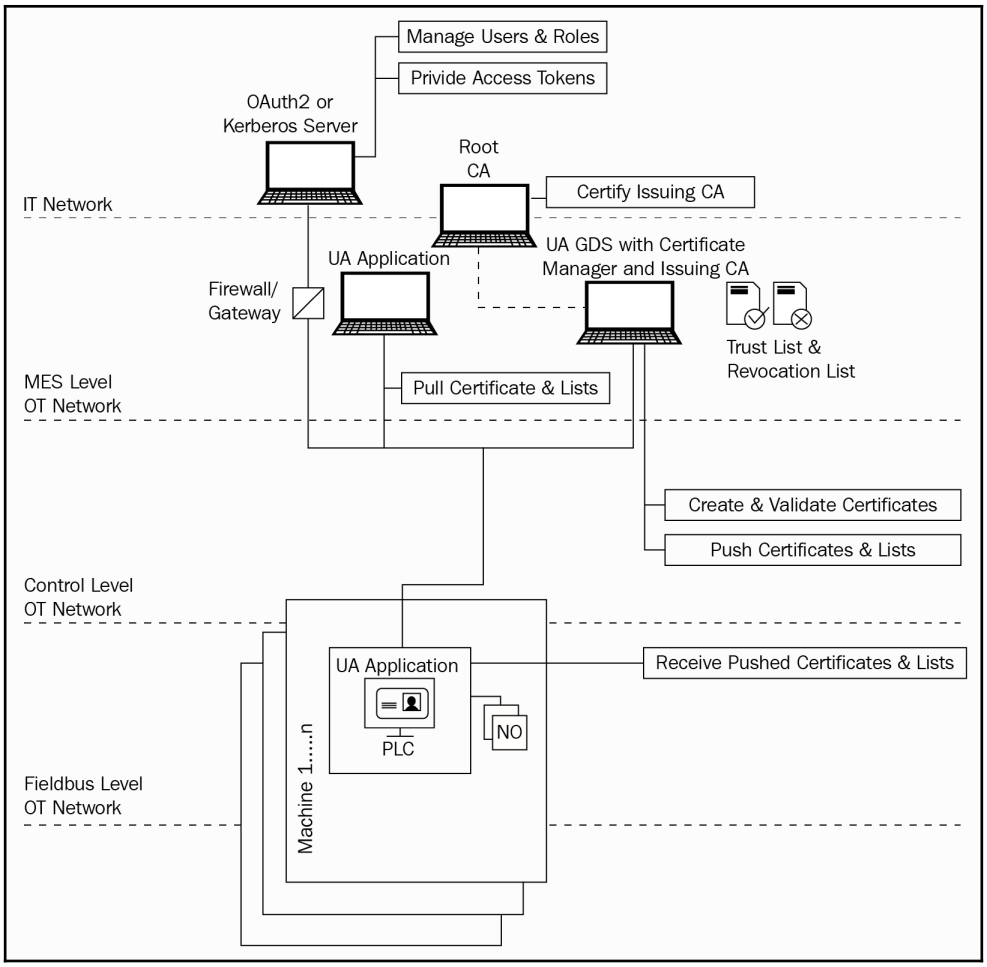

... / Energy & Utilities / Healthcare / Manufacturing / Public Sector / Transportation/...
Distributed Data Management & Interoperability
Framework
Transport
Network
Link
Physical
DDS
Web Services
DDSI-RTPS
CoAP
MQTT
HTTP
UDP
TCP
IP
TSN/ Ethernet (802.1, 802.3)
Wireless PAN (802.15)
Wireless LAN (802.11 Wi-Fi)
Wireless 2G/3G/LTE (3GPP)
Wireless Wide Area (802.16)

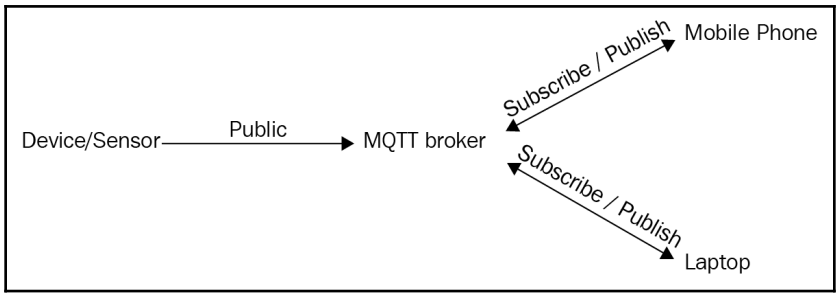
Protocol		IP/Transport	Application	Encryption	Authentication
Common Industrial Protocol (CIP)	DeviceNet	DeviceNet (Proprietary Protocol)	CIP Security	No	No
	ControlNet	ControlNet (Proprietary Protocol)		No	No
	CompoNet	CompoNet (Proprietary Protocol)		No	No
	Ethernet/IP	TCP/IP		No	No
MODBUS	Serial Modbus	Not Applicable (Serial)	Modbus (no security)	No	No
	Modbus TCP	TCP/IP	Modbus (no security)	No	No
DNP3		Secure DNP	No built-in security	Secure DNP	Secure DNP
Profibus		Not Applicable (Serial)	No built-in security	No	No
Profinet		TCP/IP, UDP/IP	No built-in security	No	No
PowerLink Ethernet		IP/Ethernet	No built-in security	No	No
EtherCAT		IP/Ethernet	No built-in security	No	No

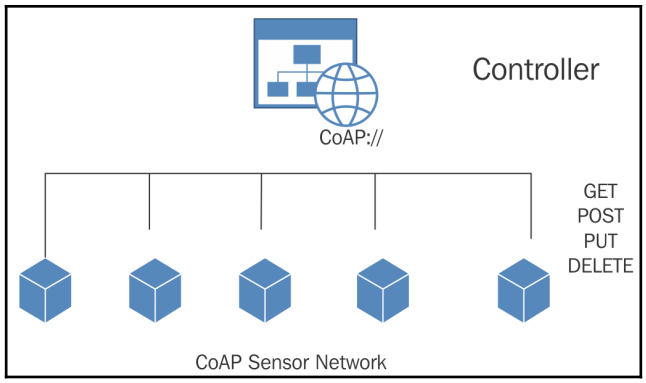
Protocol		Security Measures
Common Industrial Protocol (CIP)	DeviceNet	Logical Separation from external networks, Industrial Firewalls with deep packet inspection for intrusion detection and prevention (IDS/IPS)
	ControlNet	
	CompoNet	
	Ethernet/IP	Perimeter defense, network traffic monitoring to detect extraneous control traffic or sources (equipment).
MODBUS	Serial Modbus	Modbus Serial commands are issued as broadcast messages. Being widely used to program control elements like PLCs, RTU's, injection of malicious code can propagate into all elements. Encryption (SSL, VPN) or traffic inspection measures like (Snort), IPS (Tofino) etc. are recommended.
	Modbus TCP	Generic security measures like IDS/industrial firewalls possible for Modbus-Ethernet Actively monitor traffic to allow traffic only from legitimate devices, detect packets with erroneous values etc.
DNP3		Designed to provide high system availability. Less controls for data confidentiality and integrity. Secure DNP3 has challenge-response based authentication framework at application level, which can be used. Alternately use DNP3 encapsulated in TLS tunnels. Monitor DNP3 ports in TCP/UDP to detect any non-DNP3 traffic.
Profibus		Due to lack of authentication/security, perimeter security and network segregation are recommended.
Profinet		Profinet uses Ethernet/TCP/IP in lower layers and all IT security best practices namely network segmentation, Industrial DMZ and perimeter security using deep packet inspection are recommended.
PowerLink Ethernet		Even though communication happens in fixed time intervals, lack of authentication opens the door to device spoofing and denial of service traffic. Traffic monitoring to verify authenticity of traffic source, perimeter security and network segmentation to block intrusion and code injection attacks.
EtherCAT		Has all the vulnerabilities of Ethernet such as malicious packet/ code injection. Security measures include Deep packet inspection, source authenticity verification, network separation.



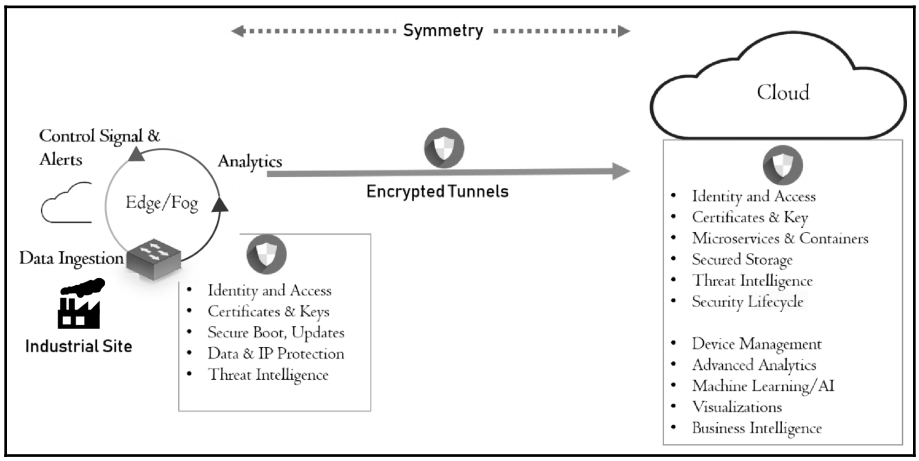

OneM2M simplified Architecture
Device
Gateway(s)
Servers
M2M Applications
M2M Service layer
Network Service Entity
Underlying Transport
AE
AE
AE
Mca
Mca
Mca
CSE
Mcc
CSE
Mcc
CSE
Mcn
Mcn
Mcn
Mcn
NSE
NSE

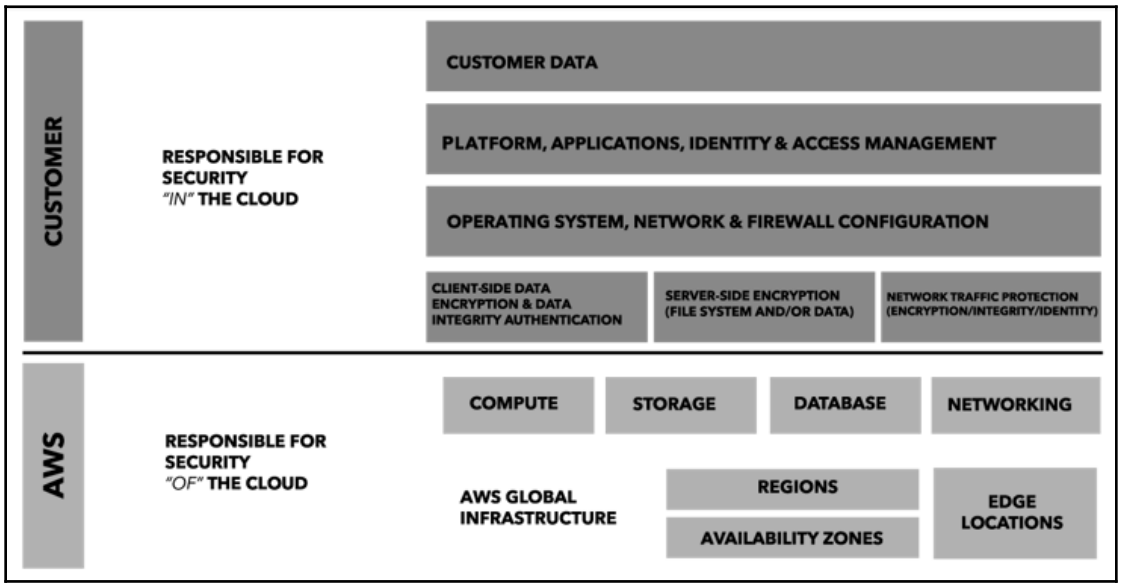

Manage Users & Roles
Privide Access Tokens
OAuth2 or
Kerberos Server
Root
CA
Certify Issuing CA
IT Network
UA Application
UA GDS with Certificate
Manager and Issuing CA
Firewall/
Gateway
Trust List &
Revocation List
MES Level
OT Network
Pull Certificate & Lists
Create & Validate Certificates
Push Certificates & Lists
Control Level
OT Network
UA Application
Receive Pushed Certificates & Lists
PLC
NO
Machine 1.....n
Fieldbus Level
OT Network

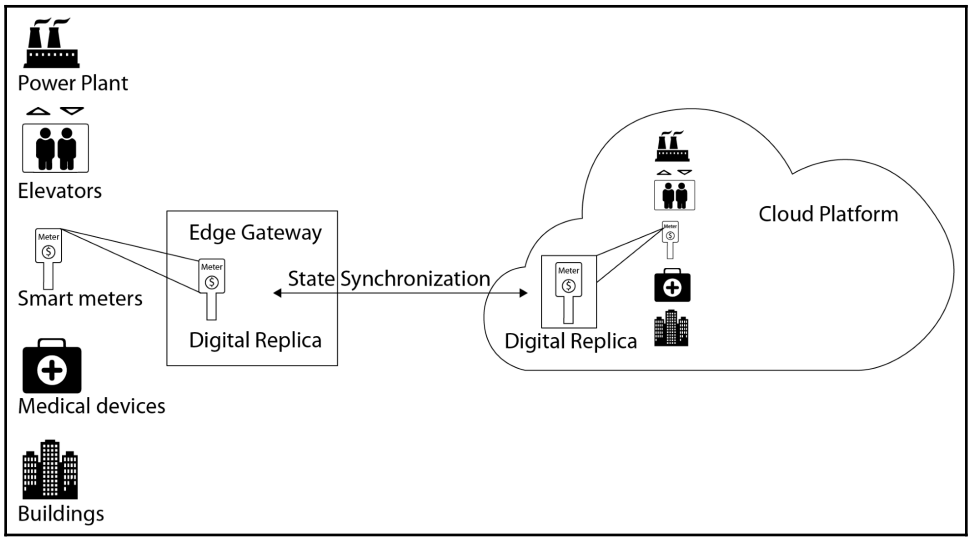

Device/Sensor
Public
MQTT broker
Subscribe / Publish
Mobile Phone
Subscribe / Publish
Laptop

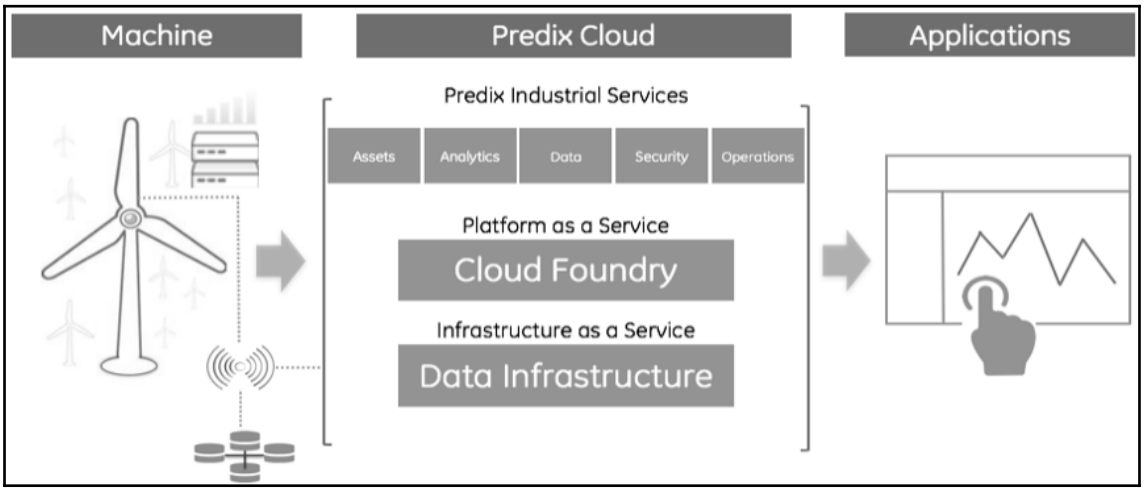

Controller
CoAP://
GET
POST
PUT
DELETE
CoAP Sensor Network

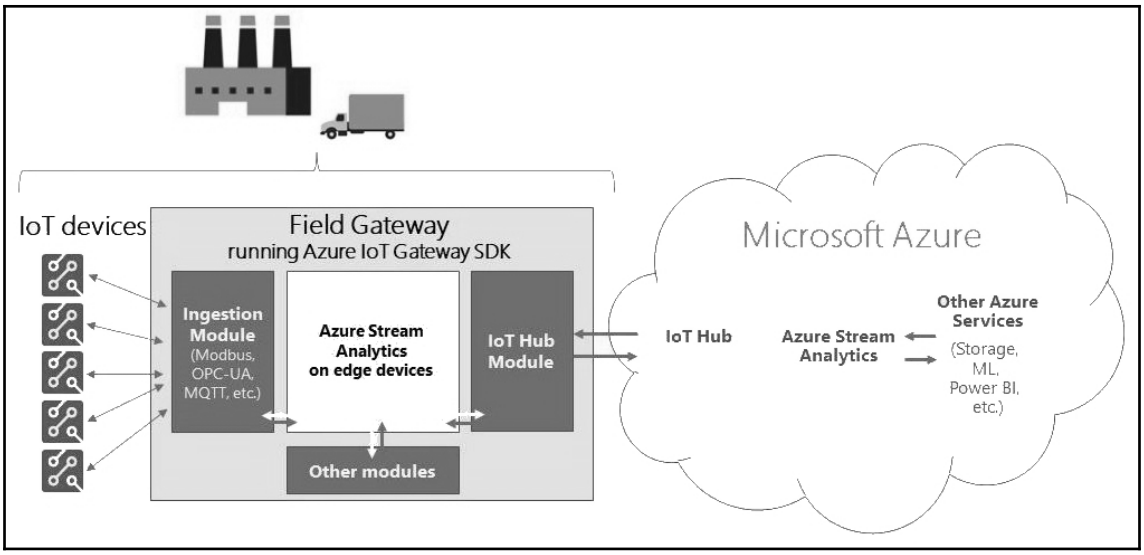
Chapter 06: Securing IIoT Edge, Cloud, and Apps

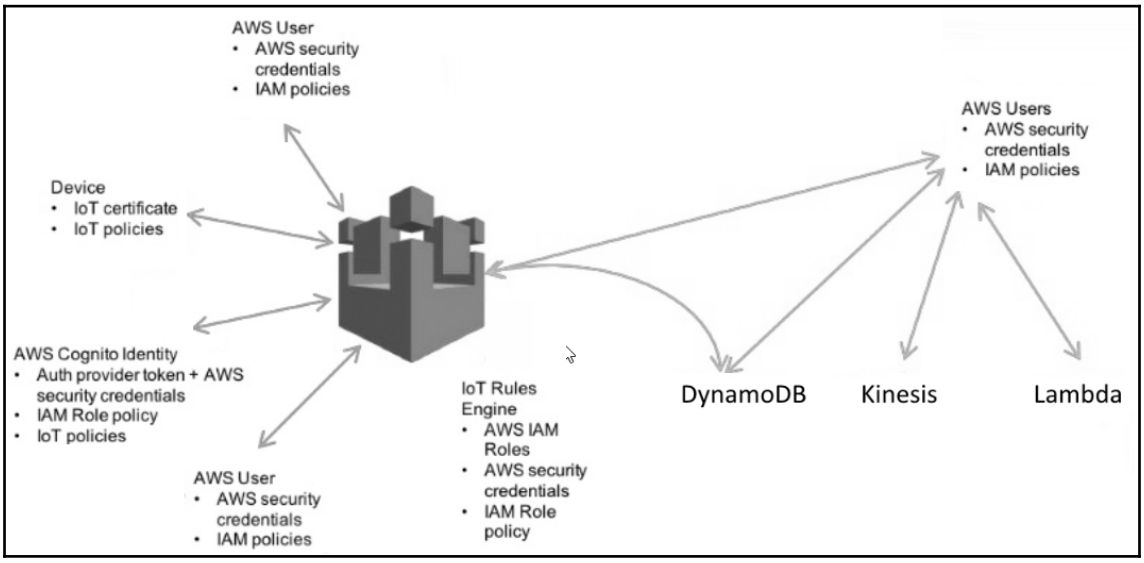


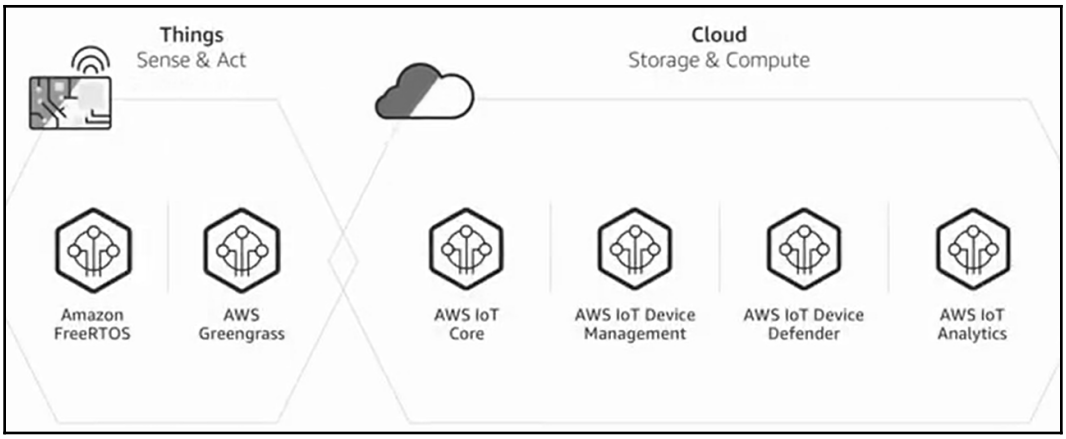



Power Plant
Elevators
Smart meters
Edge Gateway
Digital Replica
State Synchronization
Digital Replica
Cloud Platform
Medical devices
Buildings


Machine
Predix Cloud
Applications
Predix Industrial Services
Assets
Analytics
Data
Security
Operations
Platform as a Service
Cloud Foundry
Infrastructure as a Service
Data Infrastructure


IoT devices
Field Gateway
running Azure IoT Gateway SDK
Ingestion Module
(Modbus, OPC-UA, MQTT, etc.)
Azure Stream Analytics on edge devices
IoT Hub Module
Other modules
Microsoft Azure
IoT Hub
Azure Stream Analytics
Other Azure Services
(Storage, ML, Power BI, etc.)


AWS User
• AWS security credentials
• IAM policies
Device
• IoT certificate
• IoT policies
AWS Cognito Identity
• Auth provider token + AWS security credentials
• IAM Role policy
• IoT policies
AWS User
• AWS security credentials
• IAM policies
IoT Rules Engine
• AWS IAM Roles
• AWS security credentials
• IAM Role policy
AWS Users
• AWS security credentials
• IAM policies
DynamoDB
Kinesis
Lambda

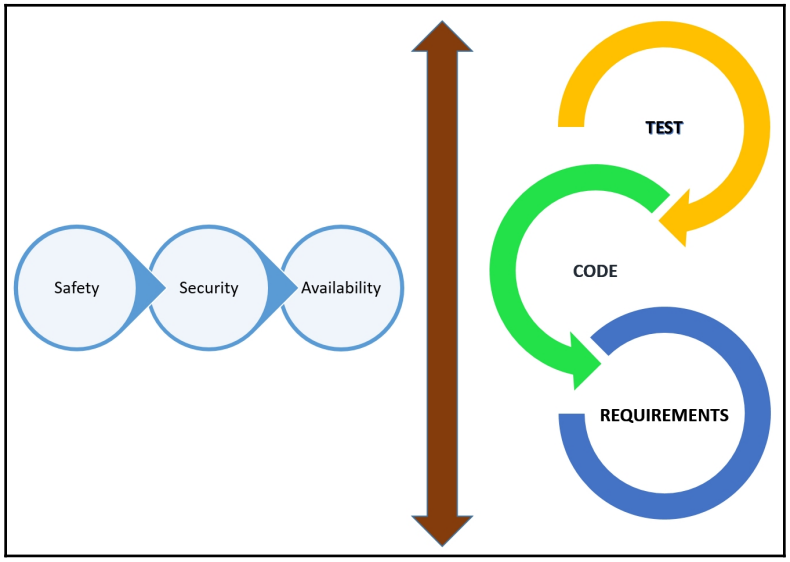


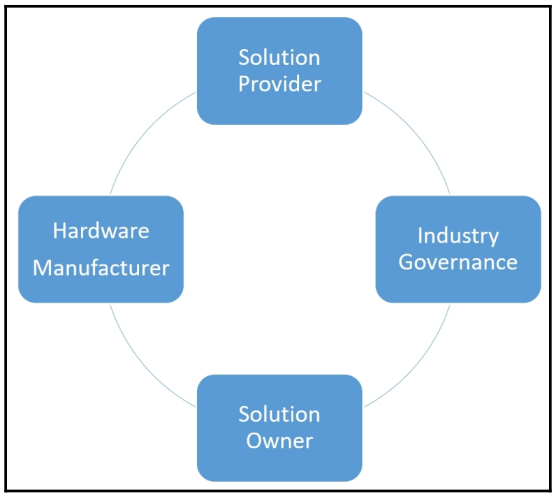
[Cloud Platform]: Security Capability Matrix	
Edge Security	[Practices implemented at the cloud-edge device such as secure boot, secure O-T-A firmware/software updates, edge access policies etc.]
Identity and Access Management	[Controls/protocols implemented for managing identity, authentication (e.g. Oauth tokens, SAML federated access etc.) and at what granularity access/authorization policies are enforced (applies to both edge and cloud)].
Infrastructure Security	[Multi-tenant/Datacenter security controls at hardware, virtualized environments e.g. container-based isolation, network, storage, monitoring etc.]
Application Security	[Application layer controls such as -- Microservice/Container architecture, app user access controls, secure development lifecycle, WAF etc.]
Data Protection	[Extent of encryption support for data-in motion/use, at rest, policies for data governance, retention, deletion etc.]
Secure Device Interaction	[How device lifecycle management is secured]
Threat Intelligence	[Documented TI capability (1 or 2 sentences max)]
Incident Response	[Incident response support (1 or 2 sentences max)]
Business Continuity	[Business continuity support (1 or 2 sentences max), use of PoPs/availability zones etc.]
Vulnerability Management	[Support for Vulnerability scanning/secure patch management particulars]
Security Monitoring	[Document supported security monitoring capabilities]
Standards Compliance	[Published list Cloud security standards the solution conforms to]

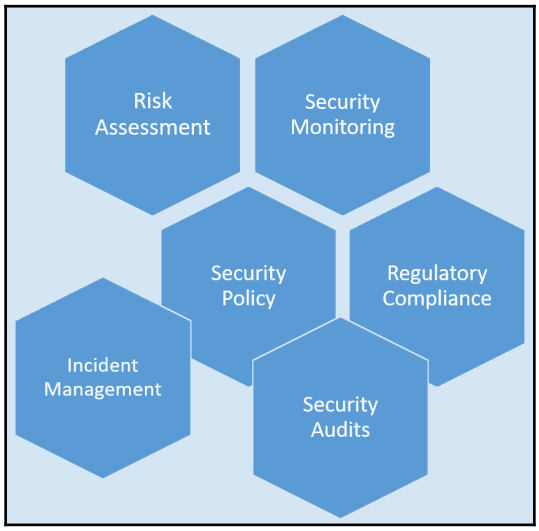
GE Digital Predix: Security Capability Matrix	
Edge Security	Secure operating environment using hardware RoT, secure boot, secureOTA firmware/software updates, edge access policies synchronized with those in the cloud, perimeter protection using GE's industrial firewalls for network segmentation and deep packet inspection.
Identity and Access Management	Identity management through SCIM APIs, PKI, digital certificates; Oauth 2.0 token for access to relevant applications, SAML federation capabilities, key management; tenant-aware fine grained access control for application, data and analytics.
Infrastructure Security	Cloud-Foundry based multi-tenant design, tenants logically isolated at run-time and storage, native logging support to monitor traffic across VLANS and VPCs for anomalies and audit.
Application Security	Microservice design, security specific microservices in Predix.io catalog, application and user level access policies for resource access, Predix secure development lifecycle (PSDL), application security review enforcement.
Data Protection	Encryption of sensitive data, TLS and digital certificates for user level encryption for data in motion. Dataflow monitoring for anomalies, policies enforced for data governance, retention and deletion.
Secure Device Interaction	Digital Twins, device provisioning and management over secure tunnels, device monitoring for anomalies.
Threat Intelligence	TI program to ingest and interpret multiple streams of threat information to preempt attacks
Incident Response	End-to-end coordination of incident response which includes incident notification, investigation, forensics, and close-out
Business Continuity	Geographically diverse PoPs and availability zones deployed for Predix Cloud using active-active model for seamless cutover.
Vulnerability Management	Vulnerability scans of open source, as well as in-house and commercial off-the-shelf (COTS) technologies
Security Monitoring	Continuous traffic monitoring to detect traffic anomalies at the edge and the cloud.
Standards Compliance	https://www.predix.com/sites/default/files/predix-the-industrial-internet-platform-from-ge-digital-brief.pdf

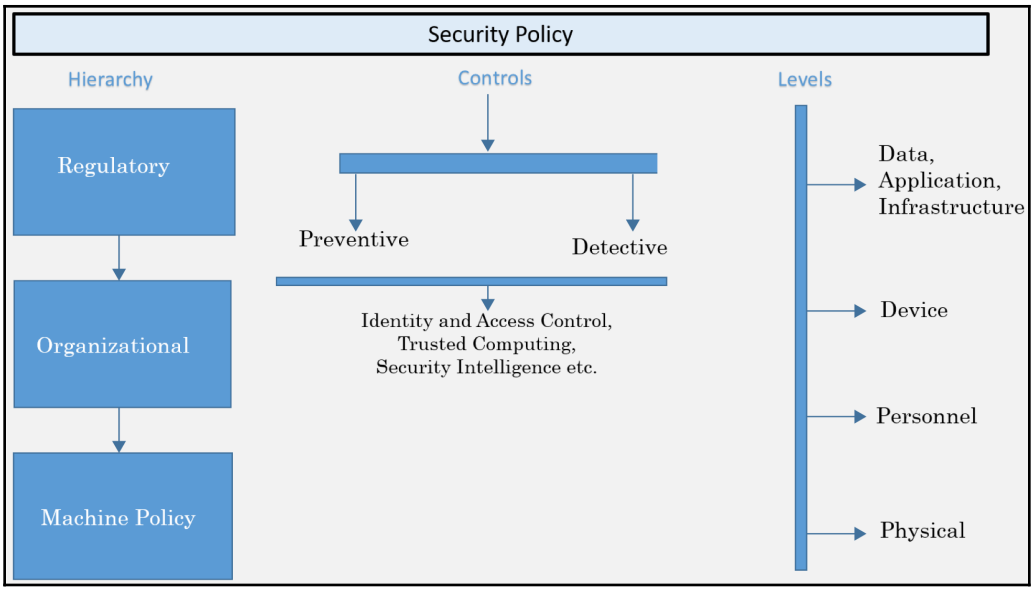
Chapter 07: Secure Processes and Governance

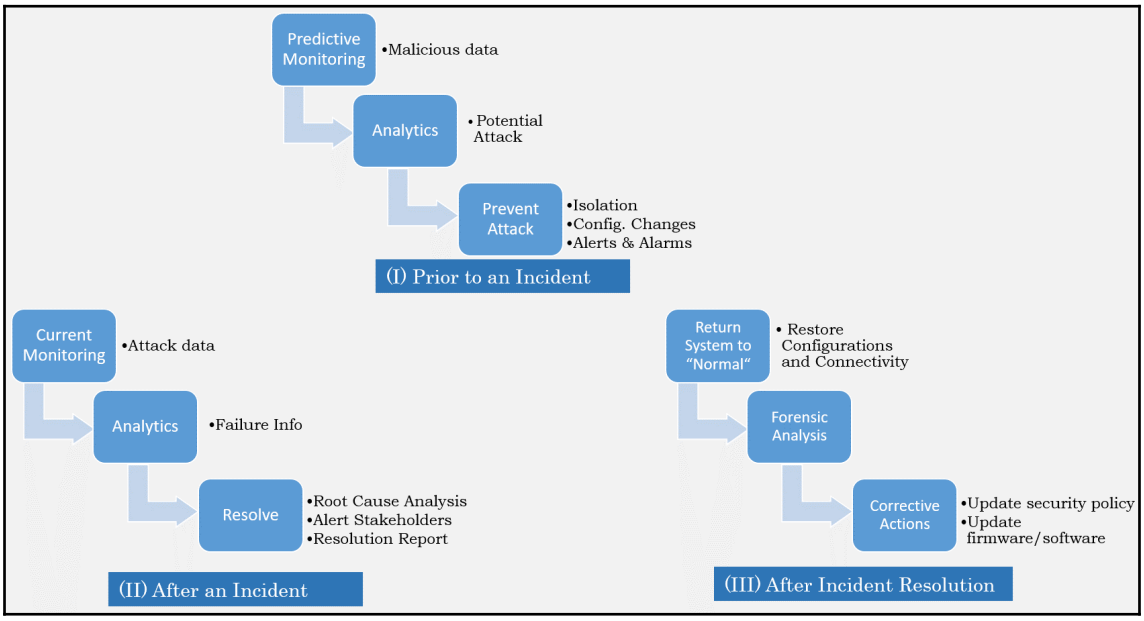
Business Case	System Definition	Development	Deployment	Operations
Early integration of security and safety in: • Business Objectives • Vision and Values • Problem definition • Customer Usage etc.	• Safety, security, availability in use case analysis, system architecture and requirements • Enumerate Security Regulations and Standards	• Secure component boundaries and APIs • Isolation, Access control, HW RoT, • Safe coding practices • Security Testing • Requirements traceability	• "Right Size" security • Use Case specific security architecture, standards and regulations. • Secure POC, Scale testing • Security based partner and vendor selection	• Secure device onboarding, provisioning • Security Monitoring, analysis and audits. • Incident Management • Enterprise Security Program

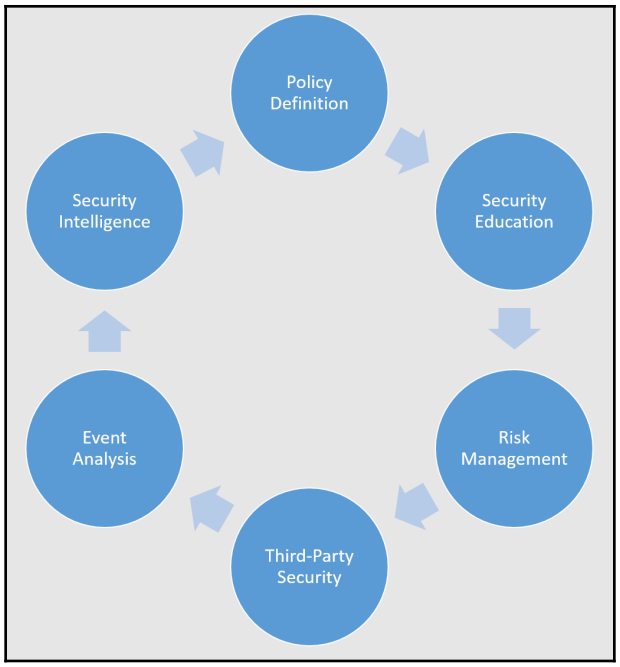



Solution Provider
Industry Governance
Solution Owner
Hardware Manufacturer

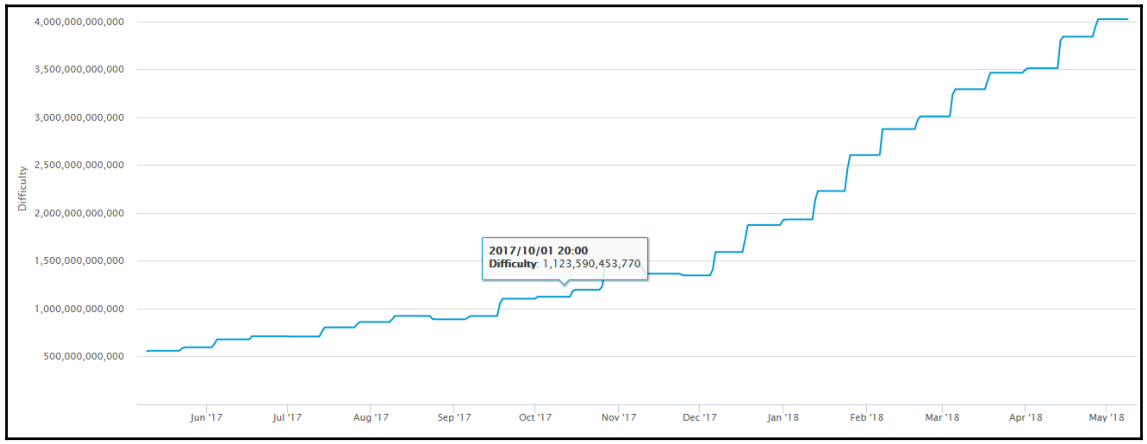

Risk Assessment
Security Monitoring
Security Policy
Regulatory Compliance
Incident Management
Security Audits

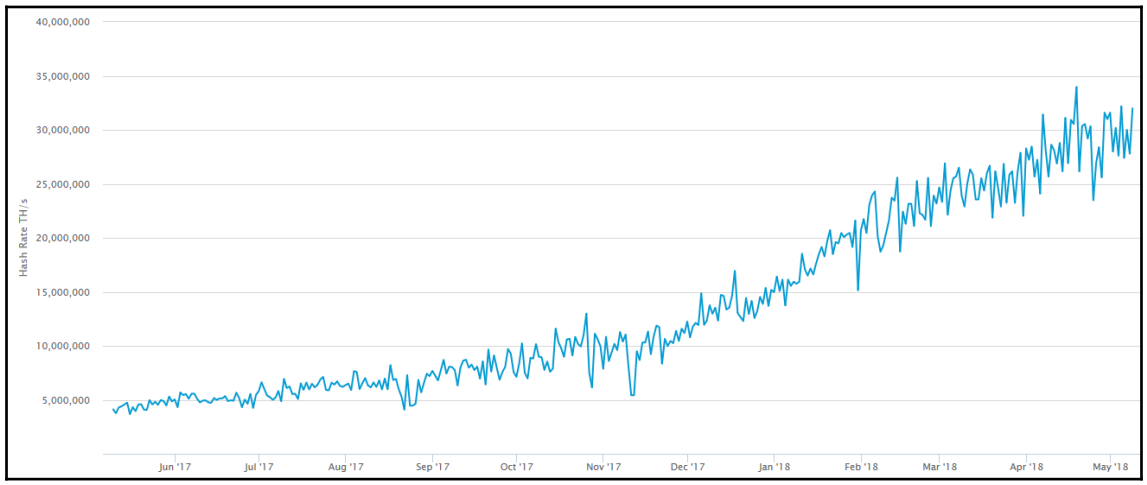

Security Policy
Hierarchy
Regulatory
Organizational
Machine Policy
Controls
Preventive
Detective
Identity and Access Control,
Trusted Computing,
Security Intelligence etc.
Levels
Data,
Application,
Infrastructure
Device
Personnel
Physical

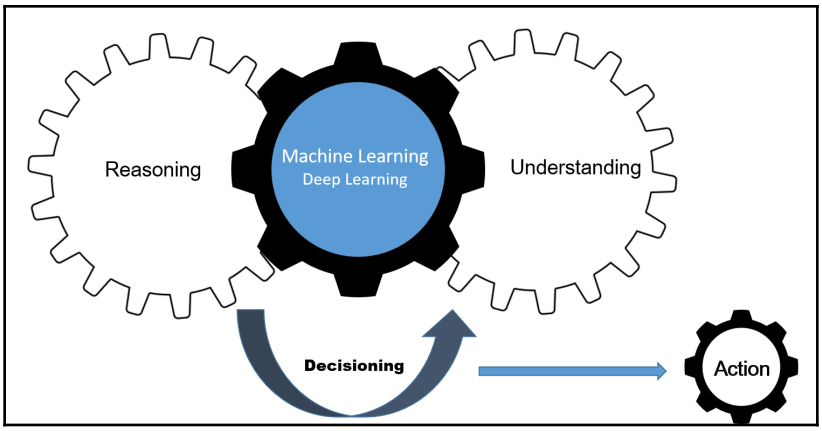

Predictive Monitoring
•Malicious data
Analytics
• Potential Attack
Prevent Attack
•Isolation
•Config. Changes
•Alerts & Alarms
(I) Prior to an Incident
Current Monitoring
•Attack data
Analytics
•Failure Info
Resolve
•Root Cause Analysis
•Alert Stakeholders
•Resolution Report
(II) After an Incident
Return System to "Normal"
• Restore Configurations and Connectivity
Forensic Analysis
Corrective Actions
•Update security policy
•Update firmware/software
(III) After Incident Resolution

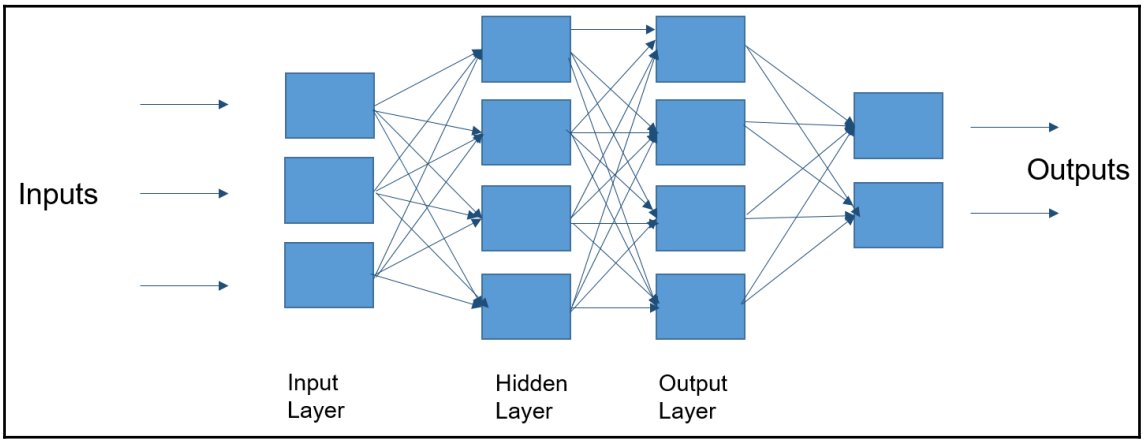

Policy Definition
Security Education
Risk Management
Third-Party Security
Event Analysis
Security Intelligence

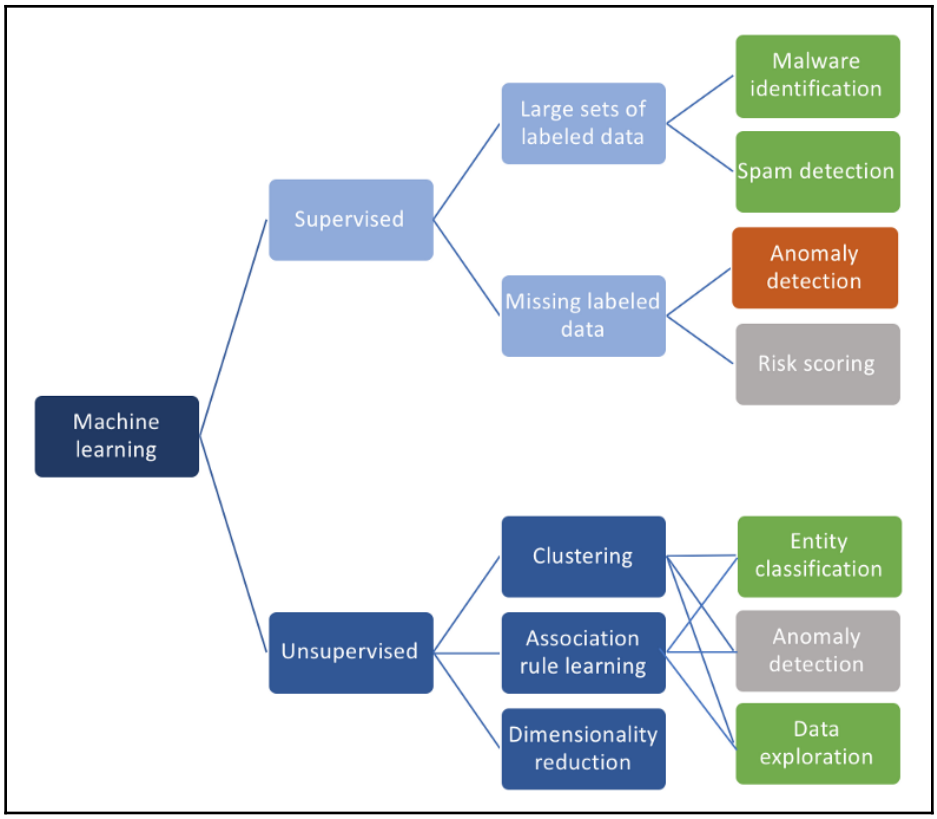
Chapter 08: IIoT Security Using Emerging Technologies



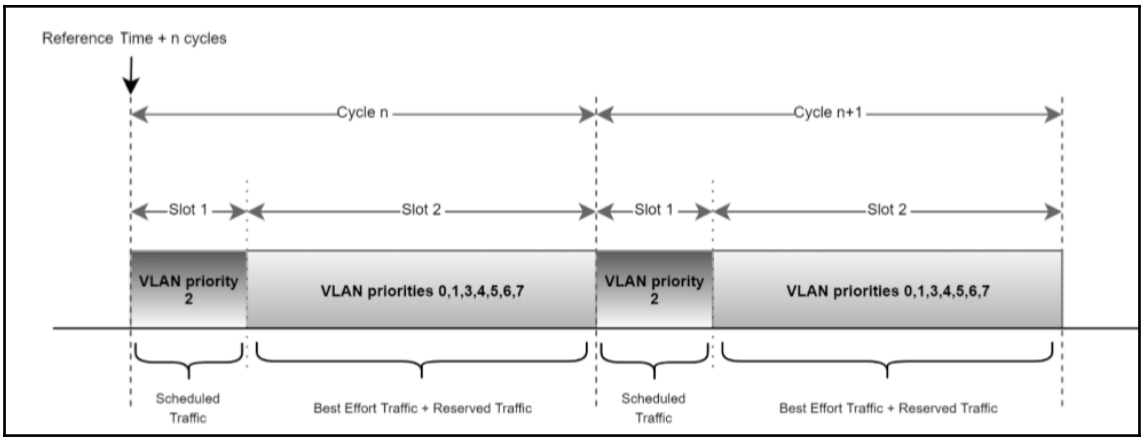



Reasoning
Machine Learning
Deep Learning
Understanding
Decisioning
Action

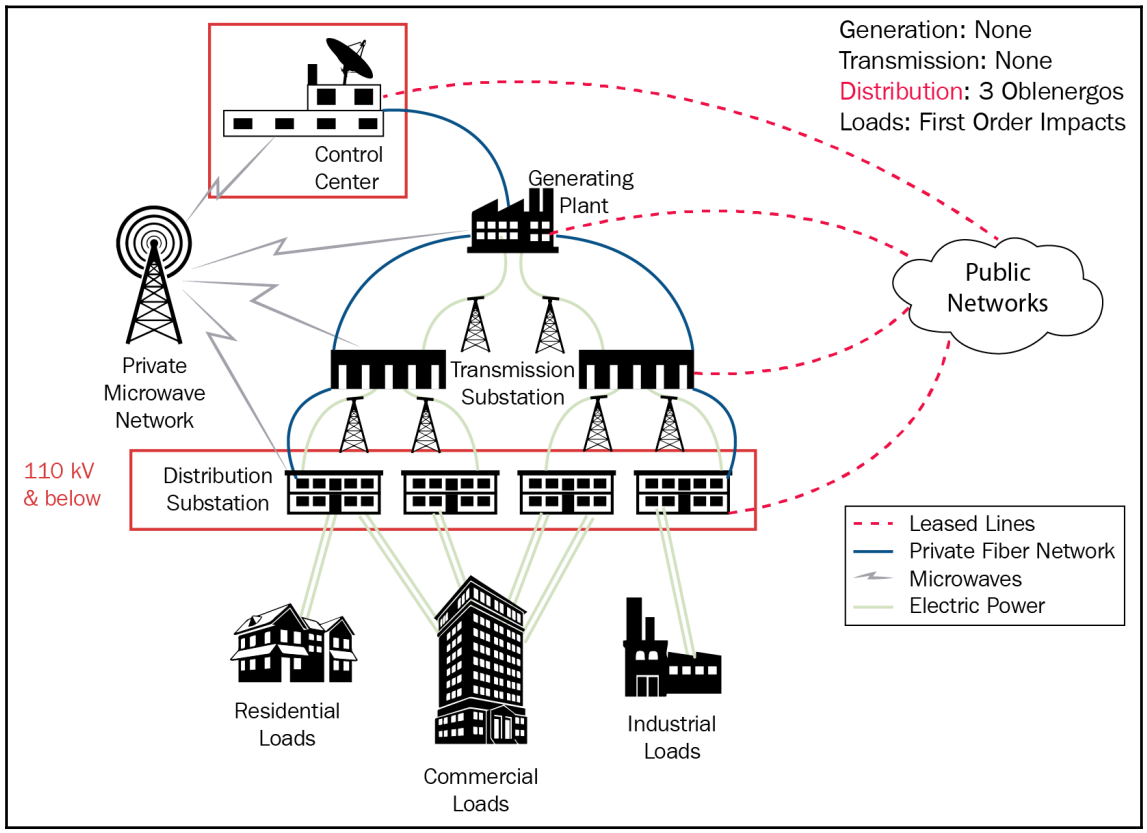

Inputs
Outputs
Input Layer
Hidden Layer
Output Layer

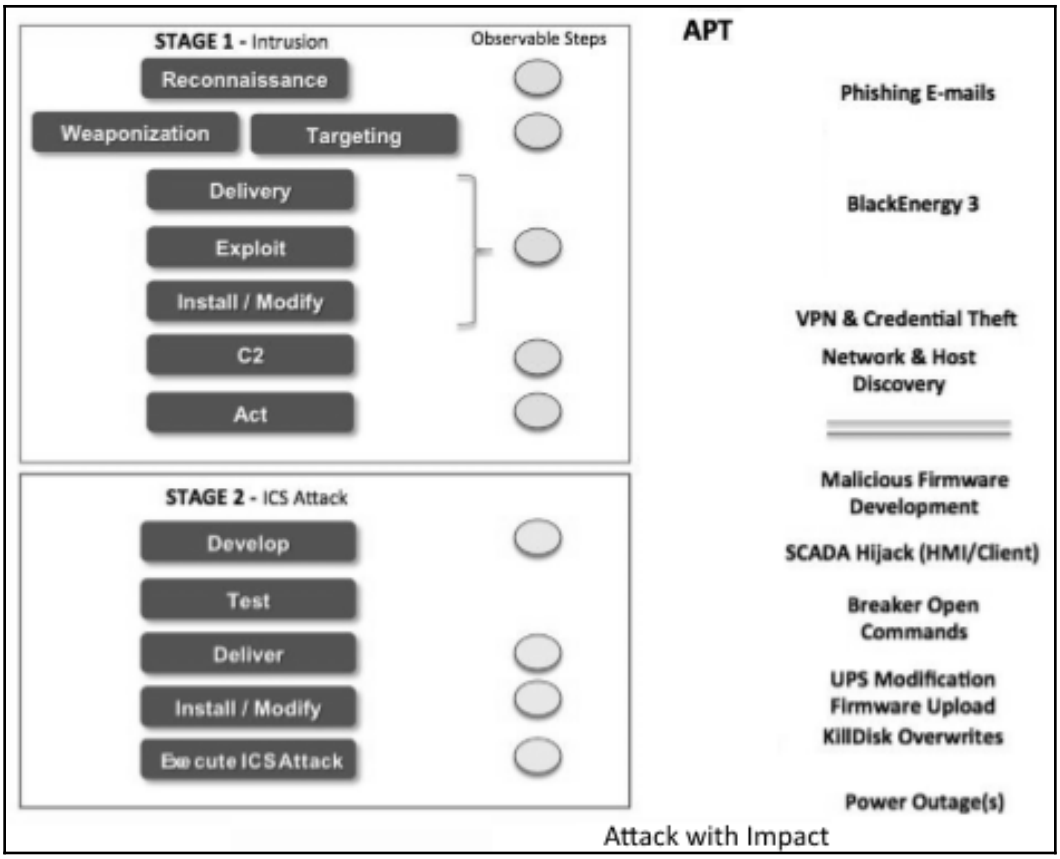


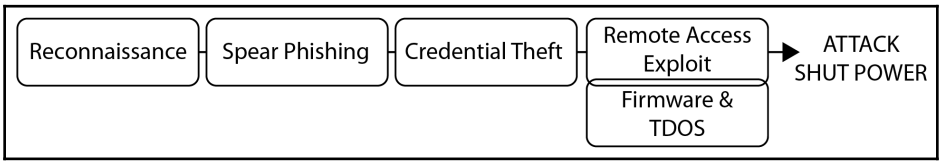
Standard	Area
IEEE 802.1ASrev, IEEE 1588	Timing & Synchronization
IEEE 802.1Qav	Queue Management and Bandwidth Reservation for Deterministic Flows (Credit Based Shaper)
IEEE 802.1Qbv	Scheduling to Provide Fast Deterministic Cyclic Flows
IEEE 802.1Qbu & IEEE 802.3br	Frame Preemption for Lower Latency of Prioritized Flows
IEEE 802.1Qch	Simple Scheduling and Bandwidth Reservation for Deterministic Flows (Peristaltic Shapers)
IEEE 802.1Qcr	Queue Management and Bandwidth Reservation for Deterministic Flows (Asynch Traffic Shaping)
IEEE 802.1Qat	Distributed Protocol for Simplified Set-up (SRP)
IEEE 802.1Qcc	System Configuration for Simplified Set-up (Centralized Config and Improved SRP)
IEEE 802.1Qcp	Support for Standardized Systems Management (YANG)
IEEE 802.1CB	Seamless Redundancy for Critical Flows
IEEE 802.1Qci	Time Aware Ingress Policing for Reliability


Reference Time + n cycles
Cycle n
Cycle n+1
Slot 1
Slot 2
Slot 1
Slot 2
VLAN priority 2
VLAN priorities 0,1,3,4,5,6,7
VLAN priority 2
VLAN priorities 0,1,3,4,5,6,7
Scheduled Traffic
Best Effort Traffic + Reserved Traffic
Scheduled Traffic
Best Effort Traffic + Reserved Traffic

Chapter 09: Real-World Case Studies in IIoT Security




STAGE 1 - Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
STAGE 2 - ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
APT
Phishing E-mails
BlackEnergy 3
VPN & Credential Theft
Network & Host Discovery
Malicious Firmware Development
SCADA Hijack (HMI/Client)
Breaker Open Commands
UPS Modification
Firmware Upload
KillDisk Overwrites
Power Outage(s)
Attack with Impact


Reconnaissance
Spear Phishing
Credential Theft
Remote Access Exploit
Firmware & TDOS
ATTACK SHUT POWER

Reconnaissance	Limit public availability of architecture, sub-system versions, network diagrams etc. Detect anomalous behavior by passive monitoring of insider and third-party activities such as device access, browsing history, timestamps etc. Regularly leverage security intelligence and forensics.
Social Engineering	Personnel training to combat malicious social engineering. Segment functional network domains. Use proxy servers and gateways to monitor and control inbound and outbound communication paths. Deep packet inspection and malware detection tools to prevent malware proliferation across network segments.
Credential Theft	Directory segmentation ((e.g., Active Directory, Domain, eDirectory, and LDAP), ability to detect various forms of Trojans, user account activity monitoring.
Data Exfiltration	Maintain a vaulted copy of known good project files, control and safety logic, and firmware. Network Security Monitoring (NSM) can be used to detect exfiltration of ICS and IT data
Remote Access Exploit	Allow a bare minimum number of trusted remote connections. Use SoC to monitor VPN connections and activities. Two-factor authentication for remote users. Disable split tunneling. Application level logic that requires operator confirmation to trigger any high-risk actuation command (e.g. UPS, Circuit breaker operations).
Firmware Updates	Secure firmware updates of endpoints using digital signatures and hardware-based root of trust.
Response and Recovery	A solid incident response plan enables remediation well before the adversaries have performed the intended attack to impact. Active and passive monitoring, alarms and response from the IR team together detects malicious activity, minimizes impact of the final attack and expedites recovery.

Chapter 10: The Road Ahead