What are Smart Cities and a Smart Transportation Systems without a Cyber Secured Fortified Smart Grid Network?

Chicago Historical Society

▲ *Traffic jams long predated the automobile. Here, trolleys, horse-drawn wagons, and a sea of pedestrians have created what seems a hopeless gridlock.*

iS5 Communications
ITS Canada – Niagara Falls
June 2018

iS5 Communications

- Founded in 2012 by ex-RuggedCom executives; headquartered in Mississauga, Canada.
- Focus on protecting critical infrastructure networks with next generation products that have advanced cybersecurity features.
- iS5 products are designed to meet and exceed stringent operational requirements such as IEC61850, IEEE1613.
- The Raptor platform was specifically architected for Operational Technology (OT) networks, but with enterprise (IT) security, performance and features.

Utility

- Grid Modernization
- Power Generation
- Transmission, Distribution & Substation Automation
- Oil & Gas

Transportation

- Air Transportation
- Rolling-Stock
- Marine & Offshore
- Intelligent Transportation Systems (ITS)

Industrial

- Machine-to-Machine (M2M)
- Factory Automation
- Remote Monitoring & Diagnostics

Surveillance

- Security
- Law Enforcement
- Investigative & Protective Services

Defence

- Homeland security
- Military Networks
- Air-to-Ground Communications
- Onboard Networks

iS5Com's innovative, hardened, and secure platforms, partner relationships, and thought leadership will expand the company's footprint into other critical infrastructure verticals

iS5 COMMUNICATIONS

iS5 Communications

- Key competencies:
  - Domain Knowledge in OT and IT networks
  - Provide End-to-End Solutions from control center to the end device
  - Expertise in Substation Automation Systems – IEC 61850
  - Design Secure Industrial Networks to meet guide lines such as:
    - NERC-CIP - USA
    - FERC – USA
    - NISA – Middle East
    - NISA - Israel
    - NCIIPC – India
    - EPCIP – Europe
    - ACORN – Australia
    - CSA - Singapore

- Products:
  - Cyber Secure Cloud Platforms for:
    - Critical Infrastructure Protection
    - Mission Critical Applications
    - Industrial and Defense Applications

- Expert Services:
  - Apply our domain expertise to assist customers to design, configure, and optimize their networks.

- Training/Educational Services:
  - Incorporate product and domain knowledge to provide specific training that meet customer requirements.

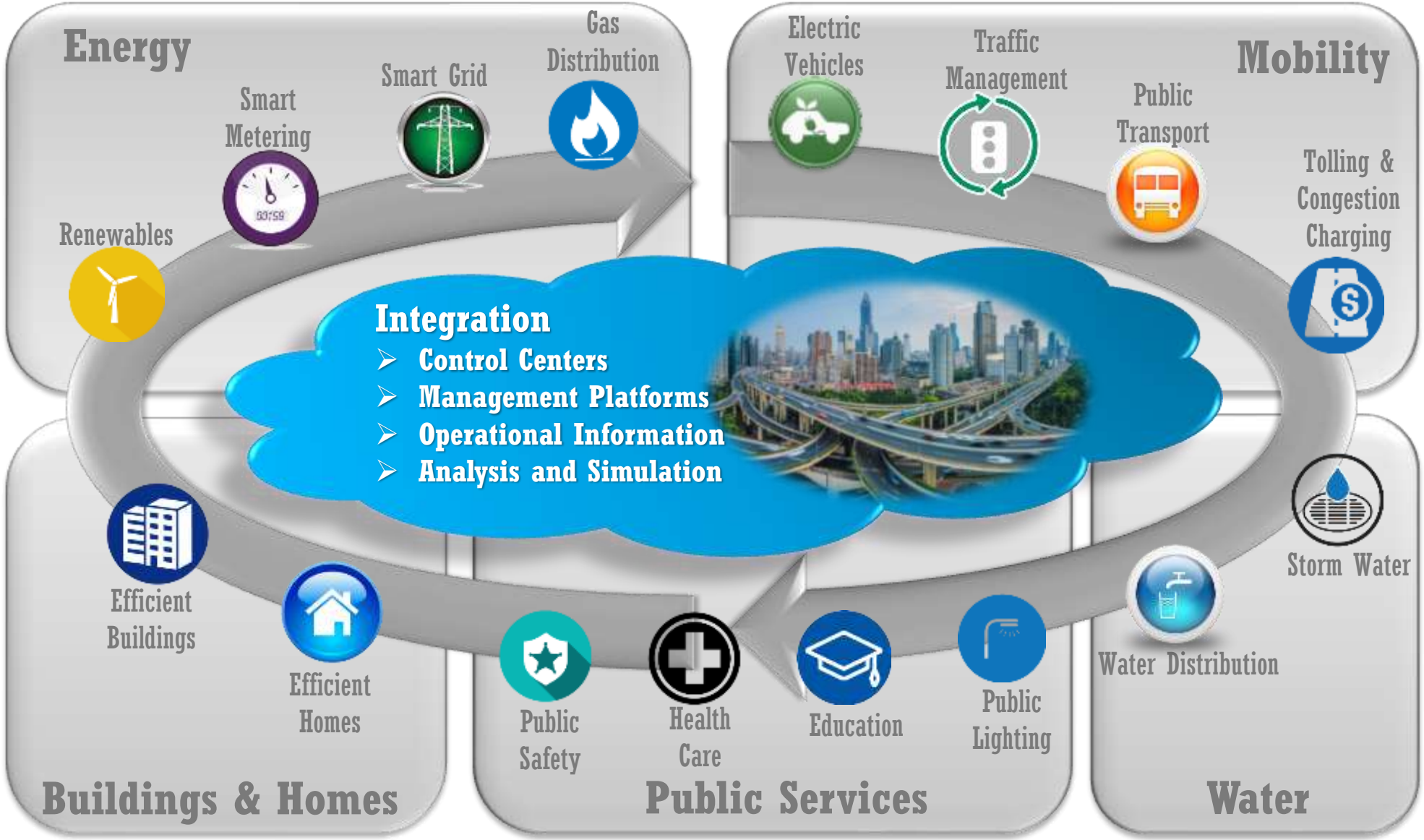
Smart Cities?

Leverage Technology to implement an infrastructure for an optimized, scalable and sustainable city for future.

Comprising of six sectors

- Smart Energy
- Smart Mobility
- Smart Public Services
- Smart Water
- Smart Buildings
- Smart Integration

What are Smart Cities?



Cyber Attacks Increasing on Vital Critical Infrastructure

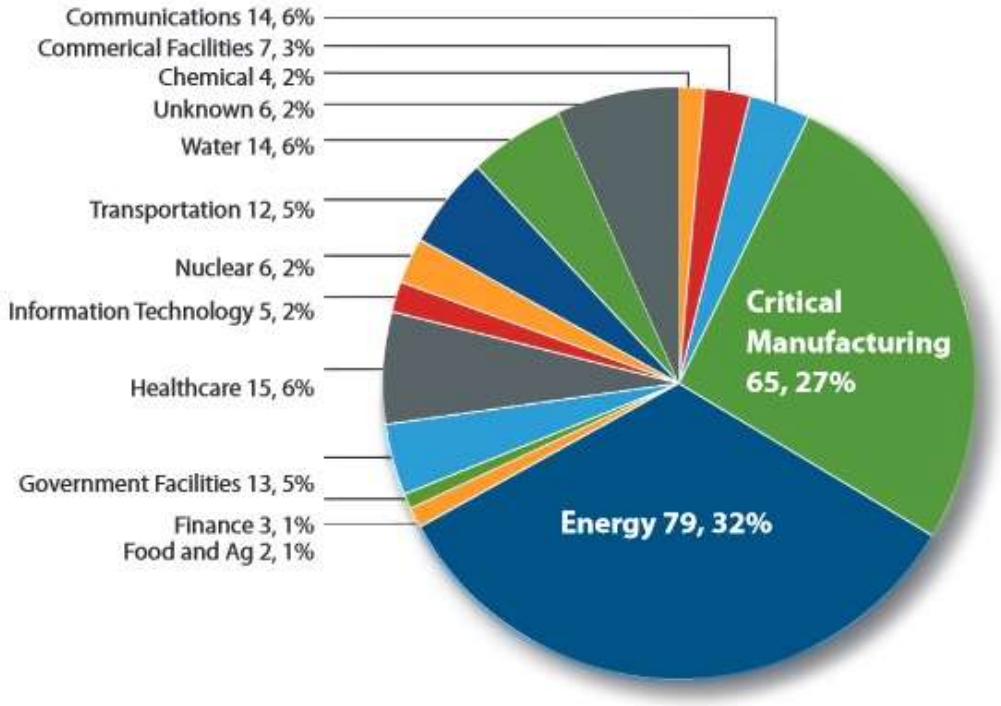
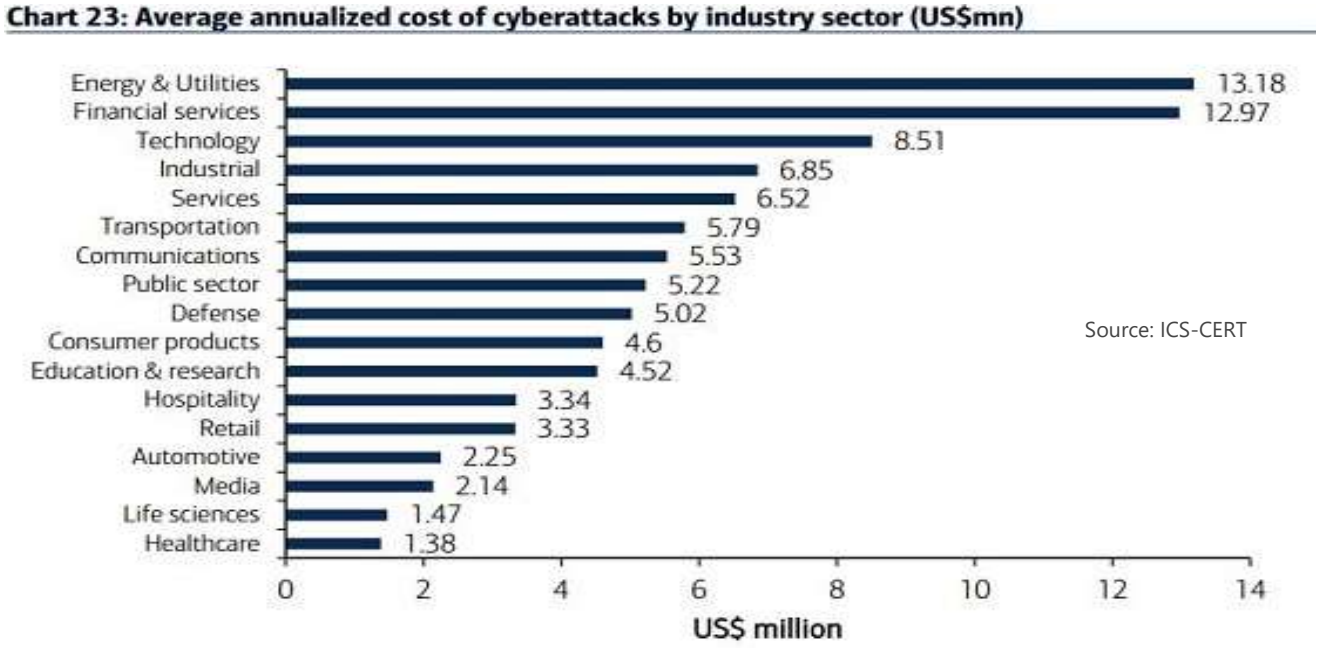


Figure 1. FY 2014 incidents reported by sector (245 total).

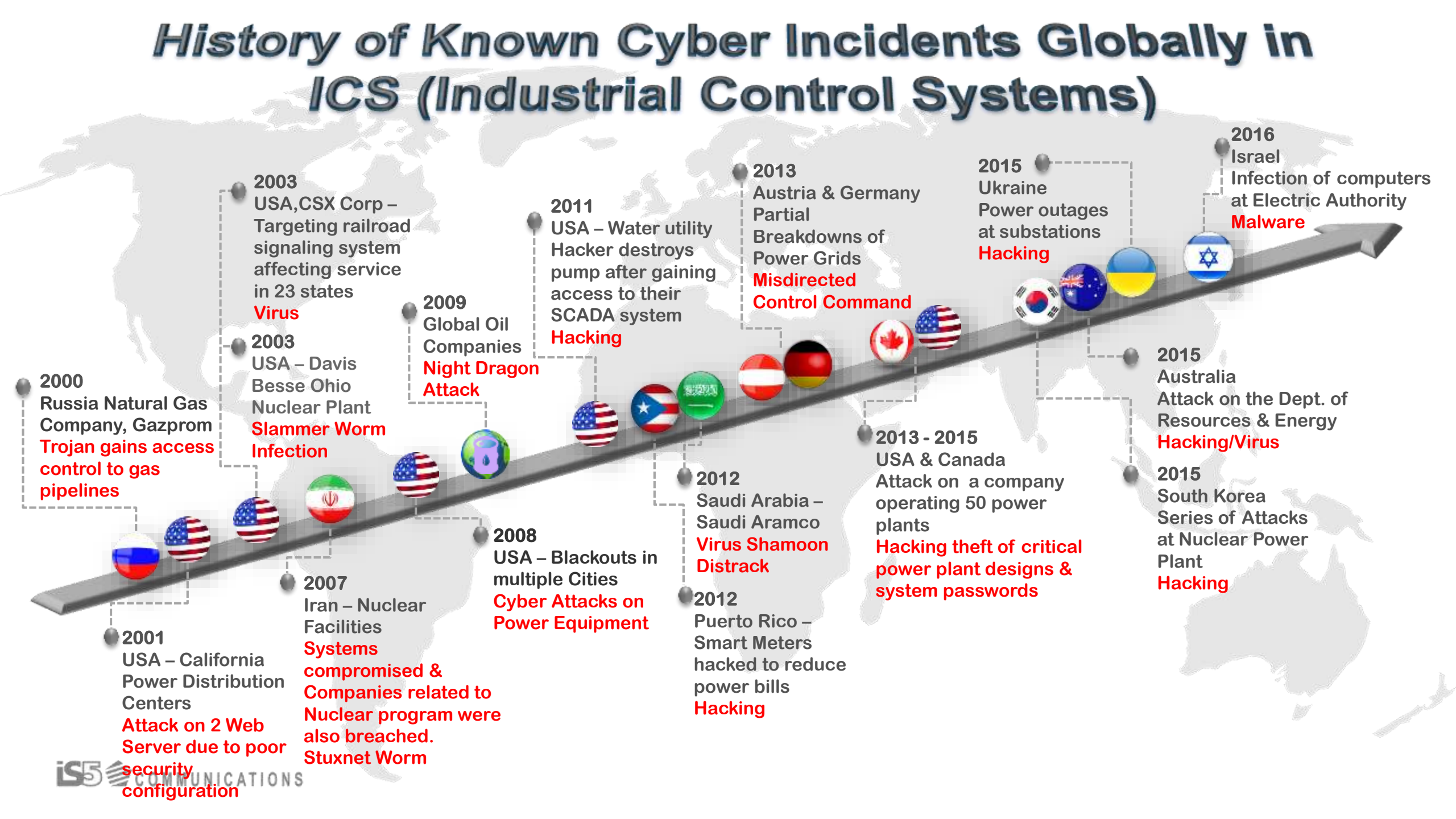


Source: Ponemon

Cyber Crime Costs Projected To Reach $2 Trillion by 2019
Source: Forbes

Source: April 2016, Canadian Underwriter/Tripwire

History of Known Cyber Incidents Globally in ICS (Industrial Control Systems)



2000
Russia Natural Gas Company, Gazprom
Trojan gains access control to gas pipelines

2001
USA – California Power Distribution Centers
Attack on 2 Web Server due to poor security configuration

2003
USA,CSX Corp – Targeting railroad signaling system affecting service in 23 states
Virus

2003
USA – Davis Besse Ohio Nuclear Plant
Slammer Worm Infection

2007
Iran – Nuclear Facilities
Systems compromised & Companies related to Nuclear program were also breached.
Stuxnet Worm

2008
USA – Blackouts in multiple Cities
Cyber Attacks on Power Equipment

2009
Global Oil Companies
Night Dragon Attack

2011
USA – Water utility Hacker destroys pump after gaining access to their SCADA system
Hacking

2012
Saudi Arabia – Saudi Aramco
Virus Shamoon Distrack

2012
Puerto Rico – Smart Meters hacked to reduce power bills
Hacking

2013
Austria & Germany Partial Breakdowns of Power Grids
Misdirected Control Command

2013 - 2015
USA & Canada
Attack on a company operating 50 power plants
Hacking theft of critical power plant designs & system passwords

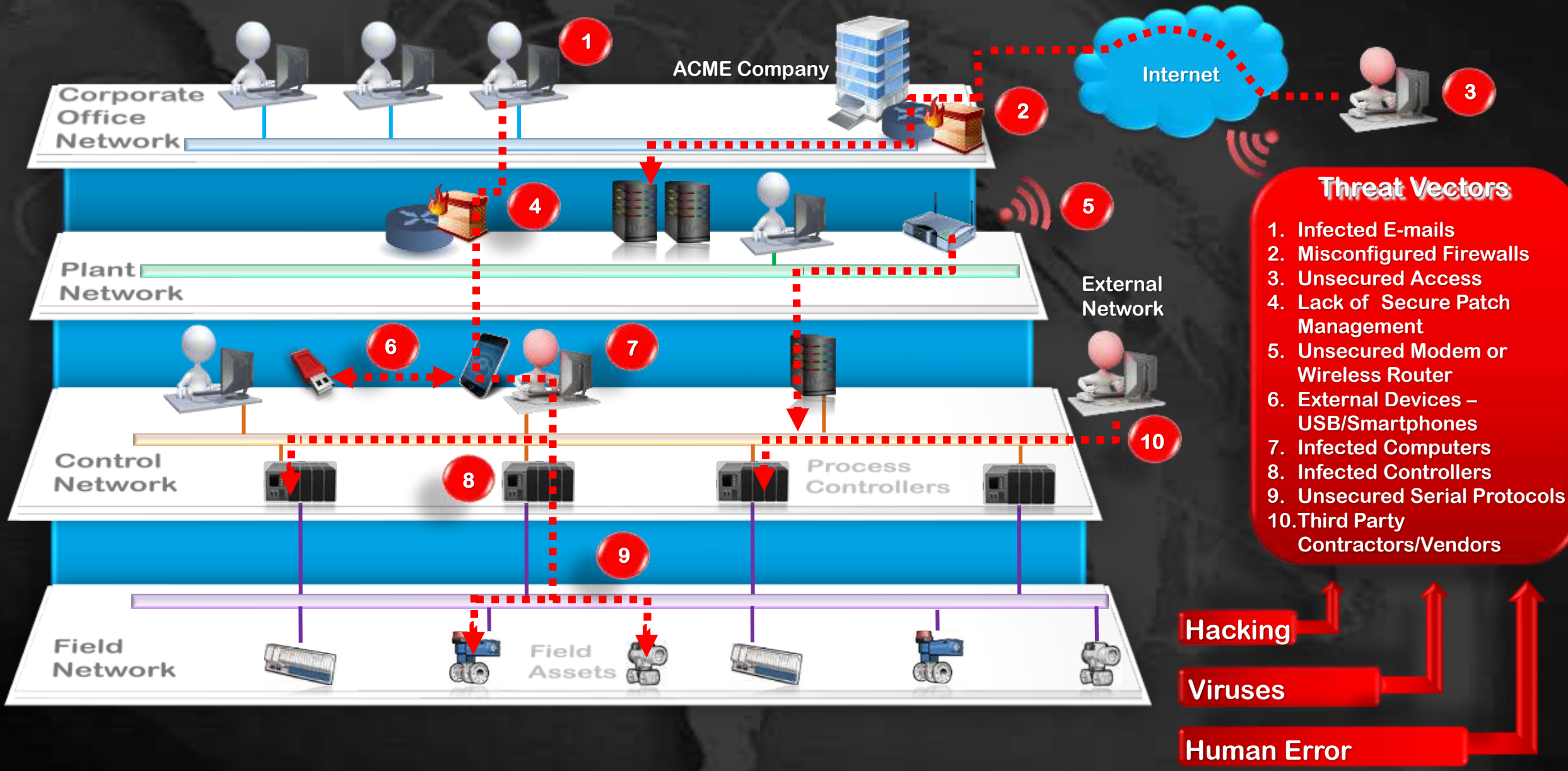
2015
Ukraine
Power outages at substations
Hacking

2015
Australia
Attack on the Dept. of Resources & Energy
Hacking/Virus

2015
South Korea
Series of Attacks at Nuclear Power Plant
Hacking

2016
Israel
Infection of computers at Electric Authority
Malware

Cyber Threat landscape for Industrial Control Systems



Threat Vectors

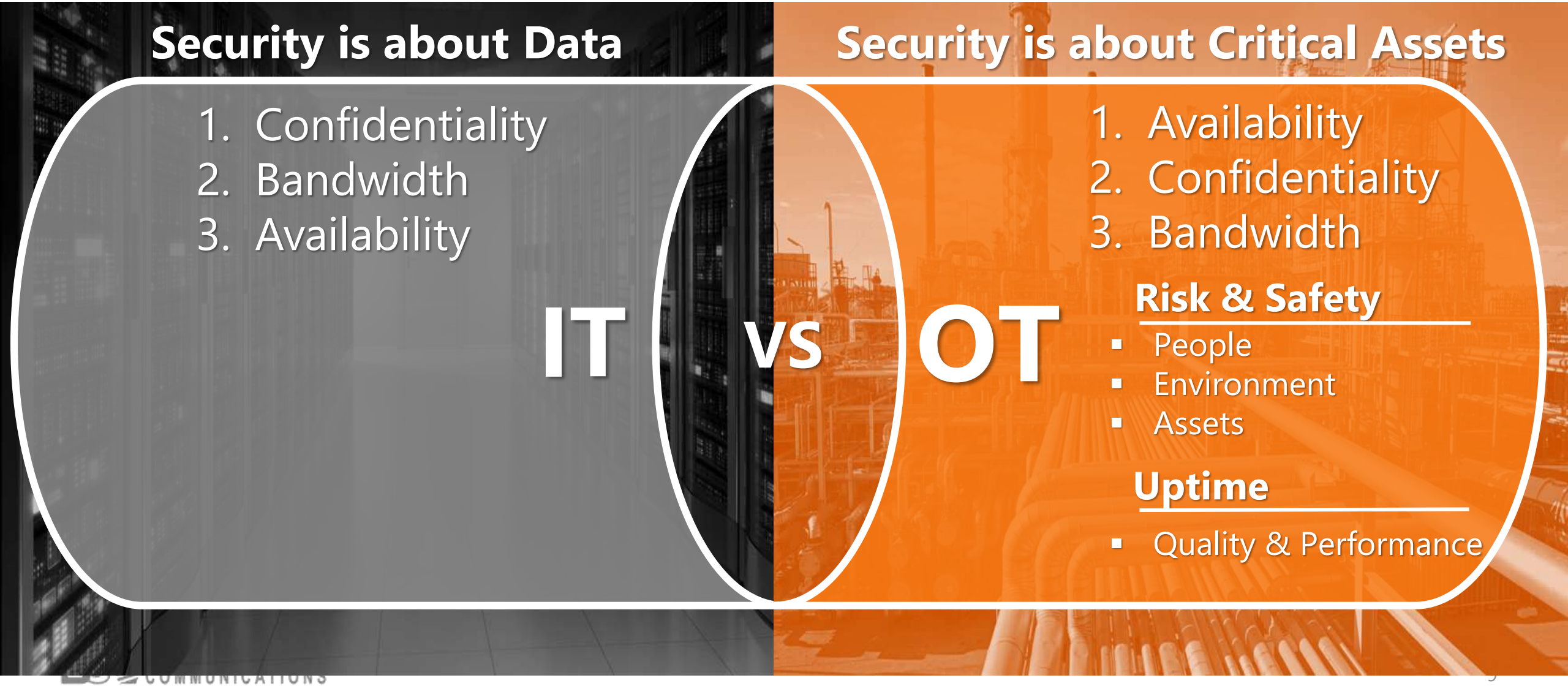
1. Infected E-mails
2. Misconfigured Firewalls
3. Unsecured Access
4. Lack of Secure Patch Management
5. Unsecured Modem or Wireless Router
6. External Devices – USB/Smartphones
7. Infected Computers
8. Infected Controllers
9. Unsecured Serial Protocols
10. Third Party Contractors/Vendors

Hacking

Viruses

Human Error

Culture is the biggest hurdle for Industrial Digital Transformation

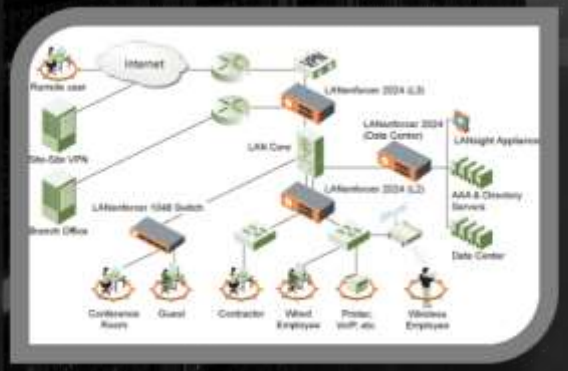


Information Security vs. Operational Security

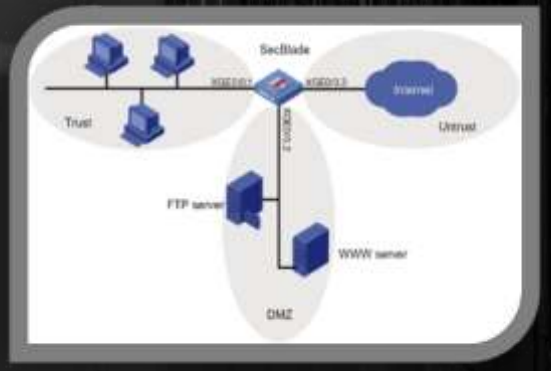
IT

Mostly L3 Security

Remote Access & WEB
Access Points Protection



User Login
Resources Access

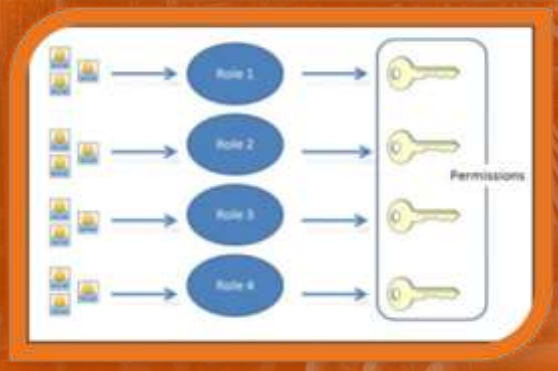


Human to Human
Stateful

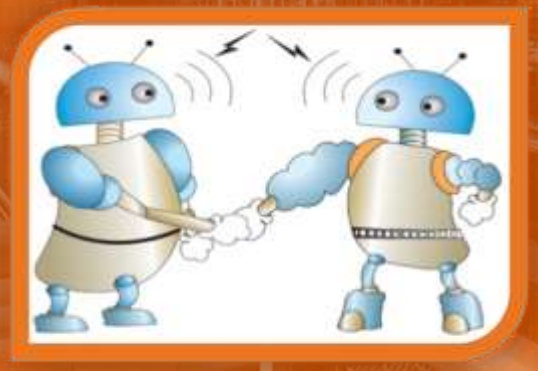
OT

L2 Security
Requirements

Exposed End Points
End Point Protection



Role Based Access Control
With Logging
Assets Access



Machine to Machine
Stateless

Unique Requirements for OT Networks Power Utilities

Strict Network Convergence Requirements

- Below 50 m/s

ZERO PACKET LOSS

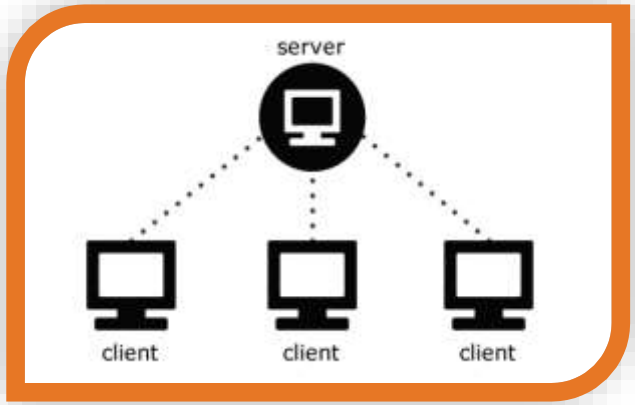
- Process Bus

Fullback Mode & Isolated Site Operation

- Substation has to run if Isolated

Industrial Protocols

- GOOSE –L2 Multicast
  Other Protocols etc.



Static Clients

SCADA Servers Require Permanent Connections to Assets

The Core Security Framework

- Critical Infrastructures Need to Be Cyber Protected
- Each Industry Has Its Own Specific Security Standards
- Each Region Has Its Own Specific Security Standards
- The Core is to Provide Control Systems Protection

These are Fundamental Security Core Components That are Common Between all Standards and Frameworks

Make Compliance work for you.

Don't work for Compliance!

Standards & Frameworks

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC CIP

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The Instrumentation, Systems &Automation Society

ISA

IEC 62443

IEC International Electrotechnical Commission

Cyber Security – Core Components

Security Recovery:
- Rectifying the Security Incident
- Identifying Corrective Measures
- Update Security Implementation
- Update Security Policy
- Updating Threat Database
- Final Reporting

Incident Response:
- Responding to Threats
- Intrusion Prevention
- Isolating Threats & Confining Them
- Identifying Exposure
- Communicate to Respective Parties

Security Assessment:
- Identify what to Protect
- Assess the Threat
- Identify Security Holes
- Establishing an Initial Security Baseline

Security Implementation:
- Develop a Security Roadmap
- Implement Security Measures
- Reassess Security
- Verify Security – Pen Testing
- Establishing a New Security Baseline
- Establishing a Security Policy
- Security Training

Security Monitoring:
- Continuous Security Health Monitoring
- Intrusion Detection and Anomaly Detection
- Analysing Trends and Utilizing Threat Intelligence

NERC – CIP


NERC – CIP – V5
BES Cyber System Identification - CIP–002–5
Security Management Control - CIP–003–5
Personnel & Training -CIP–004–5
Electronic Security Perimeter - CIP–005–5
Physical Security - CIP–006–5
System Security Management - CIP–007–5
Incident Reporting and Response Planning - CIP–008–5
Recovery Plans for BES Cyber Systems - CIP–009–5
Configuration Change Management - CIP–0010–5
Information Protection - CIP–0011–5

CIP-004-5 (Personnel and Training)

Security Awareness Training

Security Training Program

7 Years Criminal Background Check!

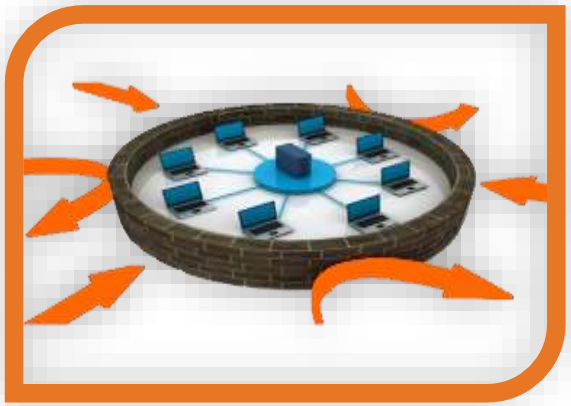
Security Policy Training

Timely Access Revoke and Audit

Access Authorization

CIP-005-5 (Electronic Security Perimeter)

Security Perimeter



Electronic Security Perimeter
External boundary of the BES Cyber System

- Identify Electronic Security Perimeter & Remote Access Connection Points

- CIP V5 Focuses on Security Perimeter as Opposed to Electronic Access Points
- Electronic Security Perimeter Shall Restrict Access to Authorized Users, Withstand Cyber Attaches and Contain any Possible Breach

Remote Access

- Identification & Multi-Factor Authentication
- Authorization with Privilege Level Assignment
- Session Encryption
- Session Logging

CIP-007-5 (Systems Security Management)

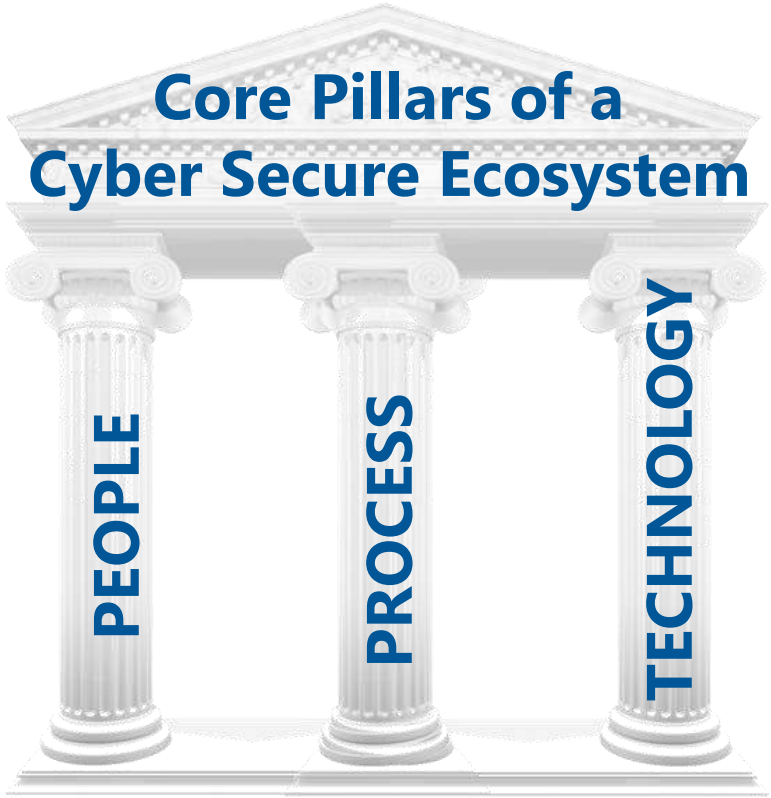
Minimize Attack Surface

Patch Management

Malicious Code Prevention

Password Management

Cyber Secure Culture



People

Qualifications
- Competency
- Training
- Situational Awareness

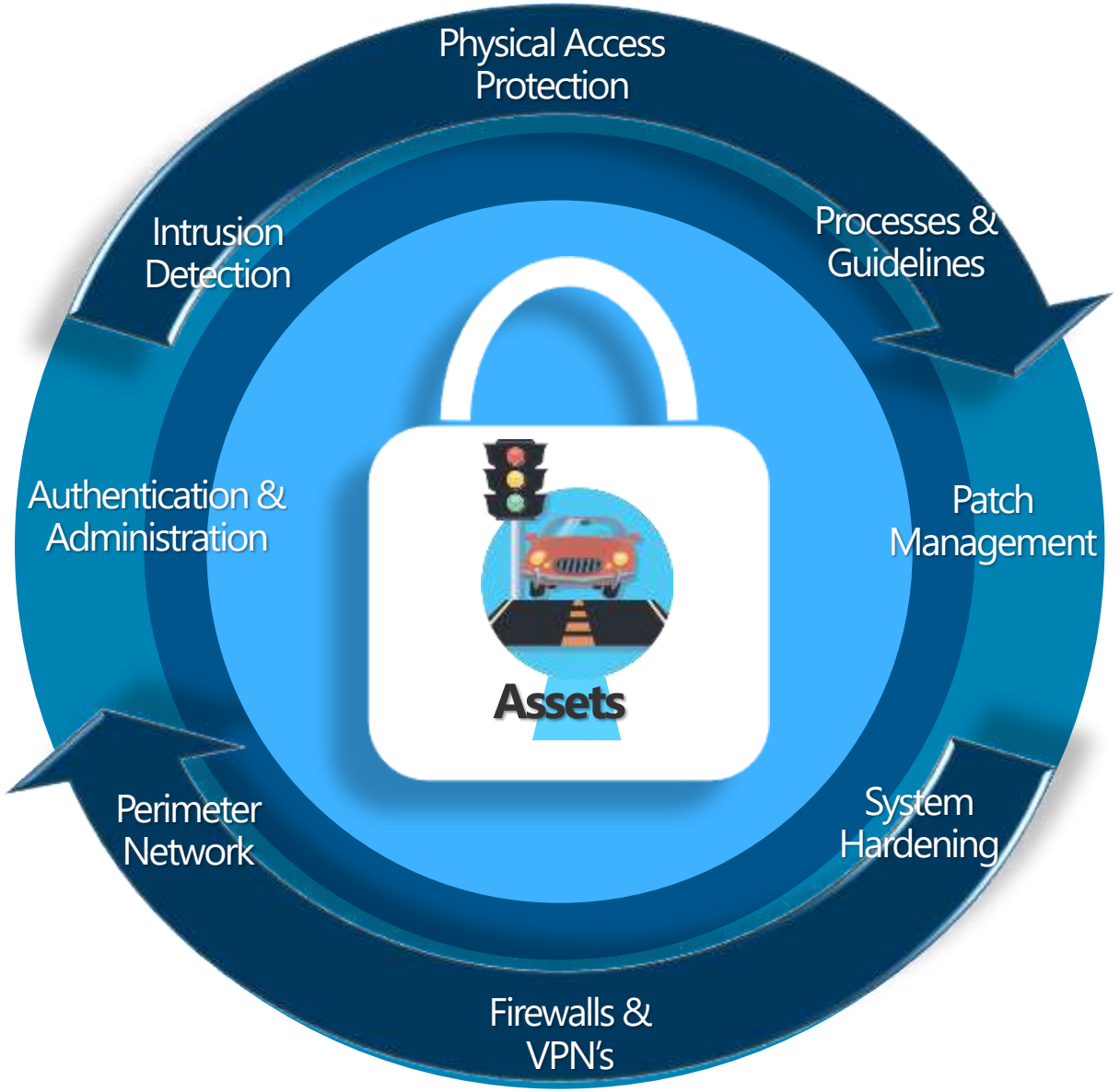
Process

Governance & Compliance
- Documentation
- Remediation
- Recovery
- Training

Technology

Tools & Utilities
- Control
- Monitor
- Tracking & Logging
- Patch Management

Defense In Depth



Standards & Frameworks

WCCD

ISO 37120

http://www.dataforcities.org/wccd/

https://www.iso.org/obp/ui/#iso:std:iso:37120:ed-1:v1:en

IEEE

Advancing Technology for Humanity

https://standards.ieee.org/develop/project/2784.html

Questions

Eric Labrie
Canadian Regional Sales Manager
ericlabrie@is5com.com
514-242-9827

Raptor for Defense in Depth in Industrial Control Systems

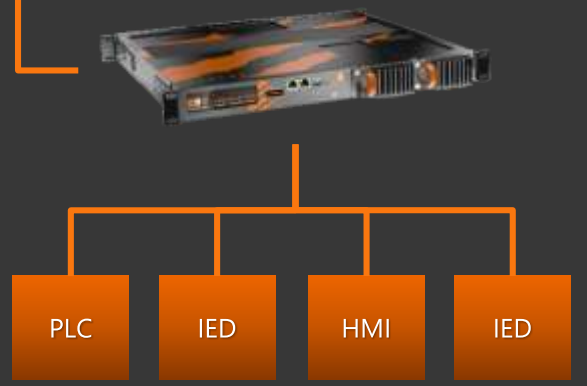
Advanced ICS Network Security Monitoring Software IDS

SpyGOOSE

NERC CIP

Features

- Integrated SCADA Network Security Monitoring Software with iS5Com.
- **Supports IEC61850 GOOSE, DNP3, Modbus, All Layer 2 Traffic**
- Supports Alert format, Syslog or UDP
- Supports Inbound Ports (At least one): stop/scup/sash (TCP22)
- Supports Outbound Ports: Syslog (TCP/UDP514)



According to NERC (North American Electric Reliability Council) CIP (Critical Infrastructure Protection) Version 5, systems communications must be audited. Any changes to the network must be run through change management and must be appropriately documented. SpyGOOSE will monitor for new devices added to the network and will automatically detect what ports they are using or serving. This documentation could be critical to providing NERC CIP compliance.

iS5 COMMUNICATIONS

Raptor for Defense in Depth in Industrial Control Systems

CYBEATS

Secure Protect Fix

HTTPS
TLS 1.2

Web Client

Device Management Dashboard

Features

Agent - Sentinel
The Agent detects threats invisible to network-based protection – even the most advanced unknown threats and remove them with surgical precision.

Monitor for vulnerabilities in software dependencies
Most vulnerabilities in IIoT devices come from third-party software dependencies. Cybeats continuously monitors for new vulnerabilities and alerts both manufacturers and users who are affected.

Anomaly detection and intrusion prevention Cybeats automatically learns which IPs and ports an IIoT device normally communicates with any exceptions to normal device behavior or traffic are flagged, alerts are generated, and all pertinent details are recorded.

Cybeats Agent running natively in Raptor (Optional)
- Firmware OTA Module
- Cyber Poling & Detection Module
- Telemetry Collection Module

HTTPS
TLS 1.2
AES 265

Cybeats Cloud Local or Provider
- Dashboard Service
- Cyber Analytics Service
- Cyber Learning Service
- Secure Firmware Distribution Service
- Device Health Monitoring Service
- Telemetry Real Time Aggregation Service
- Threat Intelligence Service
- Device Enrollment Service

Data Tier

Integrations
- Threat Intelligence

Offline Reporting Services

Hybrid cloud architecture
The Cybeats solution can be deployed either with our cloud infrastructure, or within an on premise data center for critical infrastructure customers and air-gapped environments that do not allow connectivity to the public Internet.

Dashboard Visibility – Ease of Use
Real-time alerts as soon as threats are identified, or fixes are deployed.

Secure distribution of firmware updates When a manufacturer updates its device's firmware, Cybeats notifies users and gives them choices for when and how to do the upgrade. The firmware is securely delivered through the Cybeats dashboard, thus keeping it out of the hands of hackers. Users can track their update status by device and see if an update has failed, and why

Future proof
Rather than depending on databases of known threats and vulnerabilities to protect IIoT devices, Cybeats automatically builds and maintains dynamic models of healthy device behaviors. This allows for any unusual behavior to be detected, making it ideal for identifying new and unknown threats.

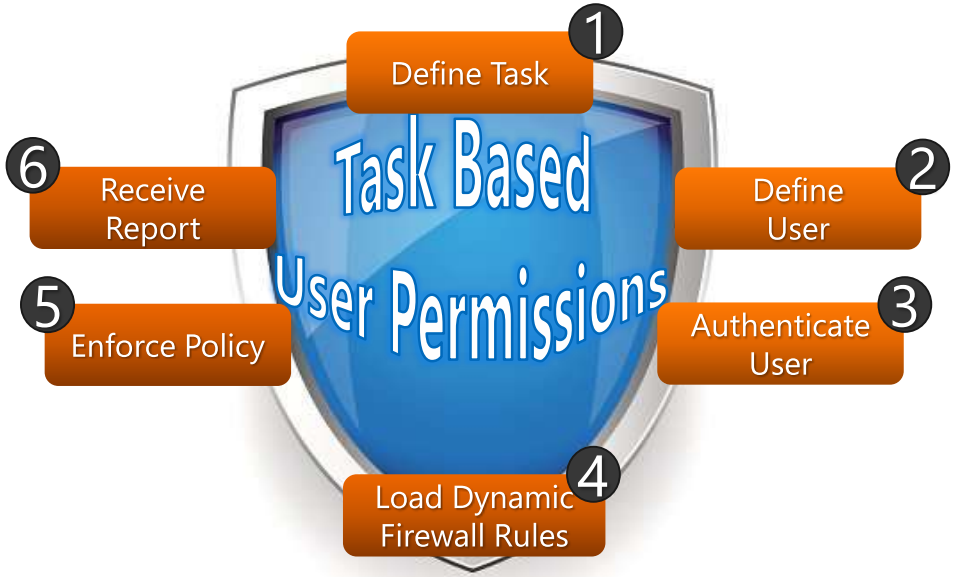
IS5 COMMUNICATIONS

Raptor for Defense in Depth in Industrial Control Systems

iPA (Intelligent Proxy Authentication)

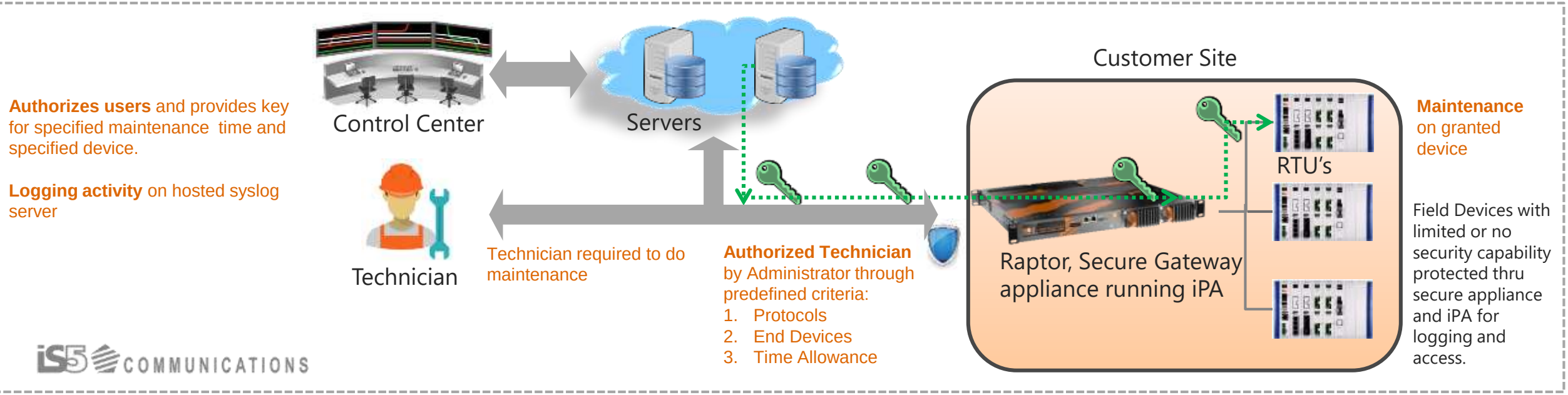
Features

- Supervising maintenance operations and preventing unauthorized access to devices even with no self authentication abilities



The Solution:

- *Access policy per maintenance* task, per user, per time, etc.
  - Restricted access to site devices
  - Applied both to IP and Serial communications
  - Full Audit Log of user activities
  - IPsec VPN for inter-site connectivity



iS5 COMMUNICATIONS

Raptor for Defense in Depth in Industrial Control Systems

Secure BOOT

BootUP

Prevent un-validated code from executing

The secure boot process detects unauthorized modifications to OEM software and system configuration information (such as device trees or certificates) at boot time, and when detected, the unauthorized code is prevented from booting.
At runtime, Trust Architecture supports detection of unauthorized modification of software or other memory contents via the Runtime Integrity Checker

Protect persistent and ephemeral device secrets against extraction or exposure

Persistent secret values programmed into the Security Fuse Processor (OTPMK and Secure Debug Response Value) cannot be extracted by any means short of physically de-processing the device. In devices with battery backed low power section, the Zeroizable Master Key cannot be extracted or exposed once provisioned (read lock set). Once initialized, the special ephemeral keys, including Job Descriptor Key Encryption Keys, Trusted Descriptor Signing Keys, cannot be extracted or exposed.

Protect persistent and ephemeral device secrets against mis-use

Upon detection of a security violation, persistent secrets are locked out until the next device reset which passes secure boot with no hardware security violations. The exceptions to this are;
Secure Debug Response Value: Only locked out by 3 failed debug challenge/response cycles.
Zeroizable Master Key: Security violations configured as ‘fatal’ zeroize the ZMK rather than locking it out. Ephemeral secrets are always cleared on the detection of a security violation.

Support strong partitioning

The private resources of one software partition must not be accessible by another software partition

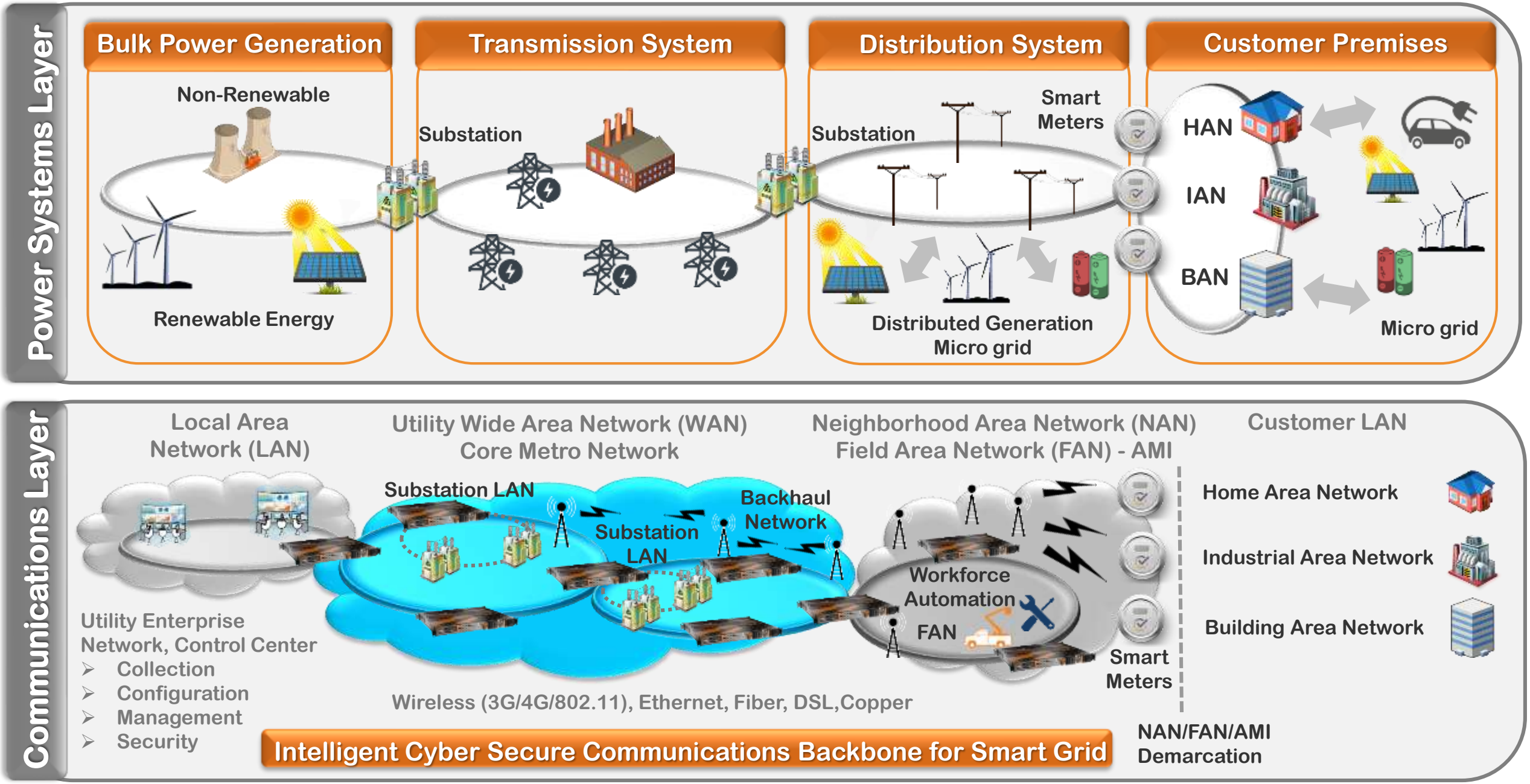
Features

Raptor is uniquely built from Ground up with “Trust Based Architecture” Hardware.

Why Secure Boot?

Most Communications systems are designed without Trust Based Architecture, unable to detect malware during the Boot sequence. “The system will load up trusted and untrusted firmware.”

Smart Grid Communications Architecture



Traditional Substation

Evolving Substation

Serial/Analog/ Legacy Communications

WAN – TDM/SONET, Modem, Microwave

Control Room

WAN

IP/Ethernet

Substation Automation, SCADA, Protocol Gateway

SCADA & HMI

Station Controller

Gateway

DNP, Modbus, Profibus

Relays

Relays

Hardwired Switchgear CT's and VT's

L2/L3 Ethernet Switch

HMI

Station Controller

L2 Ethernet Station Bus

IED's

IED's

Hardwired Switchgear CT's and VT's

Future – Digital Substation

IEC 61850 substation

Substation Automation, SCADA

Control Room

Energy APP Ecosystem

Cyber Security

SCADA/HMI Automation

Data Analytics

Sub Station Controller

Raptor Series Platform

SCADA Secure Gateways

HMI

Station Bus
IEC 61850-8-1

- Client/Server (MMS)
- GOOSE
- Time Sync (SNTP)

Redundancy Protection

IED's

RSTP/PRP Layer

IED's

Process Bus
IEC 61850-9-2

iSG18GFP

iSG18GFP

- GOOSE
- Sampled Values
- IEEE 1588 V2

RSTP/HSR Layer

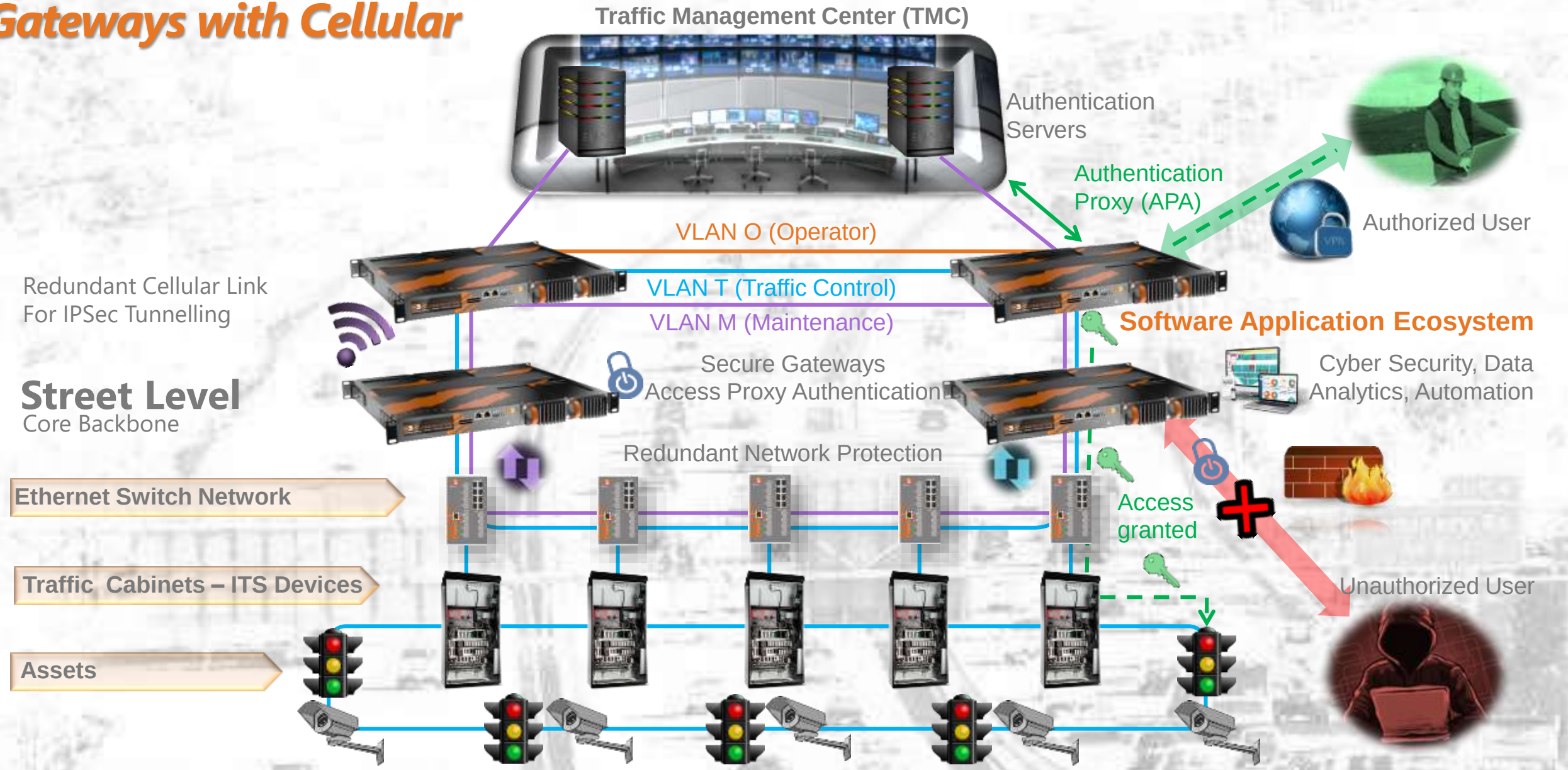
Merging Unit

Merging Unit

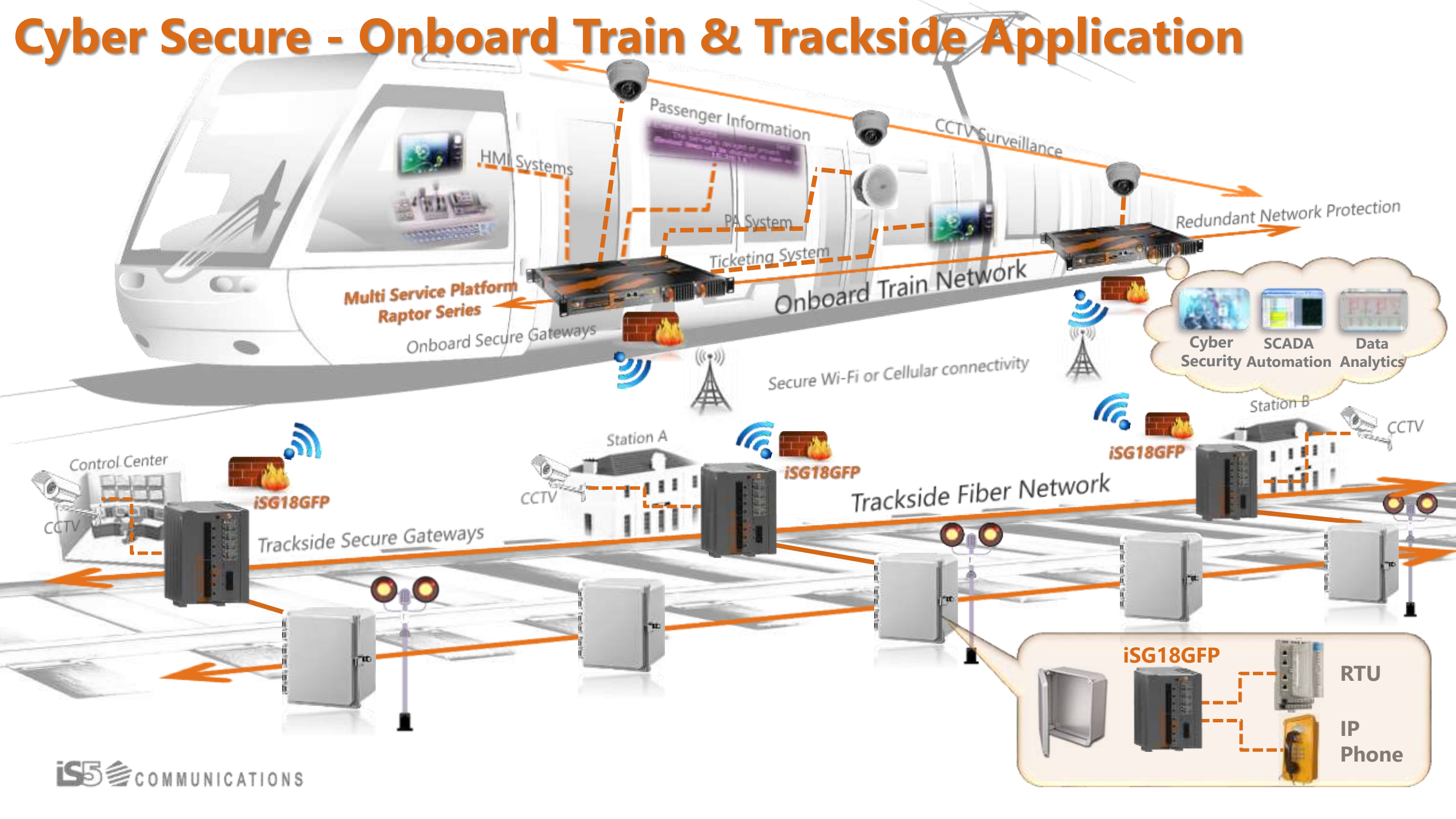
Intelligent Switch Gear

CT's and VT's

Cyber Security for ITS Application - *Redundant Secure Gateways with Cellular*



Cyber Secure - Onboard Train & Trackside Application



iS5 COMMUNICATIONS

Cyber Security for Waste Water Treatment - *Redundant Secure Gateways with Cellular/WiFi*