Check Point
SOFTWARE TECHNOLOGIES LTD.

CRITICAL INFRASTRUCTURE and INDUSTRIAL AUTOMATION SECURITY

Preventing the Kill Chain in **Industrial Control Systems (ICS) / SCADA**

ONE STEP AHEAD

Mati Epstein
Global sales manager
Critical Infrastructure and ICS

Industrial Control Systems (ICS)/SCADA are All Around Us

Check Point
SOFTWARE TECHNOLOGIES LTD.

Water & Sewage

Electricity

Transportation

Critical manufacturing

Industrial Automation

Oil & Gas

Building Management

… and we **rely on it every day** for our basic functions and needs.

Facts and Reality

Check Point
SOFTWARE TECHNOLOGIES LTD.

Dec 2014

German Steel Mill was hacked by Spear Phishing – Massive damage to the factory

Dec 2015

Blackout across western Ukraine due to BlackEnergy Spear Phishing malware attack (And again on January 19th)

March 2016

Hackers breached a water utility's control system and changed the levels of chemicals being used to treat tap water (Kemuri Water Company)

Most recent news

Check Point
SOFTWARE TECHNOLOGIES LTD.

June, 2017

NotPetya Ransomware hits Ukraine's power distribution company, Mearsk and other's OT infrastructure

July 16th, 2017

Energy sector hacking campaign targeted more than 15 U.S. firms

(Cyberscoop)

December, 2017

Triton Malware - Affecting S.E. Triconex Safety Controllers, which are used widely in critical infrastructure . Threat actors deployed malware capable of manipulating emergency shutdown systems

(Schneider Electric)

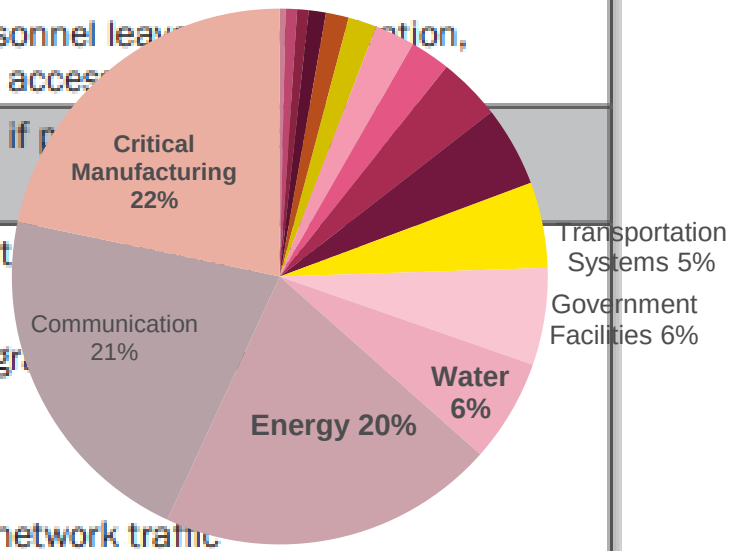
US ICS-CERT report: (Jan-18)

FY 2017 Most Pre nesses

3rd year in a row

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leav tion, especially sensitive for users with administrator acces
Allocation of Resources	3	• No backup or alternate personnel to fill position if r • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment opportunity to: ○ Maliciously modify, delete, or copy device progr ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

Most Attacked Sectors 2016



WHO ARE THE

ATTACKERS?

EXAMPLES OF
INDUSTRY ATTACKS
OVER THE
PAST YEARS

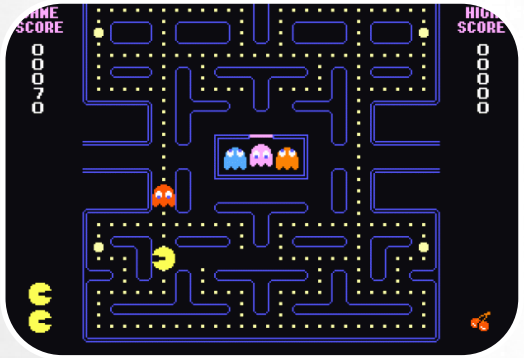
State Actors
BlackEnergy, CrashOverride

Insiders
Maroochy County Sewage

Teenagers
Lodz Tram

Activists
Operation Green Rights

Why Are These Attacks Possible?



Legacy System

Default Configuration

Less/No Updates

Less/No Encryption

Policies & Procedures

Less/No Segmentation

Latency Concerns

Attack Vectors Reaching the OT Network

Removable Media

Email Phishing and Attachments

Remote Technicians

Software Vulnerabilities

Guest Networks Unprotected Sockets

Securing against Attack Vectors

Attack Vector	Check Point solution
Removable Media	Endpoint data protection
Spear Phishing	Sandblast Emulation and Extraction
Ransomware	SandBlast Anti-Ransomware
Remote Technicians	Secured VPN Connectivity and Two Factor Authentication
Software Vulnerabilities	IDS/IPS
Virus's and BOT's	AV and AB Blades
Missing Boundary	Firewall and segmentation

Check Point
SOFTWARE TECHNOLOGIES LTD.

HOW CAN WE **SECURELY** AND **RELIABLY** STAY AHEAD?

ONE STEP AHEAD

Best Practices for Securing OT

Check Point
SOFTWARE TECHNOLOGIES LTD.

Secure Both OT and IT Environments

Protect IT with Advanced Threat Prevention Technologies

Clear Segmentation between OT and IT/Internet

Deploy Specialized ICS/SCADA Security Technologies

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Security Solutions for Industrial Control Systems/SCADA

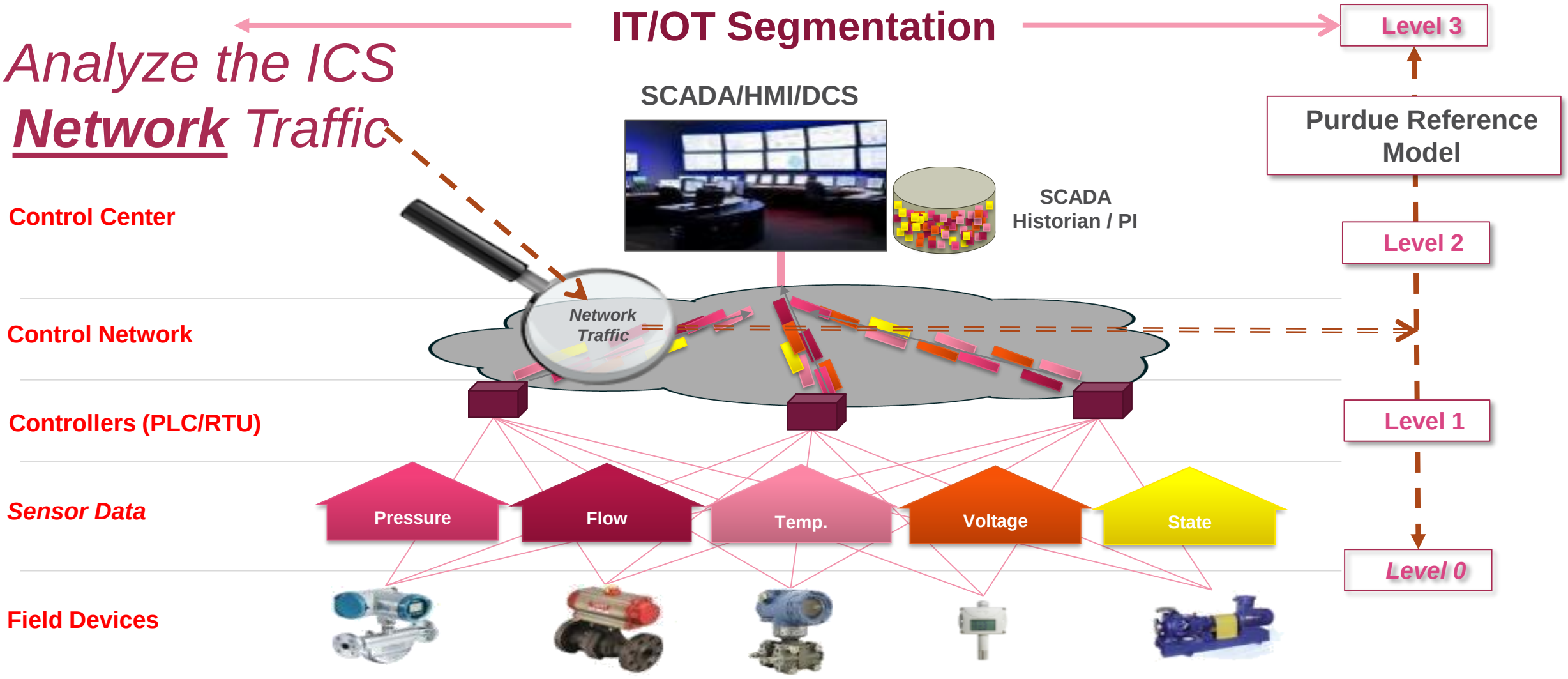
CYBER DEFENSE

- Visibility of ICS/SCADA Traffic
- **Enforcement of ICS/SCADA Traffic**
- SCADA-Aware Threat Prevention
- Ruggedized Appliances for Harsh Environments

Visibility

Real Time SCADA/ICS Network monitoring

Check Point
SOFTWARE TECHNOLOGIES LTD.



Enhanced OT Visibility

Check Point
SOFTWARE TECHNOLOGIES LTD.

Communication Information

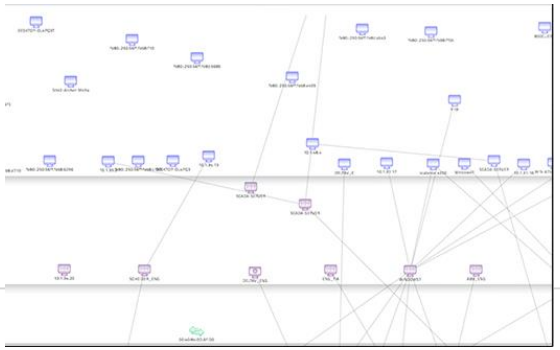
- Protocols & Commands
- Asset connections within the ecosystem
- Open/proprietary protocols

Asset Information

- IP and MAC Address
- Equipment vendor
- Equipment type (PLC, HMI, Engineering Workstation, Switch, etc.)
- Asset model name and Serial #
- Firmware version
- Physical data (rack slots)

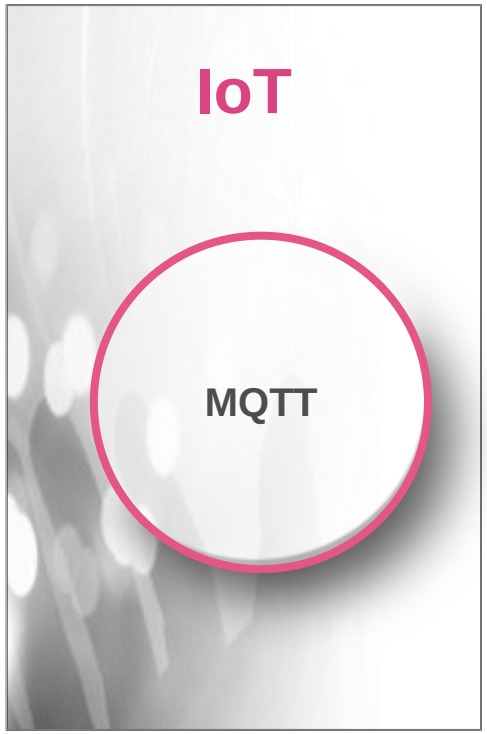
Network Mapping

- What assets you have on the network?
- How assets are communicating and who is accessing them?
- Uncover configuration issues and vulnerable assets



Visibility by SCADA Protocols and Commands

Check Point
SOFTWARE TECHNOLOGIES LTD.



MMS

CIP

Profinet

OPC
DA & UA

BACNET

IEC 60870-5-104

ICCP

MODBUS

IEC 61850

DNP3

Siemens
Step7

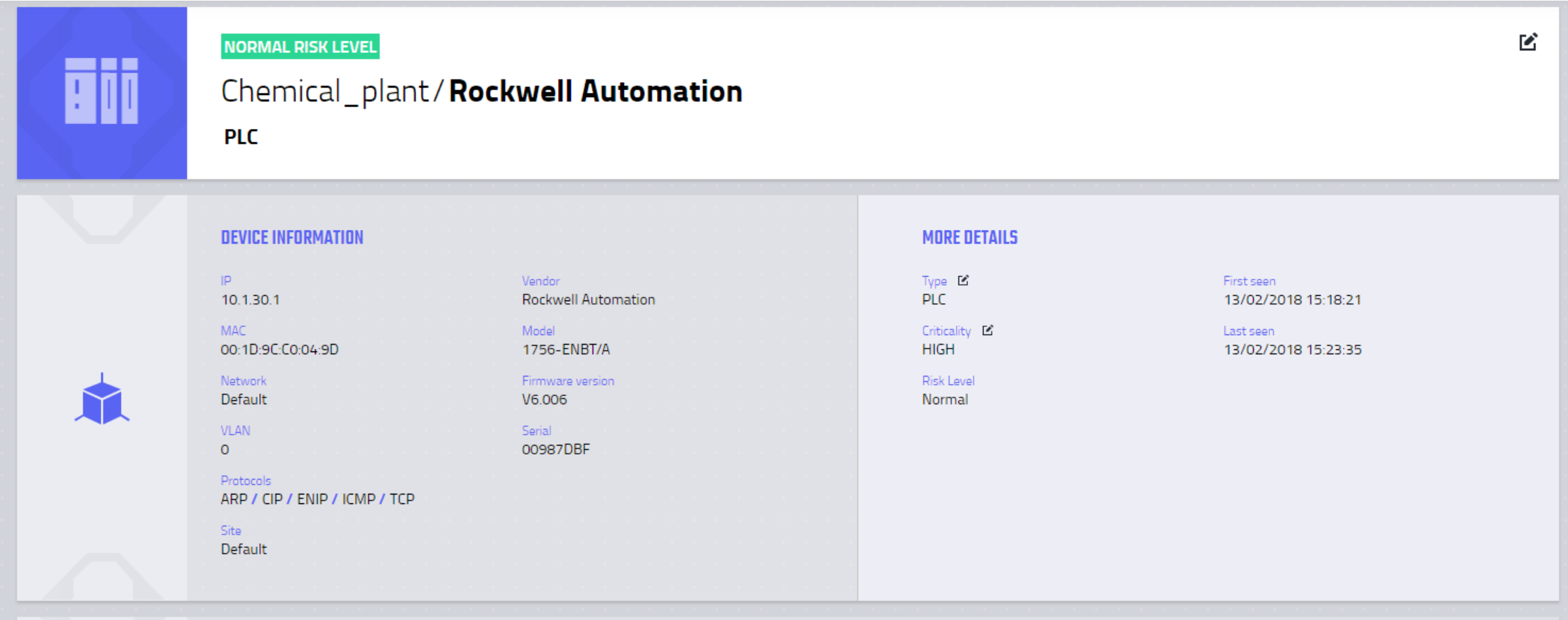
And many more…..

Over 1000 SCADA and IoT commands in Check Point Application Control

Updated list: appwiki.checkpoint.com

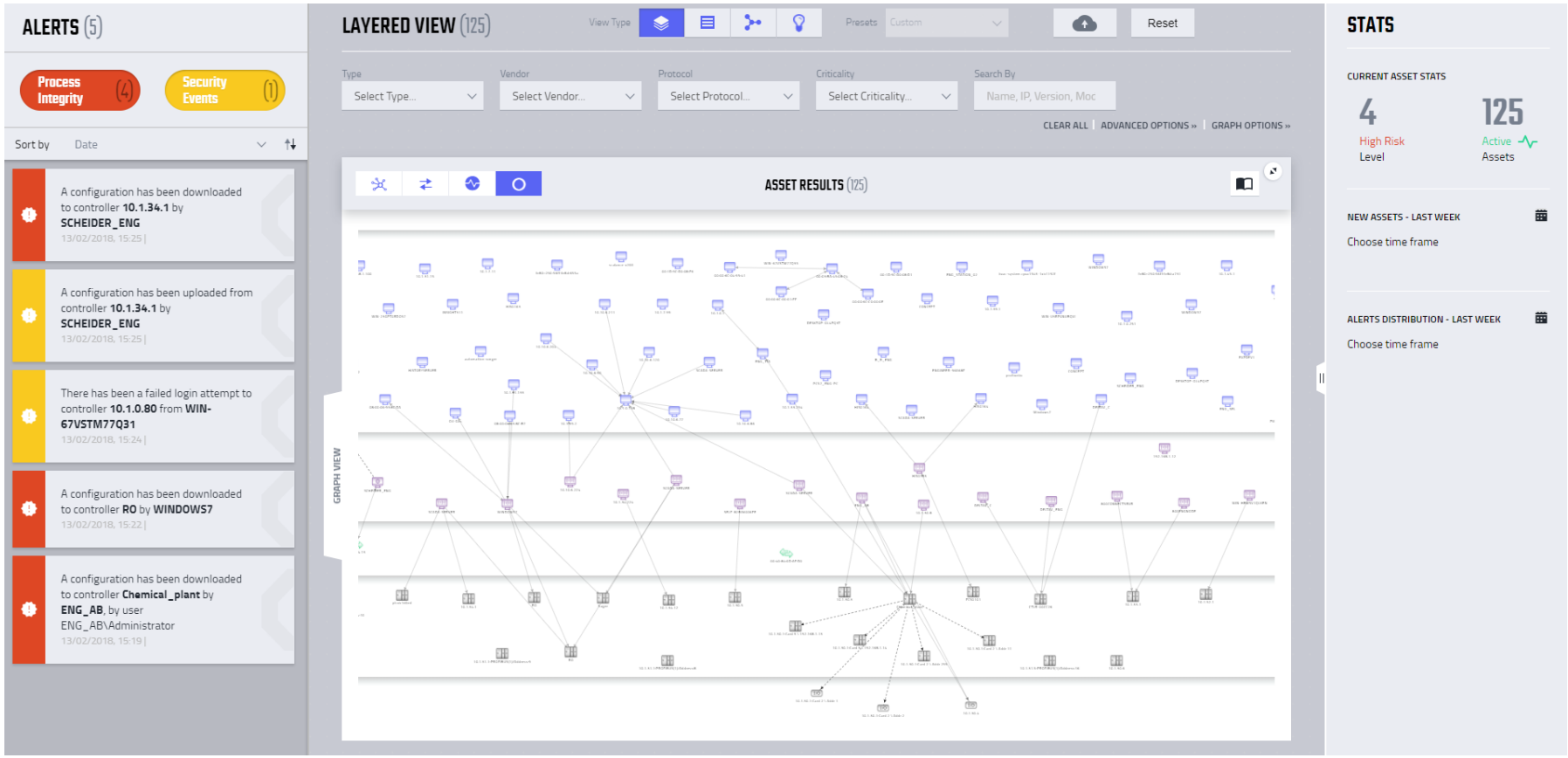
Asset information

Detailed asset information – Type, Vendor, Firmware and more



Assets View – by layered map

Asset layered view according to Perdue model, with variety of view options like neighbors assets, communication direction, ARP baseline and hide assets with no communication



Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Security Solutions for Industrial Control Systems/SCADA

CYBER DEFENSE

Visibility of ICS/SCADA Traffic

Enforcement of ICS/SCADA Traffic

SCADA-Aware Threat Prevention

Ruggedized Appliances for Harsh Environments

Enforcement

Check Point
SOFTWARE TECHNOLOGIES LTD.

Pre-defined Policies

- **Learning phase** - network traffic and logging
- Manual setting of SCADA commands baseline
- Specific Command policies
- Specific Values policies
- Time of Day and traffic patterns policies

Anomaly Detection

- **Learning phase** - Automatically Discover Assets and communication
- Anomaly-Based Behavior Analysis
- Generate High-Fidelity Baseline Model
- Generate security and process threats

Combined Enforcement of Pre-Defined + Anomaly-Based analysis

Setting the Baseline

Granular level logging of SCADA traffic –

Check Point
SOFTWARE TECHNOLOGIES LTD.

Detailed forensics for incident investigations

ANALYZED
by
Check Point
SMARTLOG &
SMARTEVENT

DETAILED

Time		B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matc...
Today	10:45:35				gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Pr
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Pro
Today	10:45:53				gw-71ec22	ModbusAll	33490	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33489	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33488	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33487	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33486	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53				gw-71ec22	ModbusAll	33485	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33484	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33483	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33482	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33481	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51				gw-71ec22	ModbusAll	33480	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot

GROUPED

Count	Source	Destination	Unit ID	Function Description
500	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Holding Registers
100	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Input Registers
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register

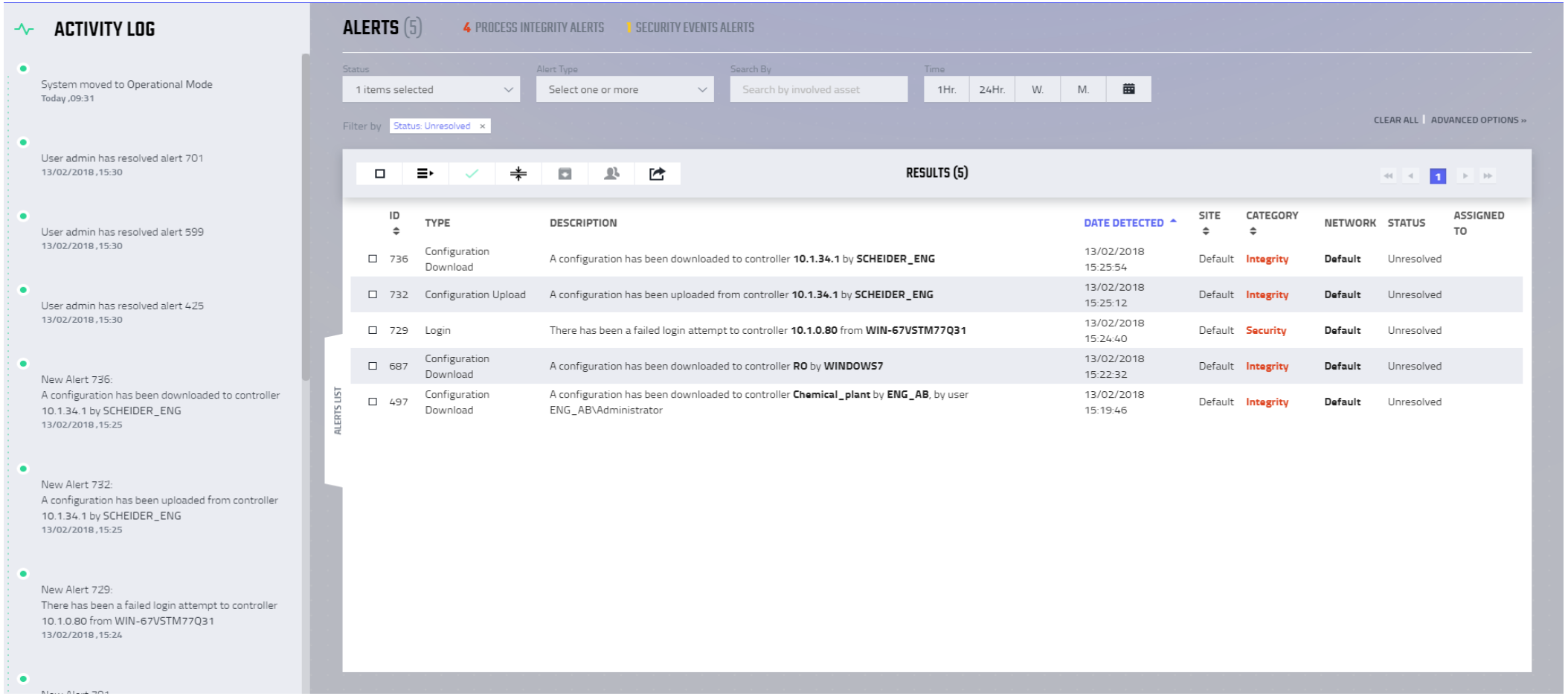
Manual setting of SCADA commands baseline

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track
1	0	baseline policy	HMI SCADA_Srv	PLC PLC_1 PLC_4	Modbus Protocol - read input register Modbus Protocol - read-write multiple registers Modbus Protocol - write multiple registers Modbus Protocol - write single register	Allow	Extended Log

- **Learning phase** – logging of network traffic
- Setting SCADA commands baseline
- Specific Command policies
- Passive (Alert) or optional Active (Block) policy

Alerts by Behavior Analysis

Alerts window with filtering capabilities and Alerts tree according to Process integrity and Security events



Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Security Solutions for Industrial Control Systems/SCADA

CYBER DEFENSE

Visibility of ICS/SCADA Traffic

Enforcement of ICS/SCADA Traffic

SCADA-Aware Threat Prevention

Ruggedized Appliances for Harsh Environments

Legacy Systems Are Often Unpatched

Check Point

SIEMENS

Siemens Global Website

ProductCERT Security Advisories

Siemens ProductCERT is the central team for respondin
security incidents and vulnerabilities related to Siemen
solutions and services. In the following, Siemens secur
bulletins issued by ProductCERT are listed.

2016

- SSA-751155 (Last Update 2016-04-08): Denial-of-Service Vulnerabilit
- SSA-623229 (Last Update 2016-04-08): DROWN Vulnerability in Indu
- SSA-301706 (Last Update 2016-04-08): GNU C Library Vulnerability i
- SSA-151221 (Last Update 2016-03-18): Incorrect File Permissions in
- SSA-833048 (Last Update 2016-03-14): Vulnerability in SIMATIC S7-1
- SSA-253230 (Last Update 2016-02-08): Vulnerabilities in SIMATIC S7
- SSA-743465 (Last Update 2016-01-15): Cross-Site Scripting Vulnerai OZW772

2015

- SSA-472334 (Last Update 2015-12-18): NTP Vulnerabilities in RUGG Devices
- SSA-763427 (Last Update 2016-04-29): Vulnerability in Communicatio modules SIMATIC CP 343-1, TIM 3V-IE, TIM 4R-IE, and CP 443-1
- SSA-921524 (Last Update 2016-04-29): Incorrect Frame Padding in F
- SSA-720081 (Last Update 2015-09-01): IP Forwarding in RUGGEDC Devices
- SSA-134003 (Last Update 2015-08-27): Web Vulnerability in S7-1200

Life Is On Schneider Electric

all the site

Solutions

Products a

Support

You are here: Home > Support > Cybersecurity > Vuln

Securi

World presence

Customer Care Centre

- Contact

Cybersecurity

- News
- Report an incident

Substitution tool

Counterfeiting

- Counterfeiting
- Definitions
- Report a counterfeit

Idea Submission

Date (dd/mm/yyyy)				
14/03/2016				
12/03/2016				
29/02/2016				
17/02/2016				
04/02/2016				
25/01/2016	StruxureWare Building Operations	Weak Credentials and OS Command Injection	Automation Server series (AS, AS-P), V1.7 and prior	SEVD-2016-025-01
20/01/2016	Altivar Drives	Modification of Drive Parameters	See disclosure	ST03406
11/01/2016	MiCOM C264	Integer Overflow	See disclosure	SEVD-2016-011-01
10/12/2015	M340 PLC	Buffer Overflow	See disclosure	SEVD-2015-344-01
25/11/2015	ProClima SW	Remote Code Execution	ProClima, all versions prior to V6.2	SEVD-2015-329-01

HOME • ABOUT • TECHNOLOGY • CYBER SECURITY • ALERTS AND NOTIFICATIONS

GLOBAL SITE - ENGLISH

Power and productivity for a better world™ ABB

Cyber security alerts and notifications

We are committed to providing our customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping our customers minimize risks associated with cyber security.

Latest alerts and notifications

Archived alerts and notifications

Subscribe to email alerts

Report a vulnerability

2015-12-10: POODLE Vulnerability in RTU500 Series
2015-12-10: POODLE Vulnerability in Relion 650 series Ver. 1.3.0
2015-12-10: POODLE Vulnerability in MicroSCADA Pro SYS600
2015-12-10: POODLE Vulnerability in SDM600 Ver. 1.1
2015-12-10: POODLE Vulnerability in AFx series
2015-12-10: POODLE Vulnerability in ETL600 series
2015-12-10: POODLE Vulnerability in ESP630 series
2015-12-10: POODLE Vulnerability in FOX660 series
2015-12-10: POODLE Vulnerability in Relion 615 series v5.0
2015-12-10: POODLE Vulnerability in COM600
2015-12-10: POODLE Vulnerability in Protection and Control IED Manager PCM600

2015-02-11: Security Bulletin for ABB 3rd Party Device Type Library HART DTM
2014-10-30: Advisory for ABB RobotStudio
2014-10-30: Advisory for ABB Test Signal Viewer
2014-04-24: (updated 2014-06-30): OpenSSL Heartbleed Vulnerability in Relion 650 series Ver. 1.3.0
2014-02-19: CMT 1000 Vulnerability bug fix
2013-11-06: Remote code execution vulnerability in CAP 501 / CAP 505 / SMS 510
2013-11-08: Remote code execution vulnerabilities in MicroSCADA
2013-10-17: Advisory for Test Signal Viewer on Windows for Robotics
2012-04-30: Advisory for AC500 web server
2012-03-23: Advisory for WebWare Components and Related Products
2012-02-28: Buffer Overflow in Robot Communications Runtime on Windows

Virtual patching

Over 300 dedicated IDS/IPS signatures

Check Point
SOFTWARE TECHNOLOGIES LTD.

Stops exploits of known vulnerabilities and detects anomalous traffic

PROTECTED by Check Point IPS

NSS Labs RECOMMEND

NSS Labs Highest Rating

Protection	Sever...
Citect SCADA ODBC Overflow Attempt	Medium
Rockwell RSLogix Denial of Service Vulnerability	Critical
SCADA Engine OPC Client Buffer Overflow Vulnerability	High
Schneider Electric UnitelWay Windows Device Driver Buffer Overflow	Critical
Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability	Critical
Siemens Automation License Manager Multiple Vulnerabilities	Critical
ScadaTEC SCADAPhone and ModbusTagServer Buffer Overflow	High
RealWin HMI Service Buffer Overflow 2	High
Automated Solutions Modbus/TCP Master OPC server Modbus TCP Header	High
RealWin INFOTAG/SET_CONTROL Packet Processing Buffer Overflow	High
Unauthorized Miscellaneous Request to a PLC	Critical
Broadcast Request from an Authorized Client	Critical
IGSS SCADA RMS Report Template WriteFile Command Buffer Overflow	Critical
IGSS SCADA STDREP Request Buffer Overflow	High
Iconics Genesis SCADA Freeing of Unitialized Memory Trigger	High
Rockwell RNA Message Negative Header Length	Critical
Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
WonderWare SuiteLink DOS Attempt	High

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT'S

Security Solutions for Industrial Control Systems/SCADA

CYBER DEFENSE

Visibility of ICS/SCADA Traffic

Enforcement of ICS/SCADA Traffic

SCADA-Aware Threat Prevention

Ruggedized Appliances for Harsh Environments

Check Point 1200R

New Purpose-Built Ruggedized Security Gateway Appliance

- **Fully** featured Check Point security gateway
- **6x1GbE ports** and firewall throughput of 2Gbps
- **Compliant** to the most rigid regulations:
  IEC 61850-3 and IEEE 1613
- **Compact fan-less** design with no moving parts; temperature range from -40°C to 75°C
- Can be used in **In-line** or **Tap (Mirror)** modes
- **Routing and networking** (e.g: BGP, OSPF, IPsec, etc.)

CrashOverride/Industroyer –
New ICS attack platform to Electric Grid Operations

- CrashOverride (called Industroyer as well) malware was the malware employed in the December 17th, 2016 cyber-attack on the Kiev, Ukraine transmission substation which resulted in electric grid operations impact. (As reported by ESET and Dragos)

- ICS-CERT reported on June 14, 2017 https://www.us-cert.gov/ncas/alerts/TA17-163A
  - The tactics, techniques, and procedures (TTPs) described as part of the CrashOverride malware could be modified to target U.S. critical information networks and systems.

- CrashOverride malware is an extensible platform that could be used to target critical infrastructure sectors, specifically using IEC104 and IEC61850 protocols.
  - The malware issues valid commands directly to RTU's.
  - Using Check Point protocols visibility and baselining would detect and alert on None-Baseline protocols and commands

- Could exploit Siemens SIPROTEC relay denial-of-service (DoS) vulnerability, leading to a shutdown of the relay.
  - Using CVE-2015-5374 to Hamper Protective Relays
  - Check Point published on June 20th an IPS signature for virtual patching protection of the DoS vulnerability

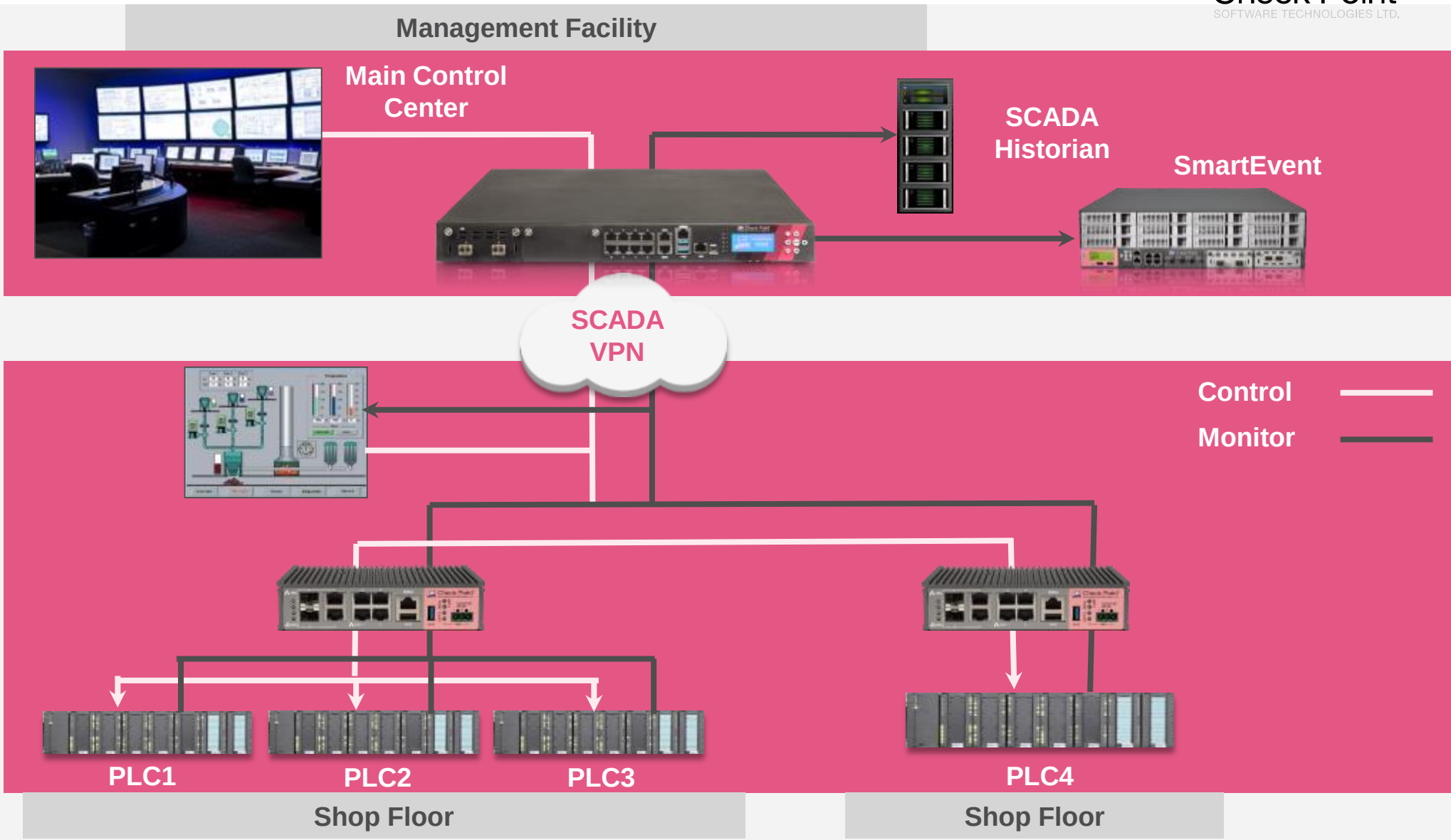
Check Point
SOFTWARE TECHNOLOGIES LTD.

CASE STUDIES

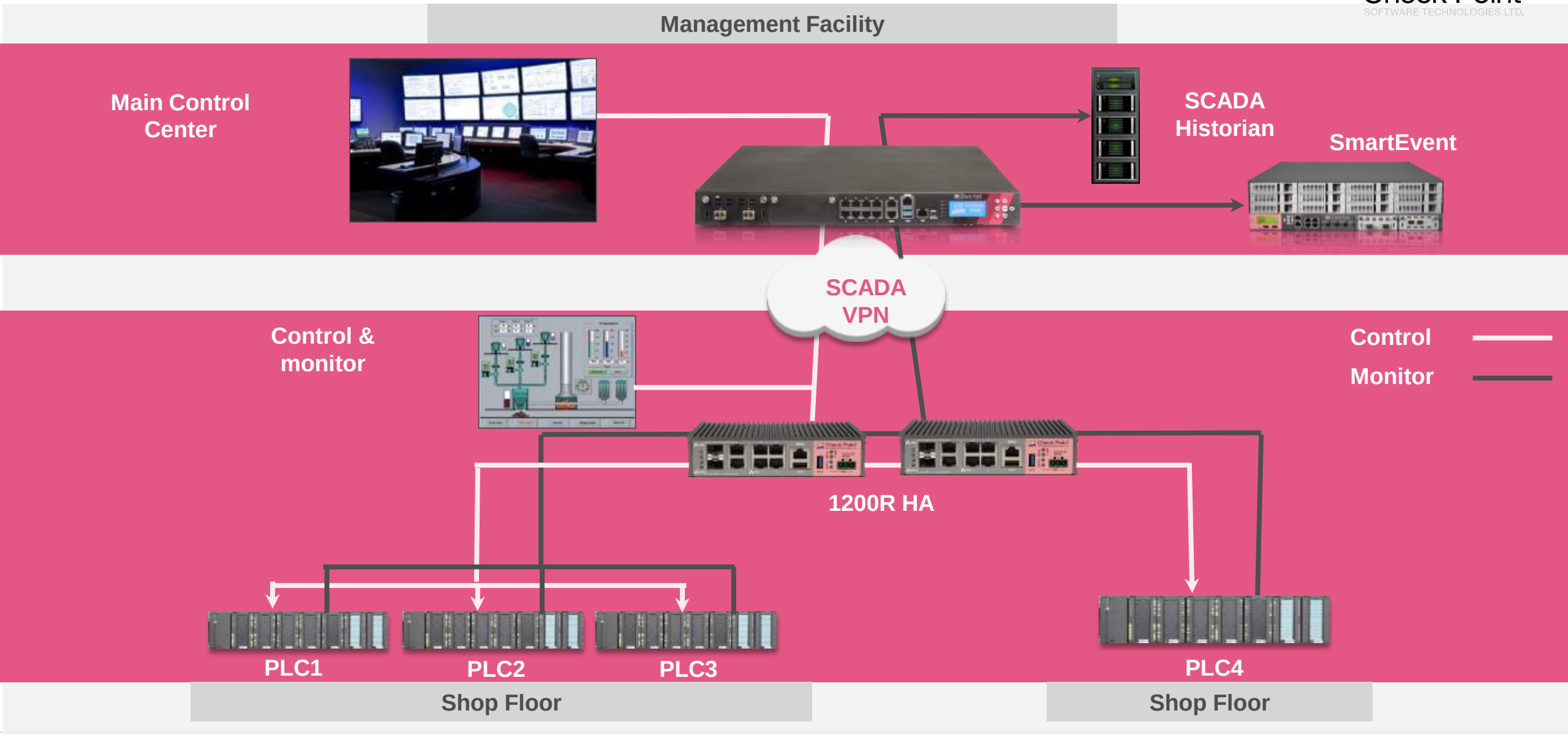
ONE STEP AHEAD

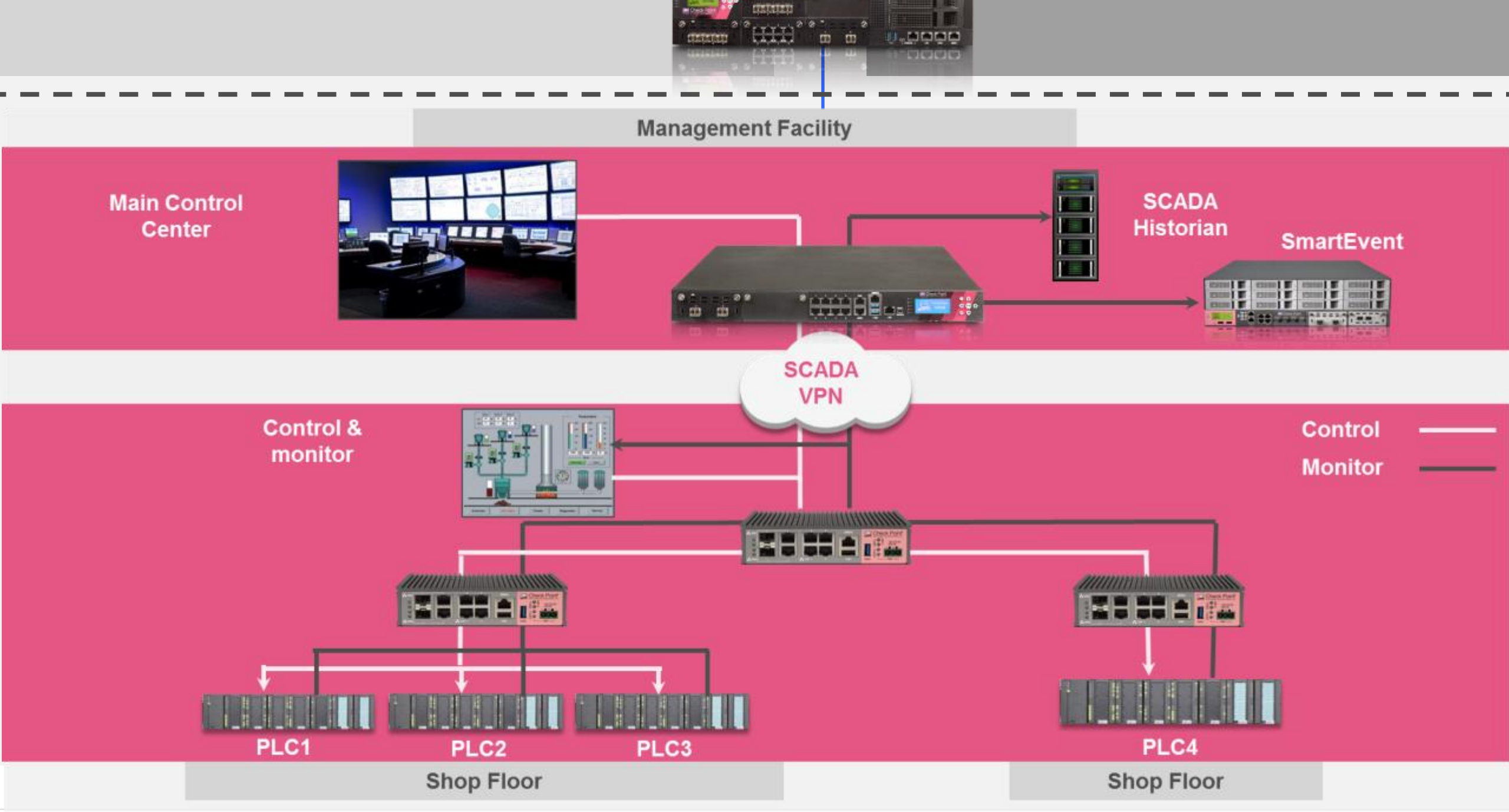
OT Security Blueprint – Micro Segmentation

Check Point
SOFTWARE TECHNOLOGIES LTD.



OT Security Blueprint – High Availability




Management Facility
Main Control Center
SCADA Historian
SmartEvent
SCADA VPN
Control & monitor
Control
Monitor
PLC1
PLC2
PLC3
PLC4
Shop Floor
Shop Floor

The Corporate Building (BMS)

Perimeter Segmentation

Functional Zone Segmentation

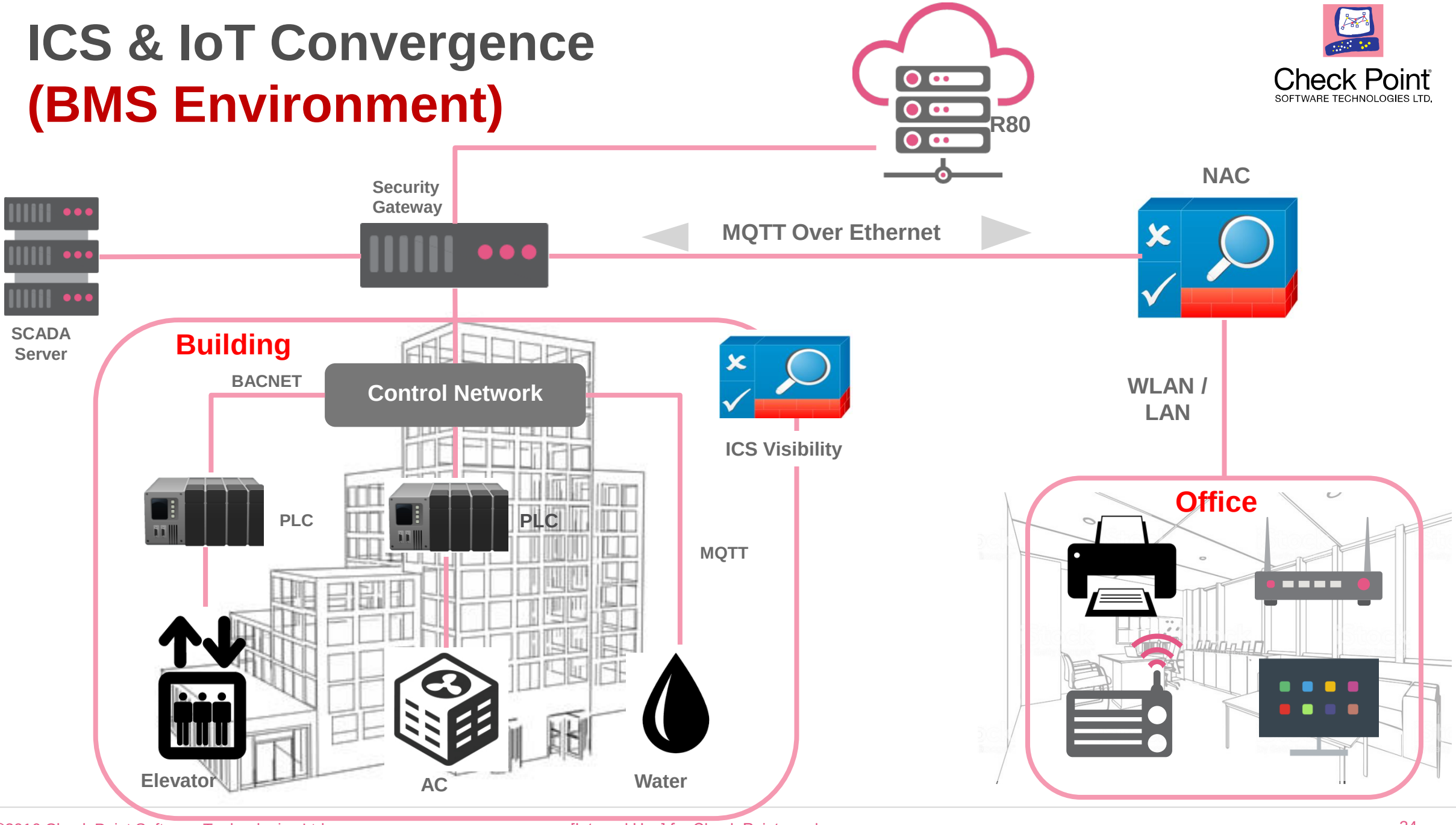
DPI of BMS Protocols

SCADA/IoT

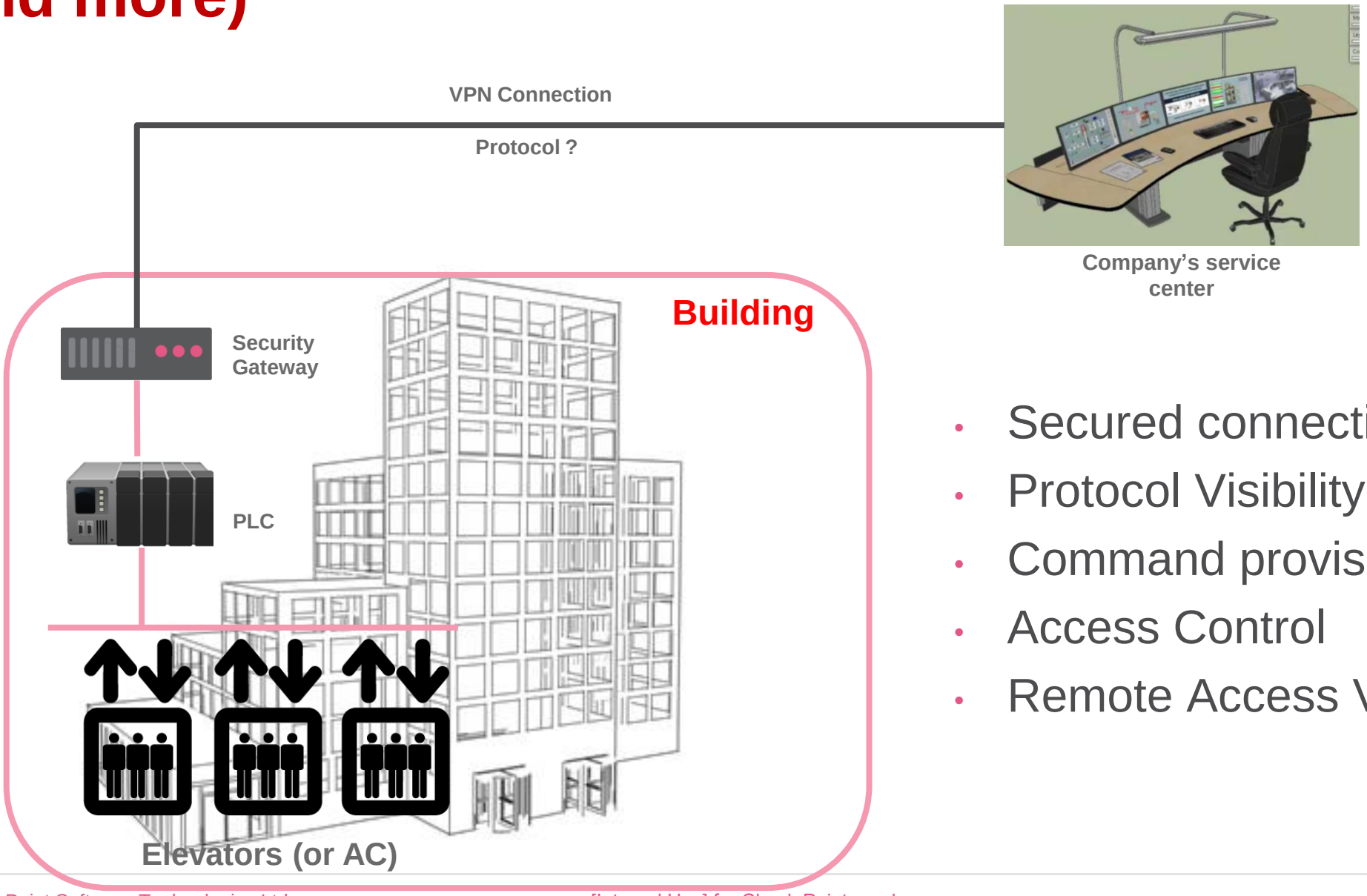
MQTT, BACNET

- Energy Management
- HVAC
- Lighting
- Elevators
- Access & Security
- Water
- And more…

ICS & IoT Convergence
(BMS Environment)



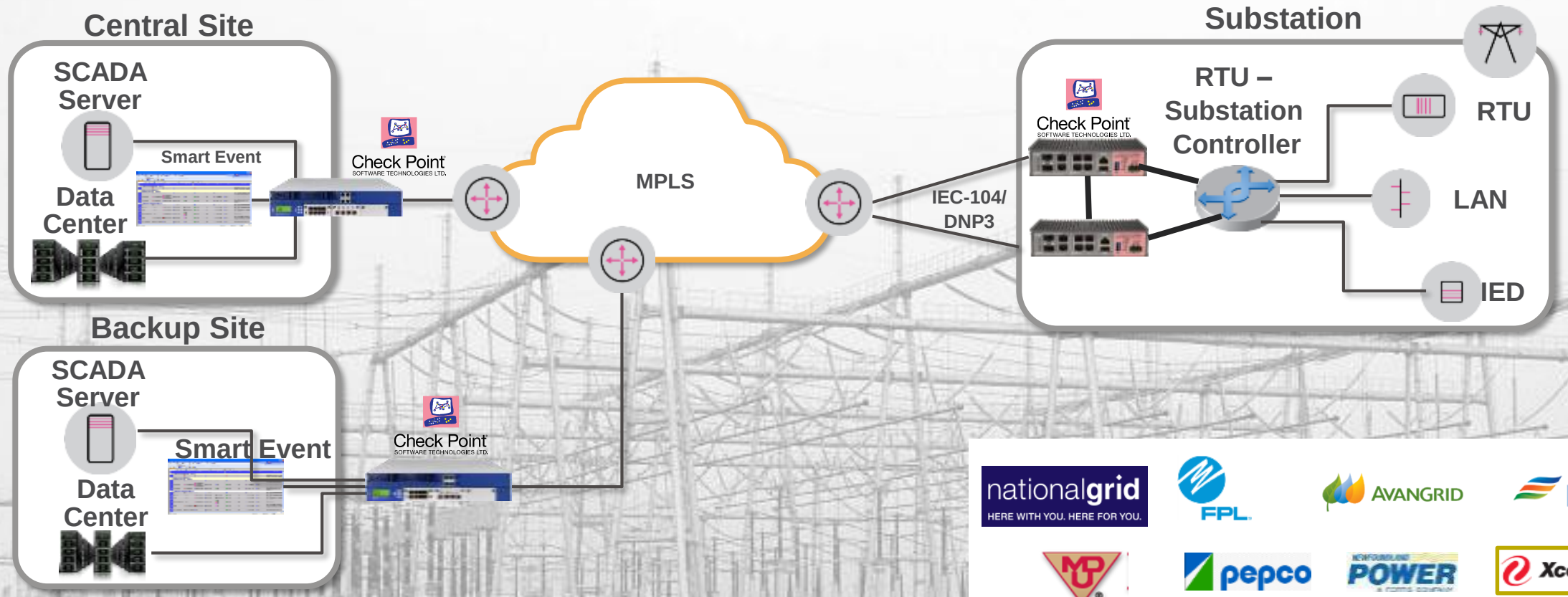
Remote Maintenance for Elevator or HVAC (and more)



- Secured connectivity (VPN)
- Protocol Visibility
- Command provisioning
- Access Control
- Remote Access VPN Client

Power Utilities — Substation Security

- Typical power utility security deployment in substations
- Single or cluster solution for combined OT and IT traffic
- SCADA security



Securing a Transmission System Operator (TSO) Control Systems

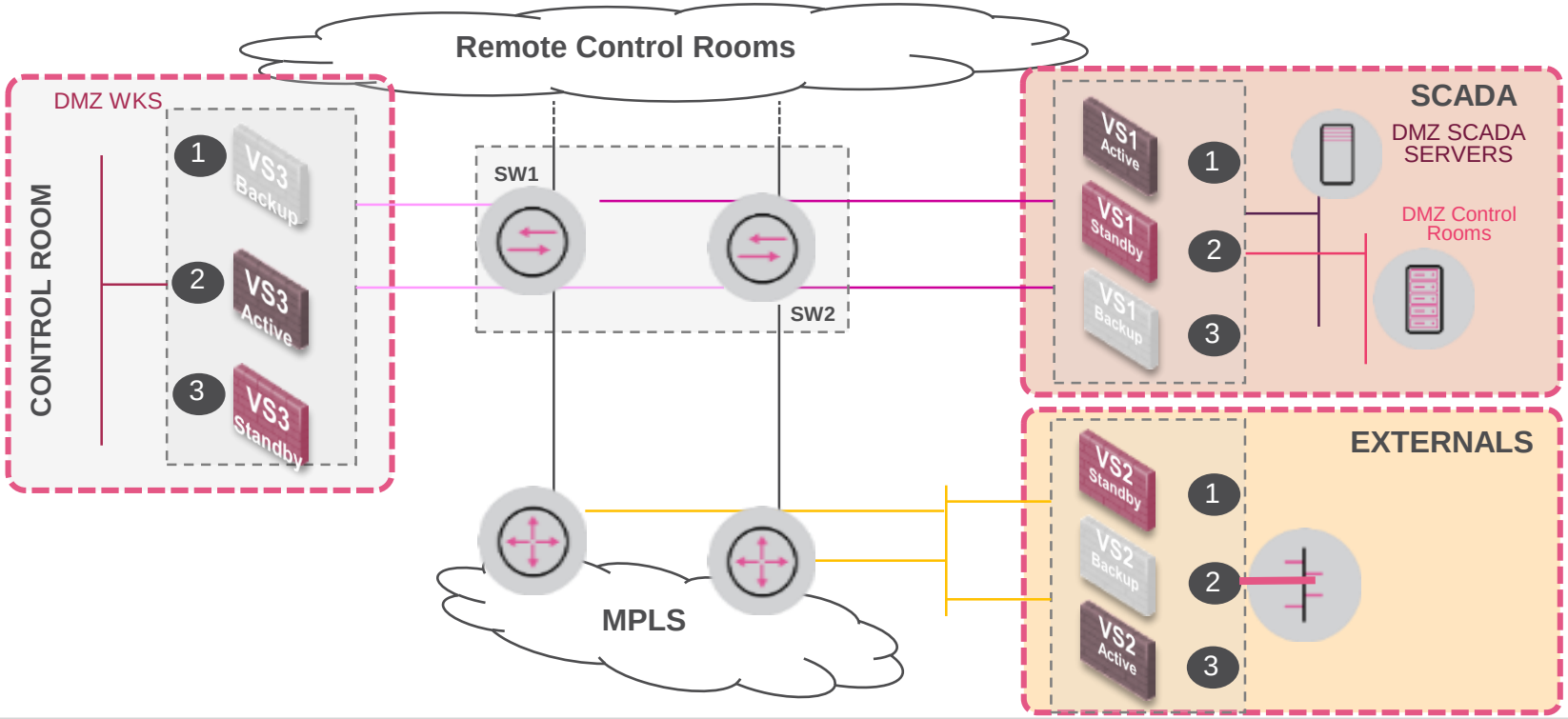
Check Point
SOFTWARE TECHNOLOGIES LTD.

Reasons to Choose Check Point

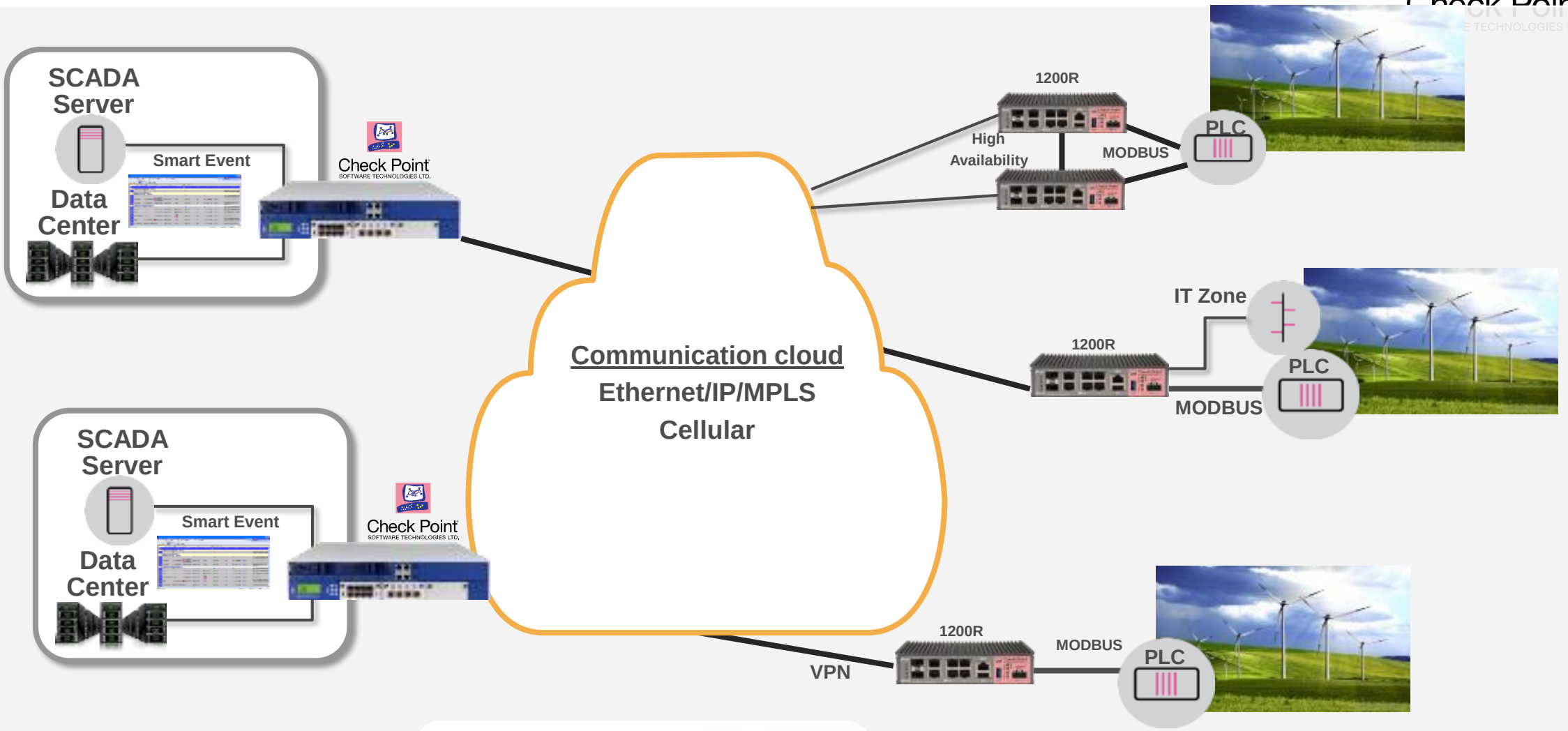
- Simple to manage
- Virtual Machine deployment
- Ability to granularly inspect SCADA protocols

Terna
e·on
HOPS
50hertz

- Each Data center is designed to control the entire national grid in case of failure of all the others
- Fully redundant topopolgy by 3 Firewalls per Data Center



Wind Farms Topology



innogy

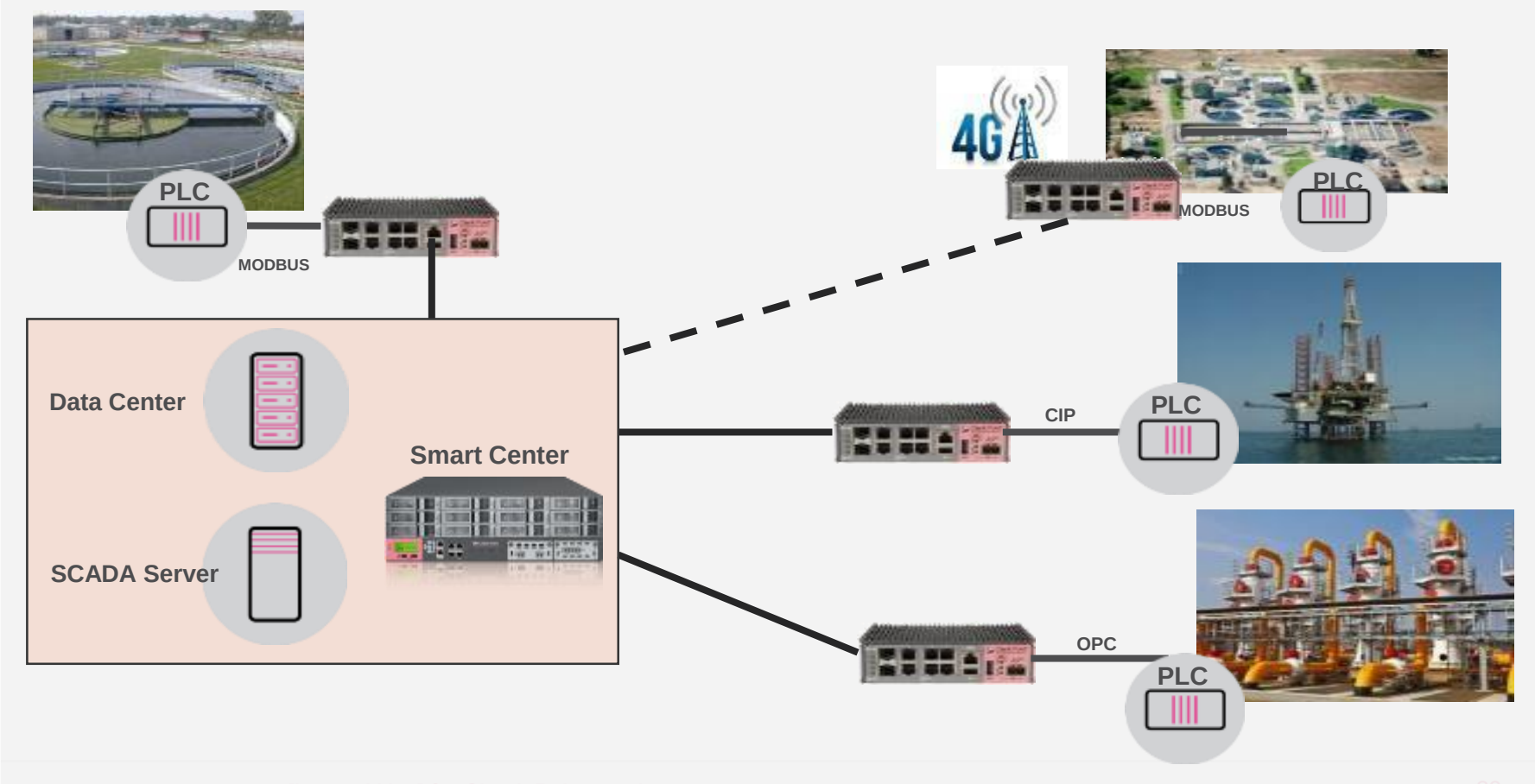
GENERG
ENERGIA NATURAL

CNR
Compagnie Nationale du Rhone

Waste Water Treatment Network

Applicable in Oil and Gas (Off/On-Shore)

- **Security Motivation –** New regulation for Critical Infrastructure
- **Challenge and CHKP Advantage –** Managing thousands of remote sites



UNIFIED IT and OT MANAGEMENT

FOR BEST ROI AND OPTIMAL PROTECTION

Customized Visibility

Unified Policy

Everywhere Monitoring

Management integration With Leading SIEM systems: Q-Radar, ARCSight, Splunk And more like Predix and others

Dedicated Compliance and Regulation Monitoring

Check Point
SOFTWARE TECHNOLOGIES LTD.

NERC CIP (v.5) Regulation Requirement CIP-007-5: Req. 3.1

Regulatory Requirements Details

- Description:
  Deploy method(s) to deter, detect, or prevent malicious code. [Taken from Requirement 7: Cyber Security - System Security Management]

Relevant Security Best Practices: 32 out of 39 items are secure

ID	Name	Blade	Status
AB106	Check the frequency of scheduled Malware Updates in the Anti-Bot blade	Anti-Bot	Secure
AB105	Check that the Malware Database is automatically updated	Anti-Bot	Secure
AV115	Check the frequency of the Anti-Virus database updates	Anti-Virus	Secure
AV114	Check that the Anti-Virus database is automatically updated	Anti-Virus	Secure
AV113	Check the frequency of scheduled Malware Updates in the Anti-Bot blade	Anti-Virus	Secure

SCADA SPECIFIC COMPLIANCE CHECKS

REPORTED
by
Check Point
COMPLIANCE BLADE

Real-time assessment of compliance with major regulations

Industrial Security Process

Visibility - Independently log all SCADA activity:

Network, Protocols, Commands, Values

Define Baseline and Policies

Set Rules based on Known / Unknown / Not Allowed or Anomaly Based Behavior Analysis

Detection - Identify Deviations and Attacks / Anomaly Detection

Based on the defined rules, time of day, attack patterns

Enforcement – Passive (Alert) / Active (Prevent)

Based on configuration and/or topology – In-line or Tap

Check Point Offering-
End to End Security suite for Critical Infrastructure IT and OT networks

Most extensive security support of ICS/SCADA protocols

Full OT to IT security segmentation

Large Scale Management – Market “Gold Standard” (Gartner)

Check Point offers complete security suite from Mobile, End-Point to the Cloud – including Private cloud for separation of IT from OT

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU

ONE STEP AHEAD