Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

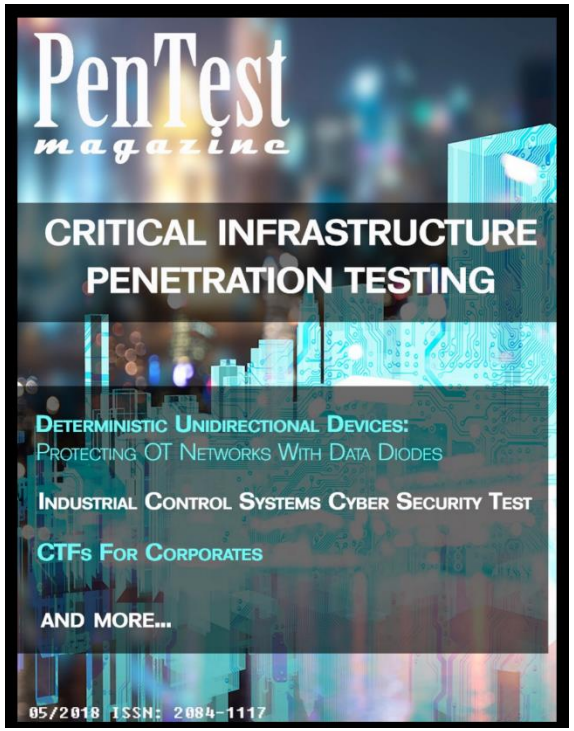
kaspersky

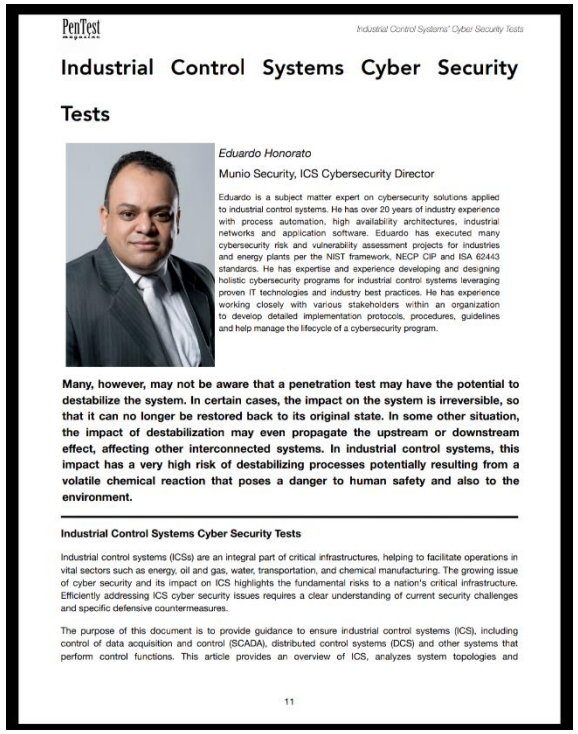
munio SECURITY

Assessing Energy Infrastructure Cybersecurity with Kics Networks

Eduardo Honorato – IACS CyberSecurity Director

PenTest Magazine




PenTest

Industrial Control Systems' Cyber Security Tests

Industrial Control Systems Cyber Security Tests

Eduardo Honorato

Munio Security, ICS Cybersecurity Director

Eduardo is a subject matter expert on cybersecurity solutions applied to industrial control systems. He has over 20 years of industry experience with process automation, high availability architectures, industrial networks and application software. Eduardo has executed many cybersecurity risk and vulnerability assessment projects for industries and energy plants per the NIST framework, NECP CIP and ISA 62443 standards. He has expertise and experience developing and designing holistic cybersecurity programs for industrial control systems leveraging proven IT technologies and industry best practices. He has experience working closely with various stakeholders within an organization to develop detailed implementation protocols, procedures, guidelines and help manage the lifecycle of a cybersecurity program.

Many, however, may not be aware that a penetration test may have the potential to destabilize the system. In certain cases, the impact on the system is irreversible, so that it can no longer be restored back to its original state. In some other situation, the impact of destabilization may even propagate the upstream or downstream effect, affecting other interconnected systems. In industrial control systems, this impact has a very high risk of destabilizing processes potentially resulting from a volatile chemical reaction that poses a danger to human safety and also to the environment.

Industrial Control Systems Cyber Security Tests

Industrial control systems (ICSs) are an integral part of critical infrastructures, helping to facilitate operations in vital sectors such as energy, oil and gas, water, transportation, and chemical manufacturing. The growing issue of cyber security and its impact on ICS highlights the fundamental risks to a nation's critical infrastructure. Efficiently addressing ICS cyber security issues requires a clear understanding of current security challenges and specific defensive countermeasures.

The purpose of this document is to provide guidance to ensure industrial control systems (ICS), including control of data acquisition and control (SCADA), distributed control systems (DCS) and other systems that perform control functions. This article provides an overview of ICS, analyzes system topologies and

11


PenTest

How to Assess Energy Infrastructure Cybersecurity

How to Assess Energy Infrastructure Cybersecurity

Eduardo Honorato

Munio Security, ICS Cybersecurity Director

Eduardo is a subject matter expert on cybersecurity solutions applied to industrial control systems. He has over 20 years of industry experience with process automation, high availability architectures, industrial networks and application software. Eduardo has executed many cybersecurity risk and vulnerability assessment projects for industries and energy plants for the NIST framework, NECP CIP and ISA 62443 standards. He has expertise and experience developing and designing holistic cybersecurity programs for industrial control systems leveraging proven IT technologies and industry best practices. He has experience working closely with various stakeholders within an organization to develop detailed implementation protocols, procedures, guidelines and help manage the lifecycle of a cybersecurity program. He is currently ISA (International Society of Automation) Director of Cybersecurity in Brazil.

As the report says, the dynamics of the energy industry could be creating an imminent cyber storm. As a first step, we need to understand how these companies use technology in the automation of their work and how we can improve safety.

Introduction

Nowadays the world is full of threats of high potential and impact, since we have many news stories of hacks and crimes related to cyber. Although most of the news is attacks on commercial companies, banks and other types of businesses, energy infrastructure can be a very easy target for other governments, criminals and terrorist groups.

One point to understand is how the generation and delivery of energy works. Electricity is generated in power plants and goes through a complex system, sometimes called a grid, electrical substations, transformers, and power lines that connect electricity producers and consumers. Most local area networks are interconnected for commercial and reliability purposes, forming larger, more reliable networks that enhance coordination and planning of the electricity supply. Below is an image that best illustrates this explanation.

21

kaspersky

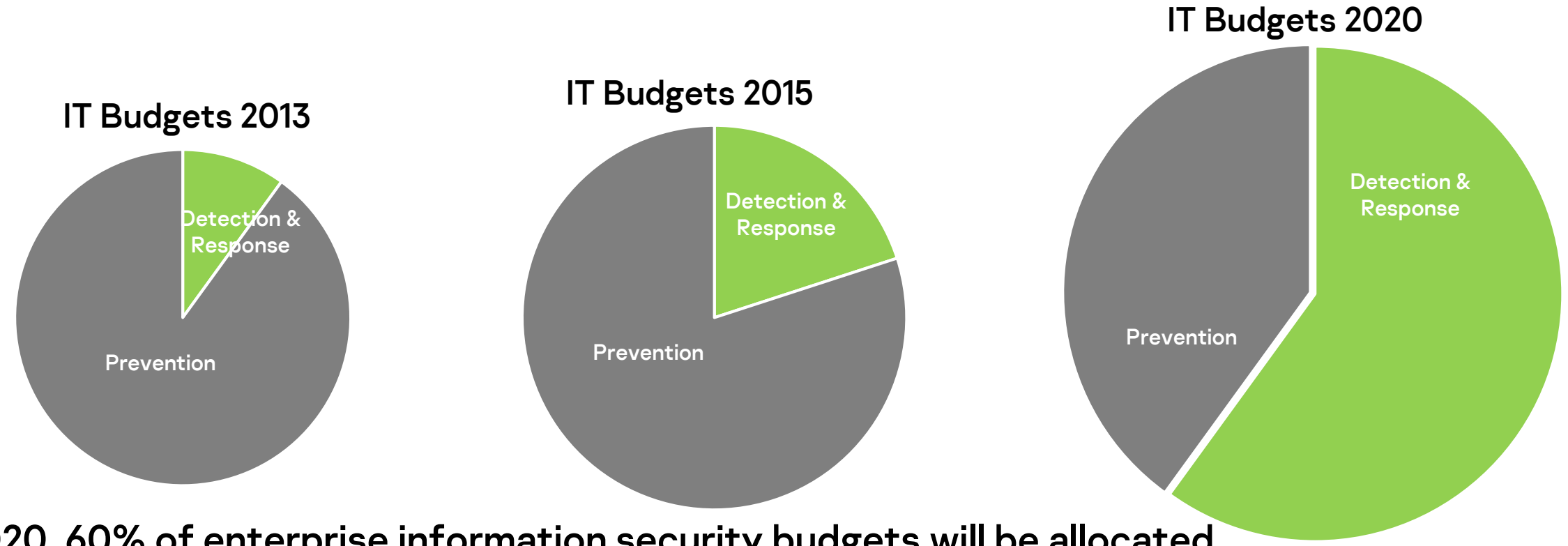
munio SECURITY

Munio Security protects against **“operational disruptions”** caused by cyber threats, malicious insiders and human error, by providing visibility and control to industrial networks.

kaspersky

munio SECURITY

It's become apparent that prevention is not enough. A strategic shift is occurring—from prevention-centric strategies to detection and response.



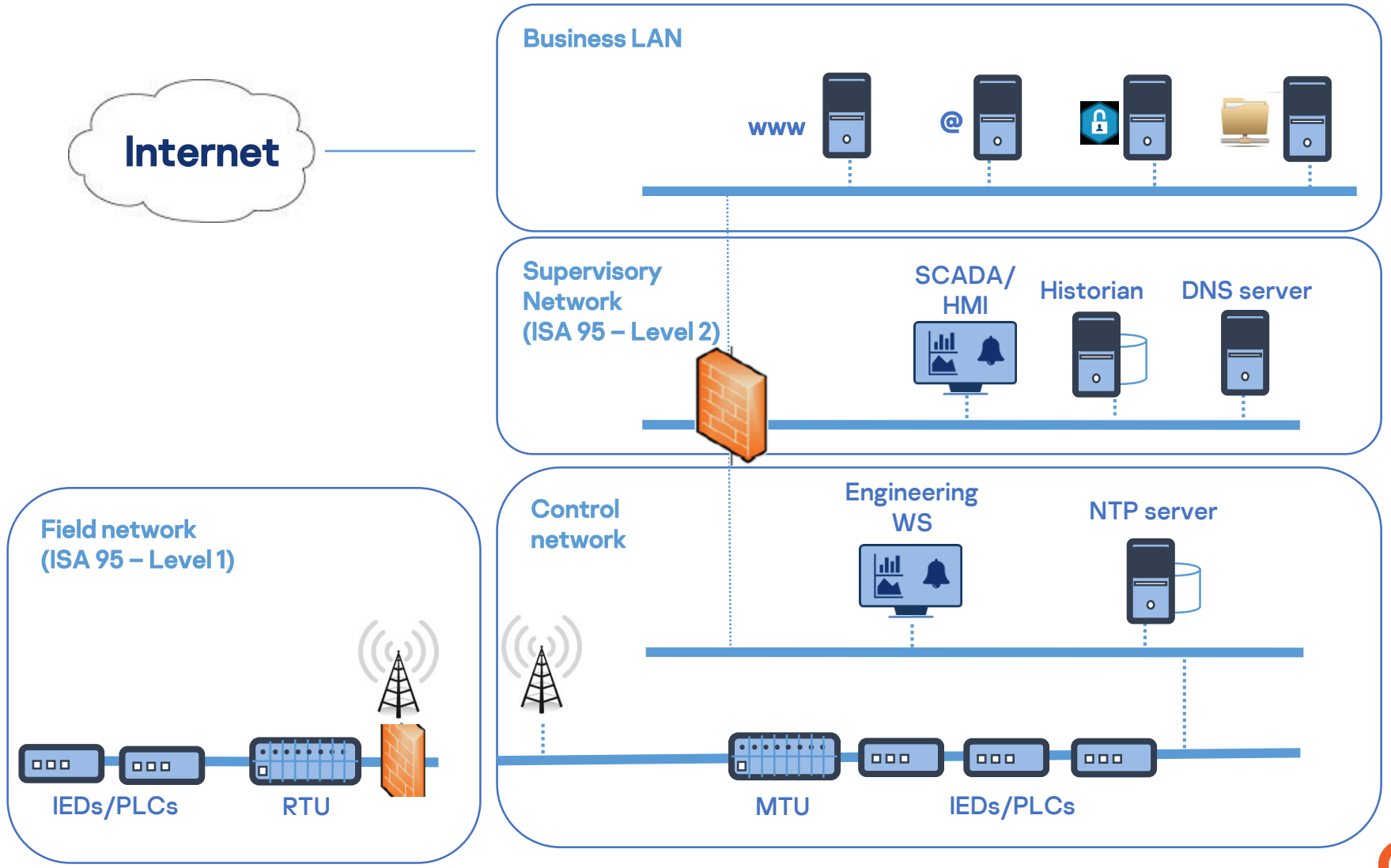
By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from 20% in 2015. – *Gartner, 2016*

kaspersky

Sources: Gartner, Shift Cybersecurity Investment to Detection and Response, January 2016; Gartner, Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update, April 2016
Note: Excludes security services from estimated overall market spend for enterprise information security

munio SECURITY

How does an ICS network look like

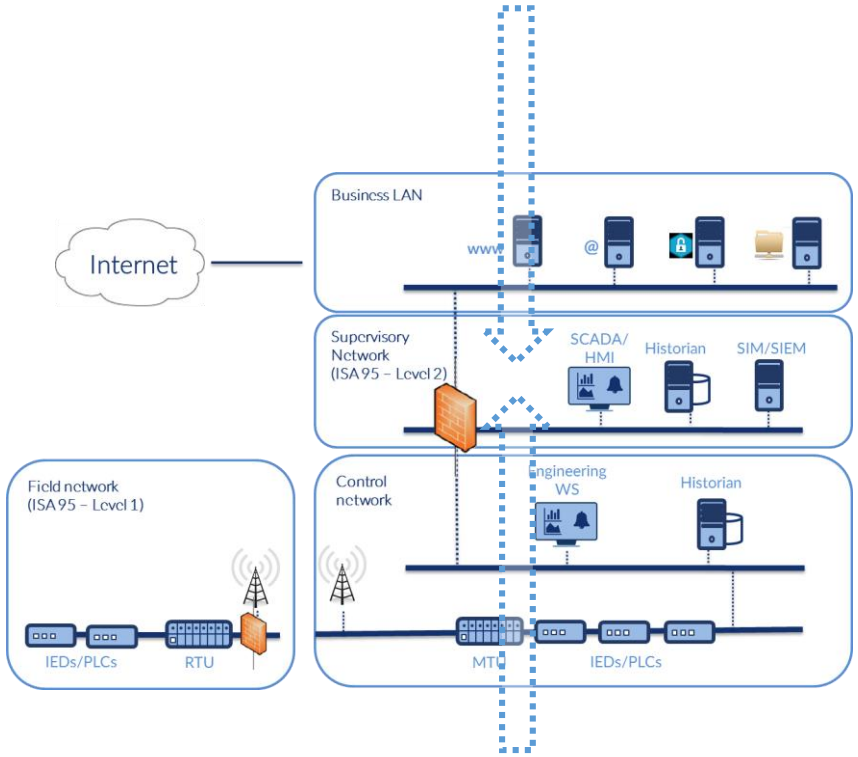


kaspersky

munio SECURITY

IT/OT protocols in ICS networks

Information Technology (IT)



Operational Technology (OT)

Common IT services/protocols

Web: HTTP/HTTPS
Authentication and identity: LDAP
DBs: TCP/IP on specifics ports
File sharing: SFTP, SSH
Secure connection: SSL/TLS
Name service: DNS, LLMNR, SMB
Time synchronization: NTP
Configuration/Patch service: SSH, TELNET
Network monitoring: SNMP
...

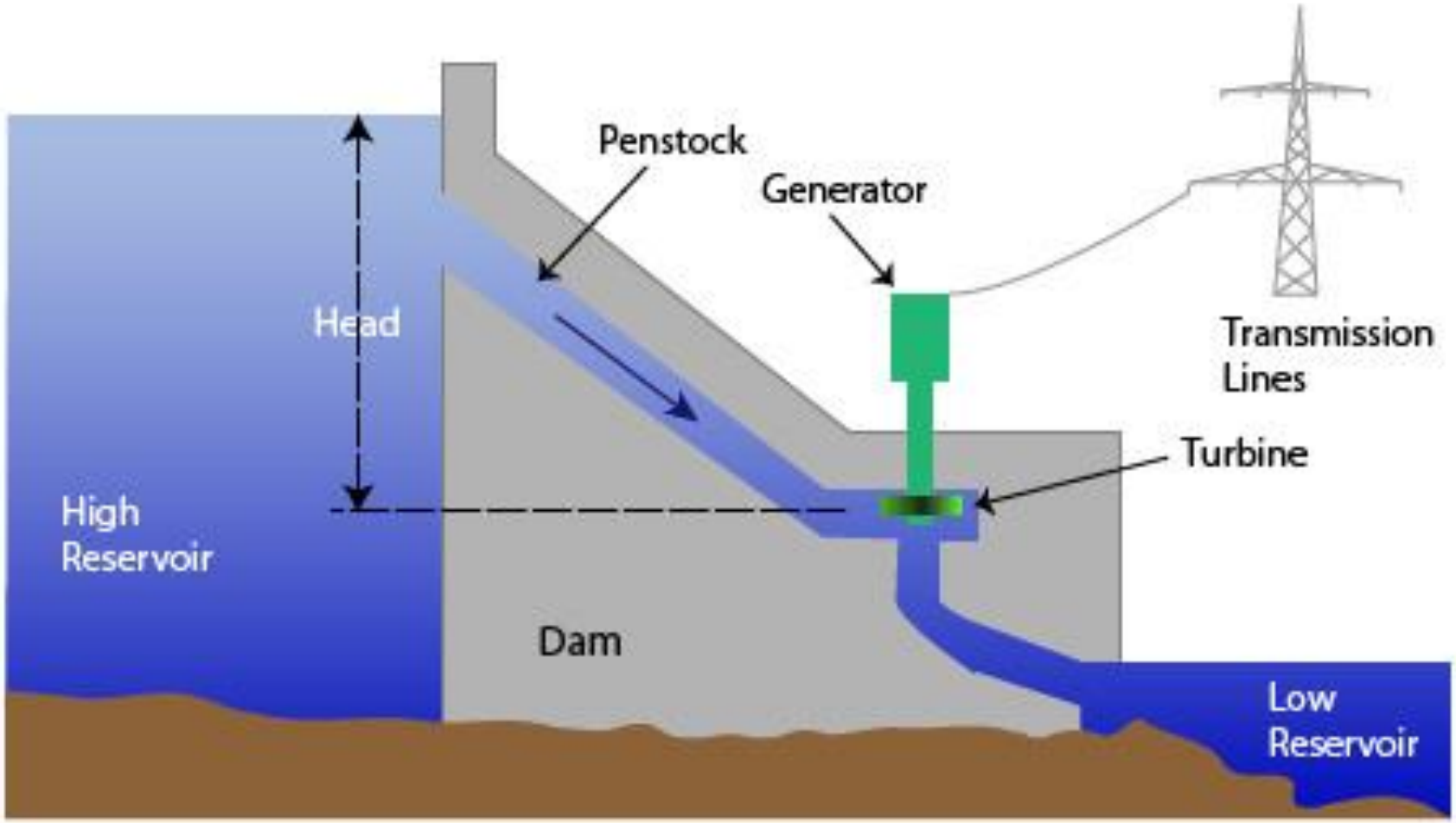
Common OT protocols

DNP3, IEC 101/104,
ICCP
IEC 61850 (MMS, GOOSE, SV)
MODBUS, MODBUS/TCP
OPC DA/AE
EtherNet/IP,
Proprietary protocols,
...

kaspersky

munio SECURITY

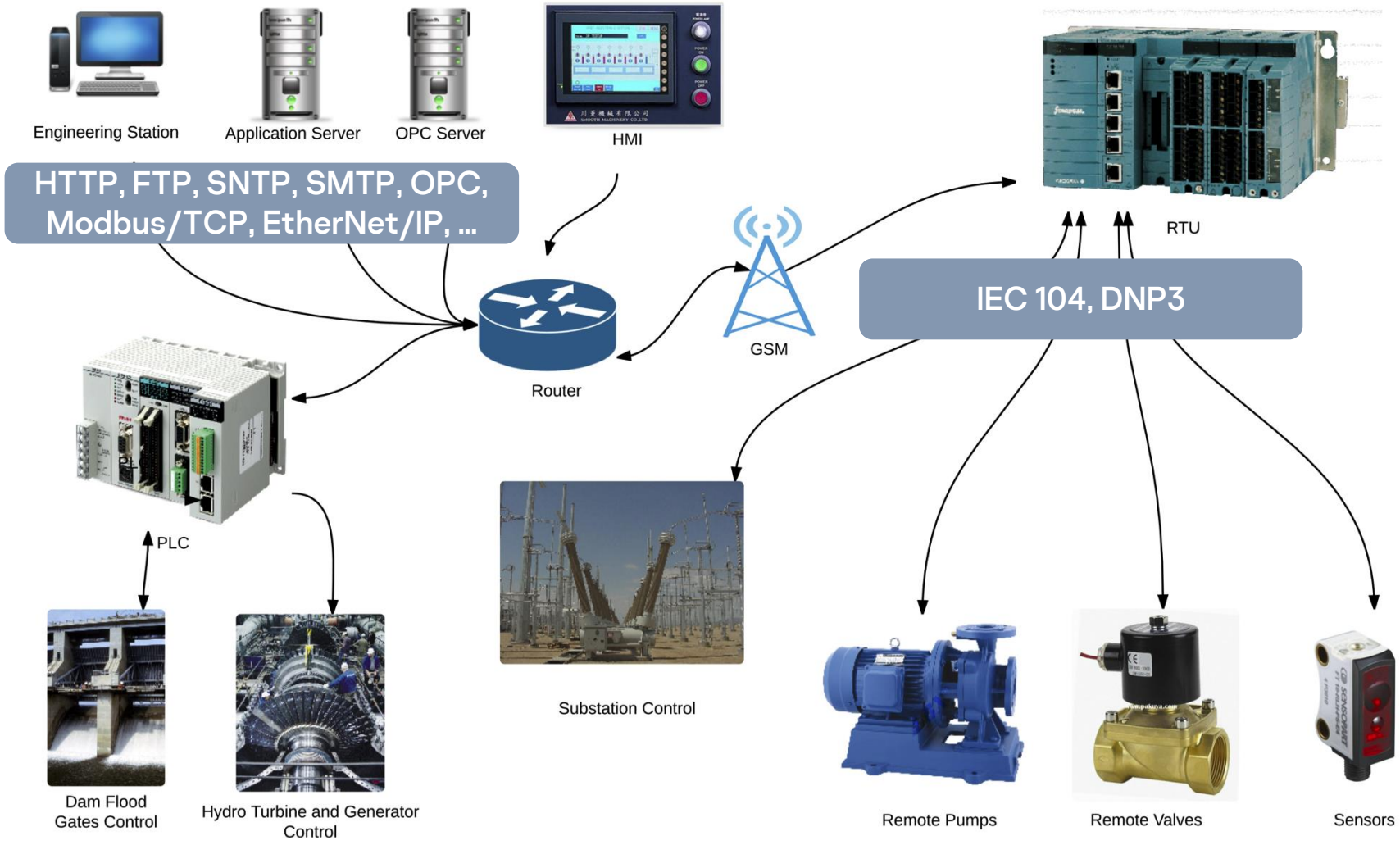
Example: Hydroelectric Power Generation Overview



kaspersky

munio SECURITY

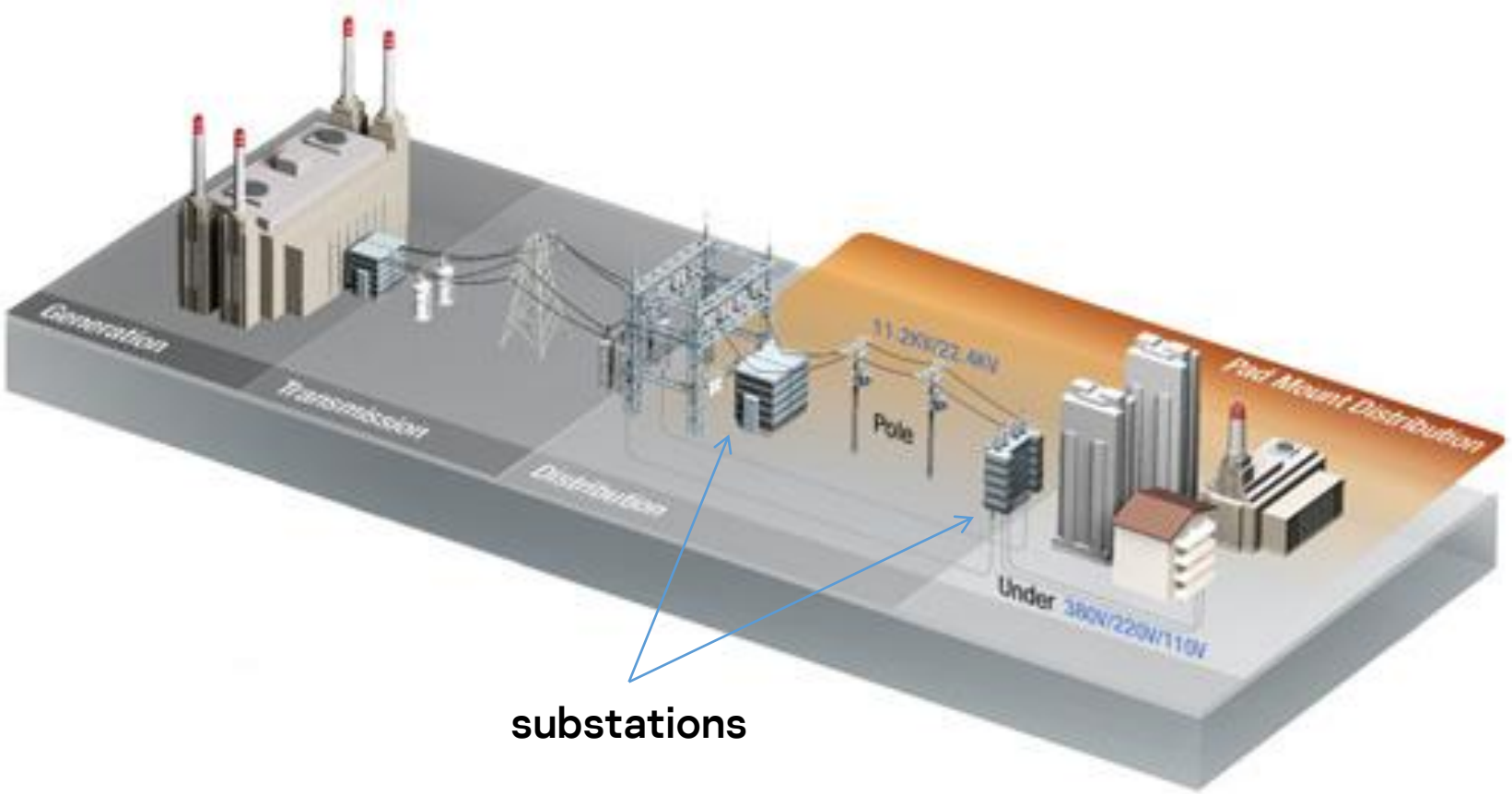
Example: Hydroelectric Power Generation Systems & Protocols



kaspersky

nuniq SECURITY

Example: Electric Power Distribution Overview



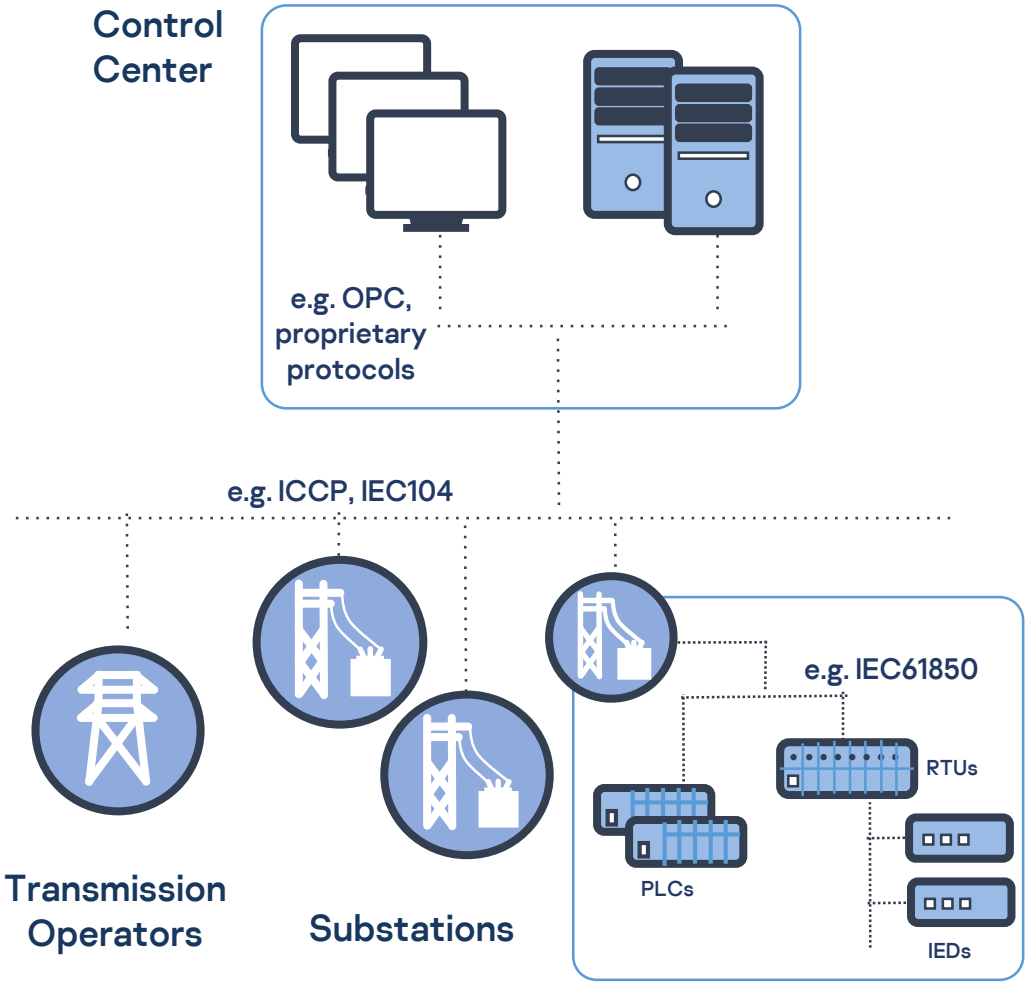
substations

Source: http://www.moxa.com/

kaspersky

munio SECURITY

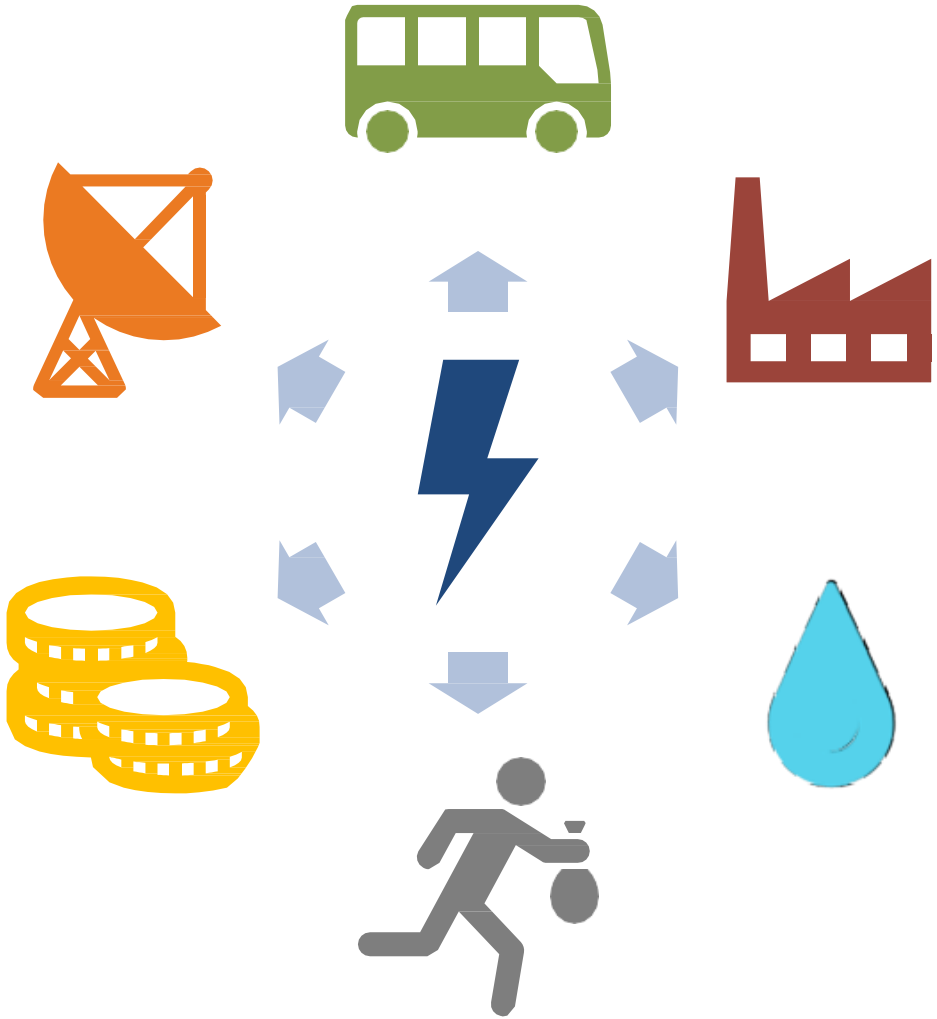
Example: Electric Power Distribution Systems & Protocols



kaspersky

munio SECURITY

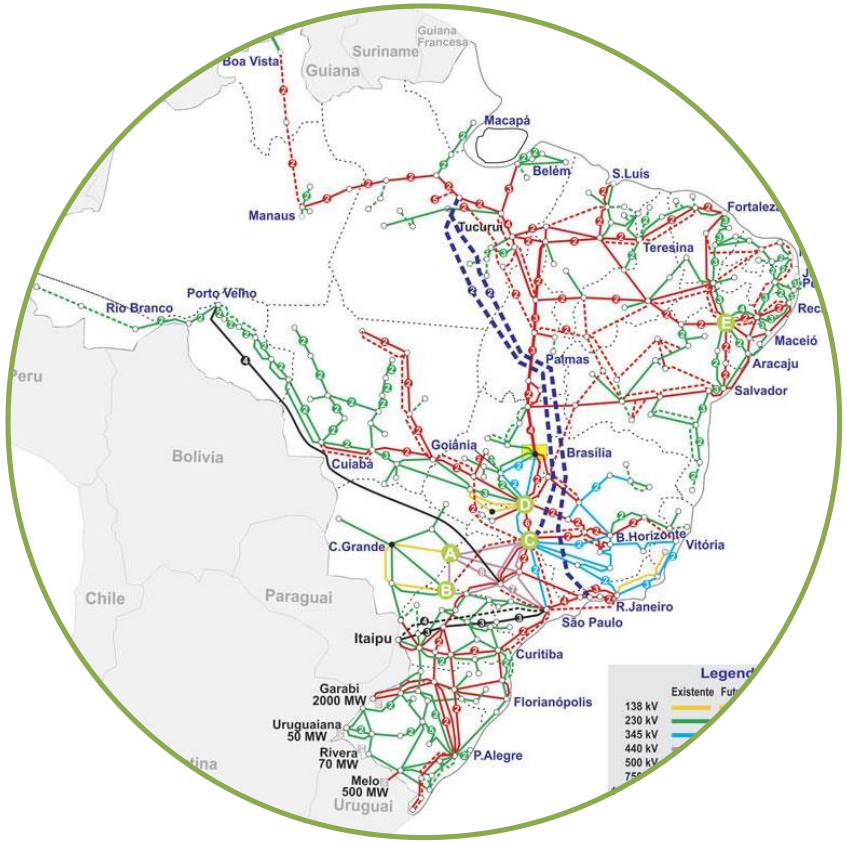
Electricity is the core of the critical infrastructure



kaspersky

munio SECURITY

Interconnected systems – Chain Disconnections



- Integrated power generation & distribution
- Critical paths on a few substations
- Vulnerabilities exploitaition can easily lead to blackouts

kaspersky

munio SECURITY

IT vs. ICS networks (at least in theory)

IT network

ICS network

kaspersky

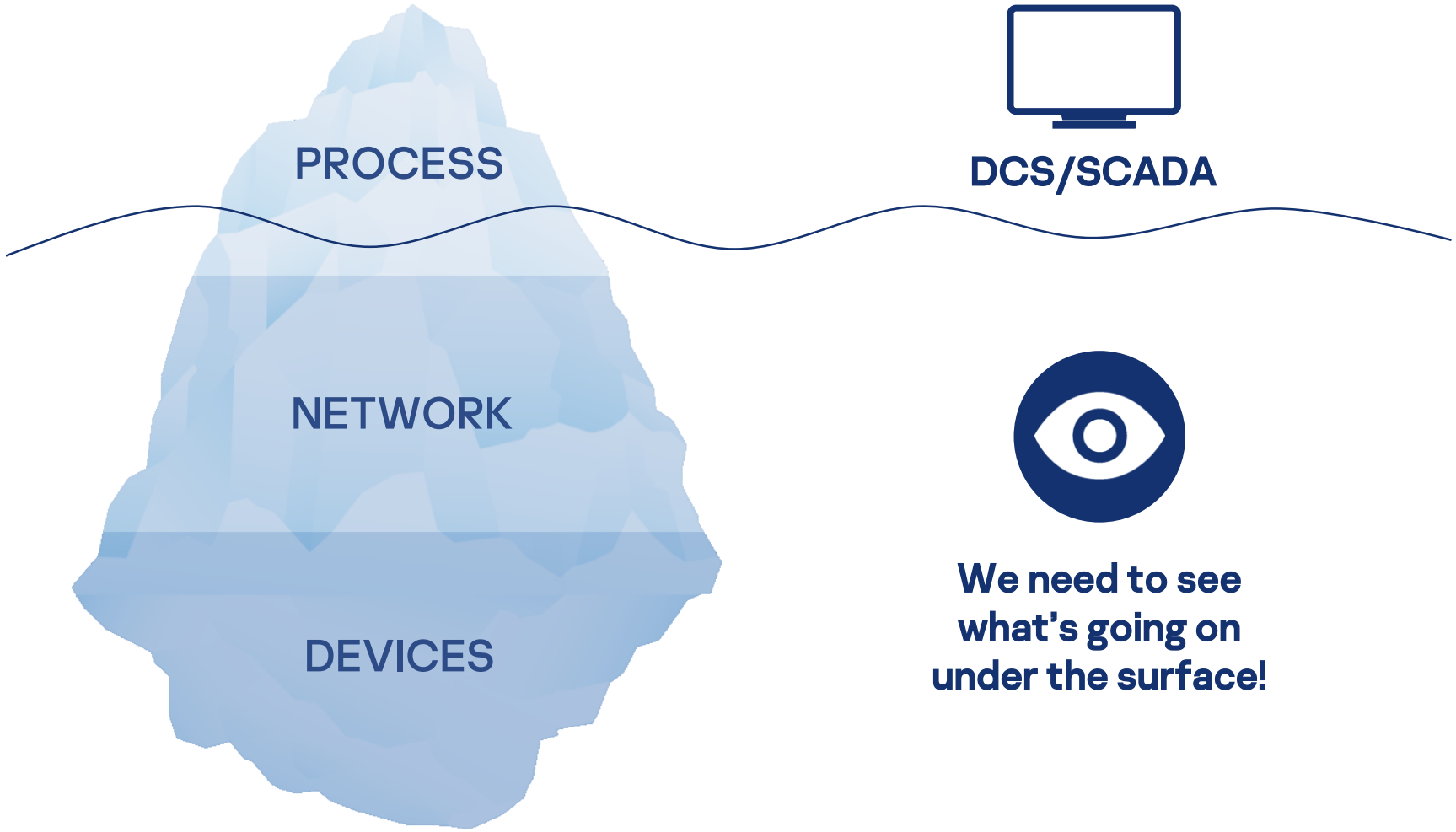
munio SECURITY

In practice, industrial networks look often like...

kaspersky

munio SECURITY

The main problem: lack of visibility



kaspersky

munio SECURITY

Without visibility you can't have Security

Cyber attacks may paralyze digital power structures

A Continuous Process for Securing ICS

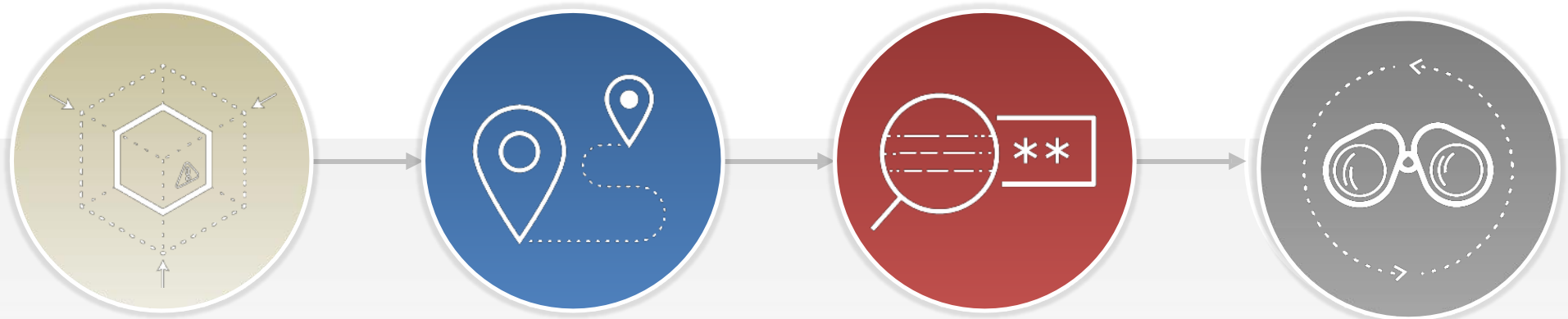
Can you effectively manage and respond to events?

Without visibility you can't have security

kaspersky

munio SECURITY

4 Steps to Assessing Energy Infrastructure Cybersecurity



1. Define protection surface

2. Map the flows, asset and Architecture

3. Asset Management Risk Management

4. Monitor and maintain the OT network

kaspersky

munio SECURITY

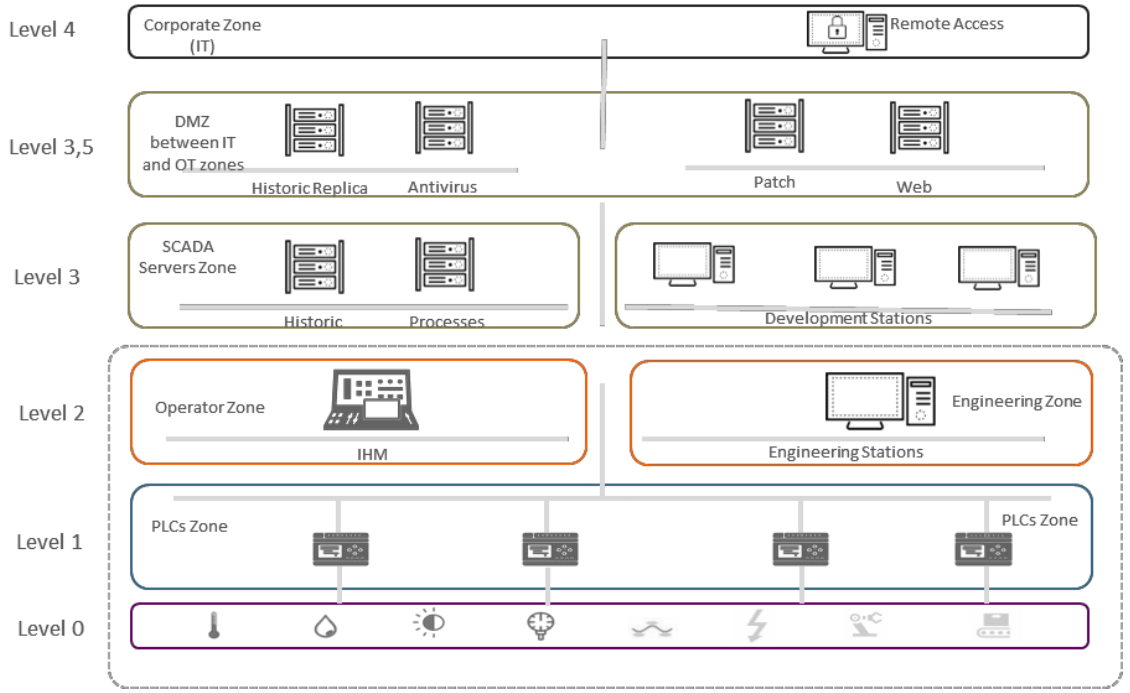
1. Define protection surface

Understand external requirements

- Contractual obligations
- Laws & regulations (e.g NERC-CIP, ISA/IEC 62443)

Electric Power Industry

- NERC CIP-002-5 BES Cyber System Categorization
- NERC CIP-003-5 Security Management Controls
- NERC CIP-004-5 Personnel & Training
- NERC CIP-005-5 Electronic Security Perimeter(s)
- NERC CIP-006-5 Physical Security of BES Cyber Systems
- NERC CIP-007-5 Systems Security Management
- NERC CIP-008-5 Incident Reporting and Response Planning
- NERC CIP-009-5 Recovery Plans
- NERC CIP-010-1 Configuration Management and Vulnerability
- NERC CIP-011-1 Information Protection



Translate external requirements into cybersecurity requirements

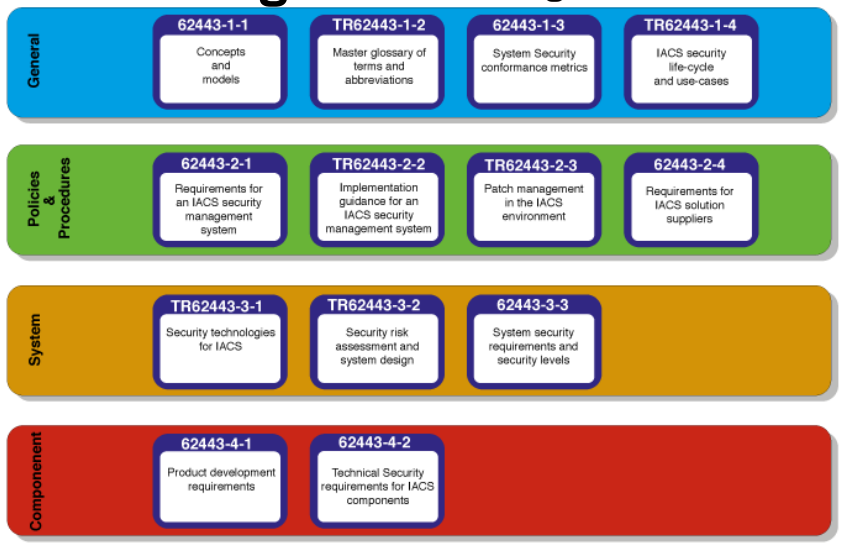
kaspersky

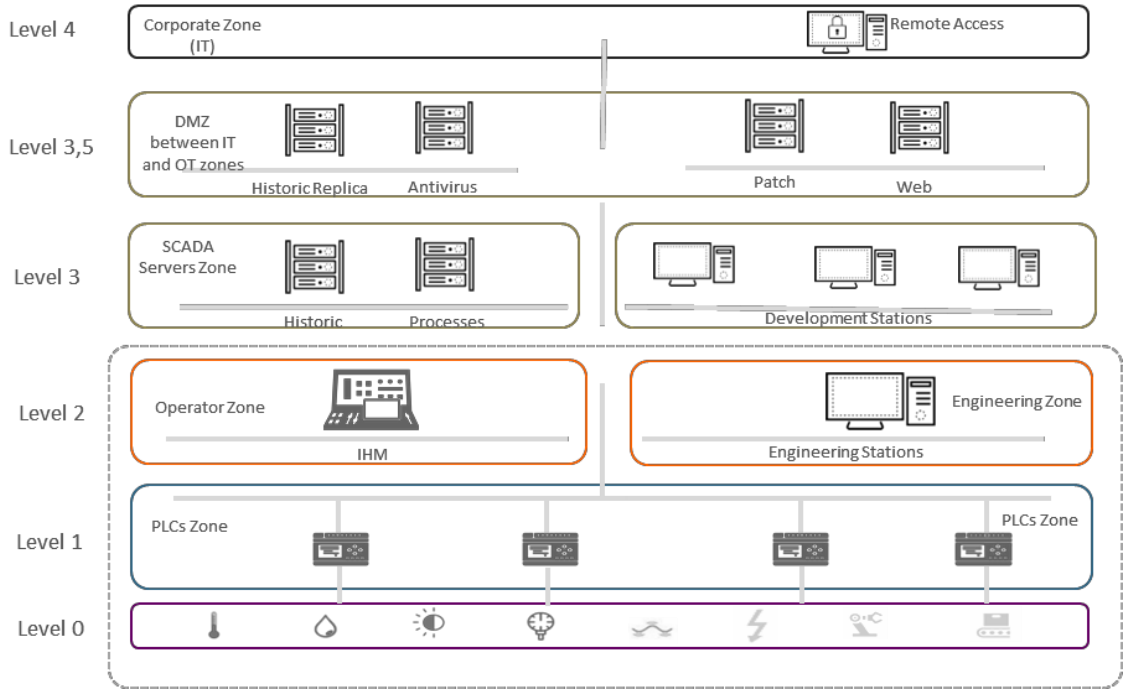
munio SECURITY

1. Define protection surface

Understand external requirements

- Contractual obligations
- Laws & regulations (e.g NERC-CIP,



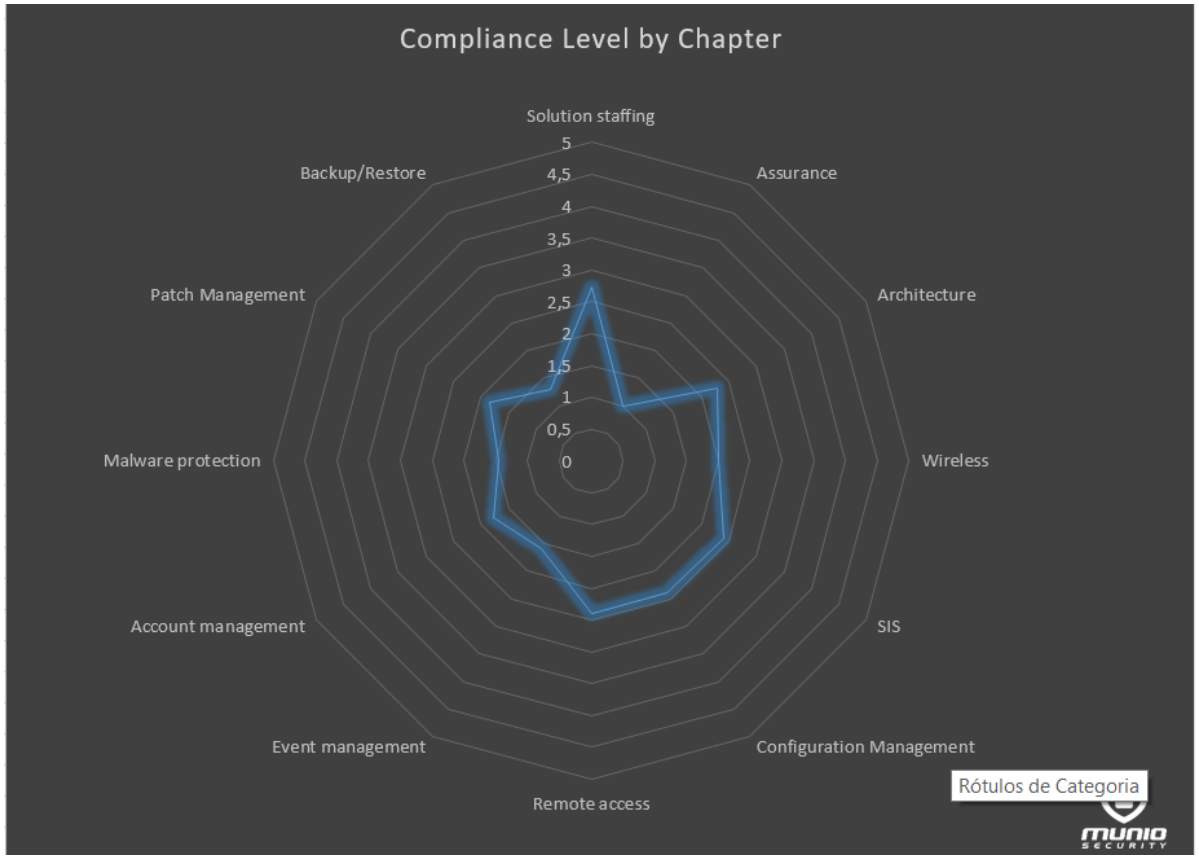


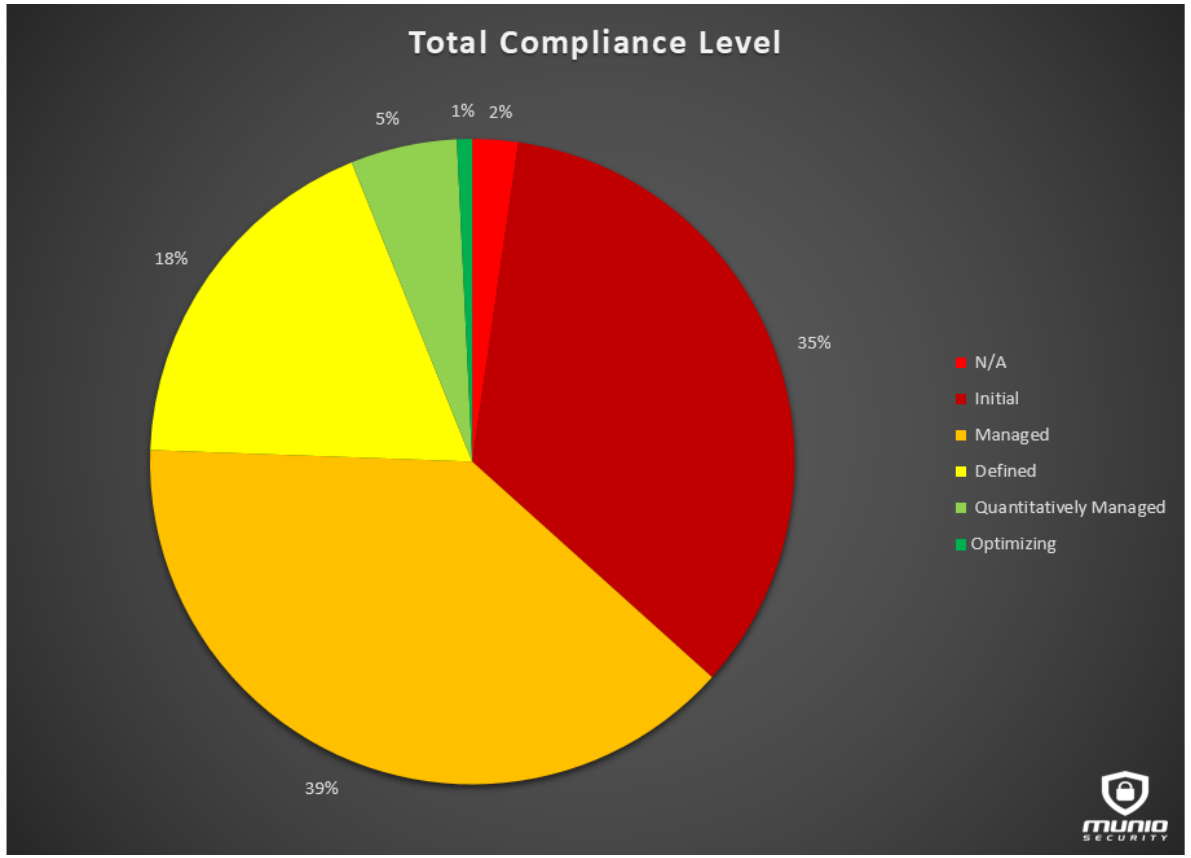
Translate external requirements into cybersecurity requirements

kaspersky

munio SECURITY

1. Define protection surface





kaspersky

munio SECURITY

1. Define protection surface

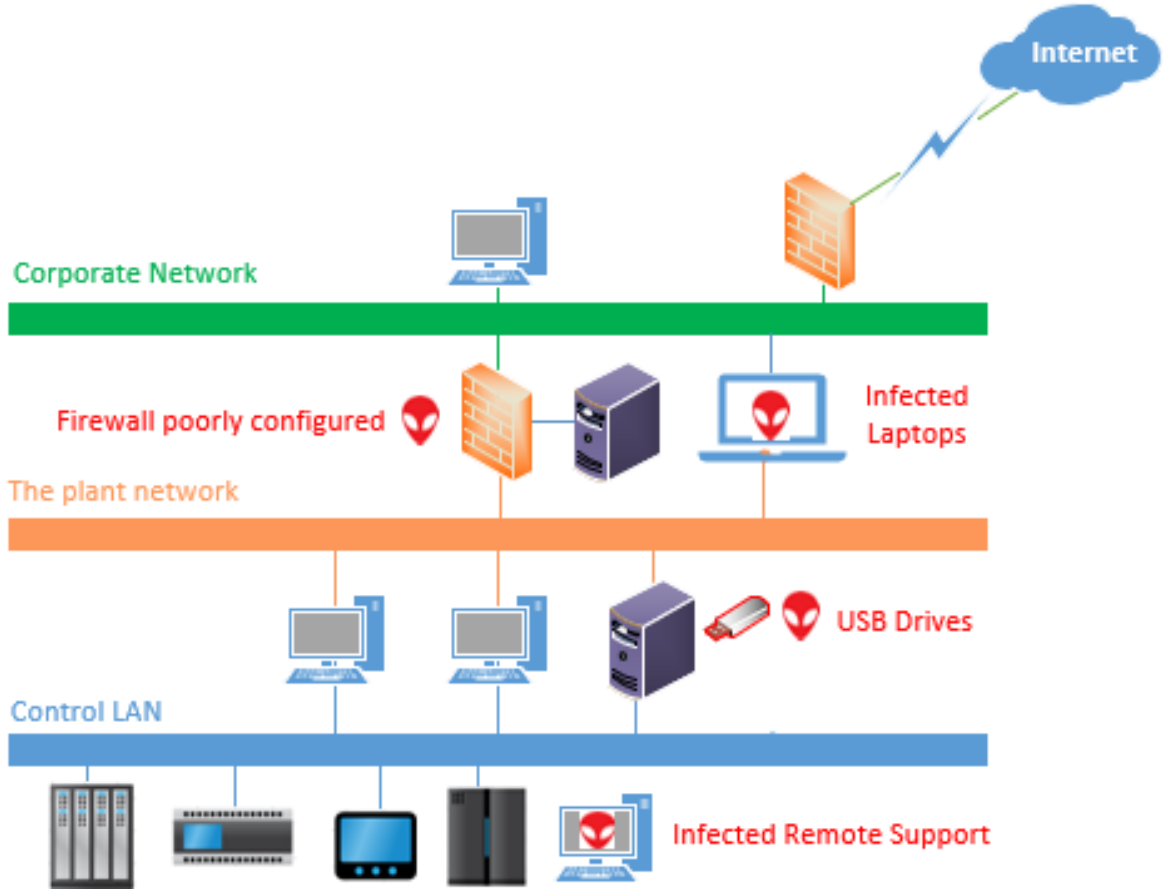
Relatório por Capitulo

SP.01 - Solution Staffing - Pessoal de Solução

Initial	SP.01.01	O provedor de serviços deve ter a capacidade de garantir que ele designe apenas o pessoal provedor de serviços para atividades relacionadas à Solução e que tenham sido informadas e cumpram as responsabilidades, políticas e procedimentos exigidos por esta especificação.
Initial	SP.01.01-1	O provedor de serviços deve ter a capacidade de garantir que apenas designe subcontratado ou pessoal consultor para atividades relacionadas à Solução e que tenham sido informadas e cumpram as responsabilidades, políticas e procedimentos exigidos por esta especificação.
Managed	SP.01.02	O provedor de serviços deve ter a capacidade de garantir que apenas designe prestador de serviços, subcontratado ou pessoal de consultoria para atividades relacionadas à Solução e que tenham sido informadas e cumpram as responsabilidades, políticas e procedimentos relacionados à segurança exigidos pelo proprietário do ativo.
Managed	SP.01.02-1	O provedor de serviços deve ter a capacidade de garantir que somente o prestador de serviços, subcontratado ou consultor participe de atividades relacionadas à Solução e que tenham sido informadas e cumpram os processos de Gerenciamento de Mudança (Management of Change (MoC)) e Permição para Trabalhar (Permit To Work (PtW)) do proprietário do ativo. para alterações envolvendo dispositivos, estações de trabalho e servidores e conexões entre eles.
Defined	SP.01.03	O provedor de serviços deve ter a capacidade de garantir que ele designe apenas o pessoal provedor de serviços para atividades relacionadas à Solução e que tenham sido informados das políticas, procedimentos e obrigações contratuais necessárias para proteger a confidencialidade dos dados do proprietário do ativo.

2 - Pathways inside the control network

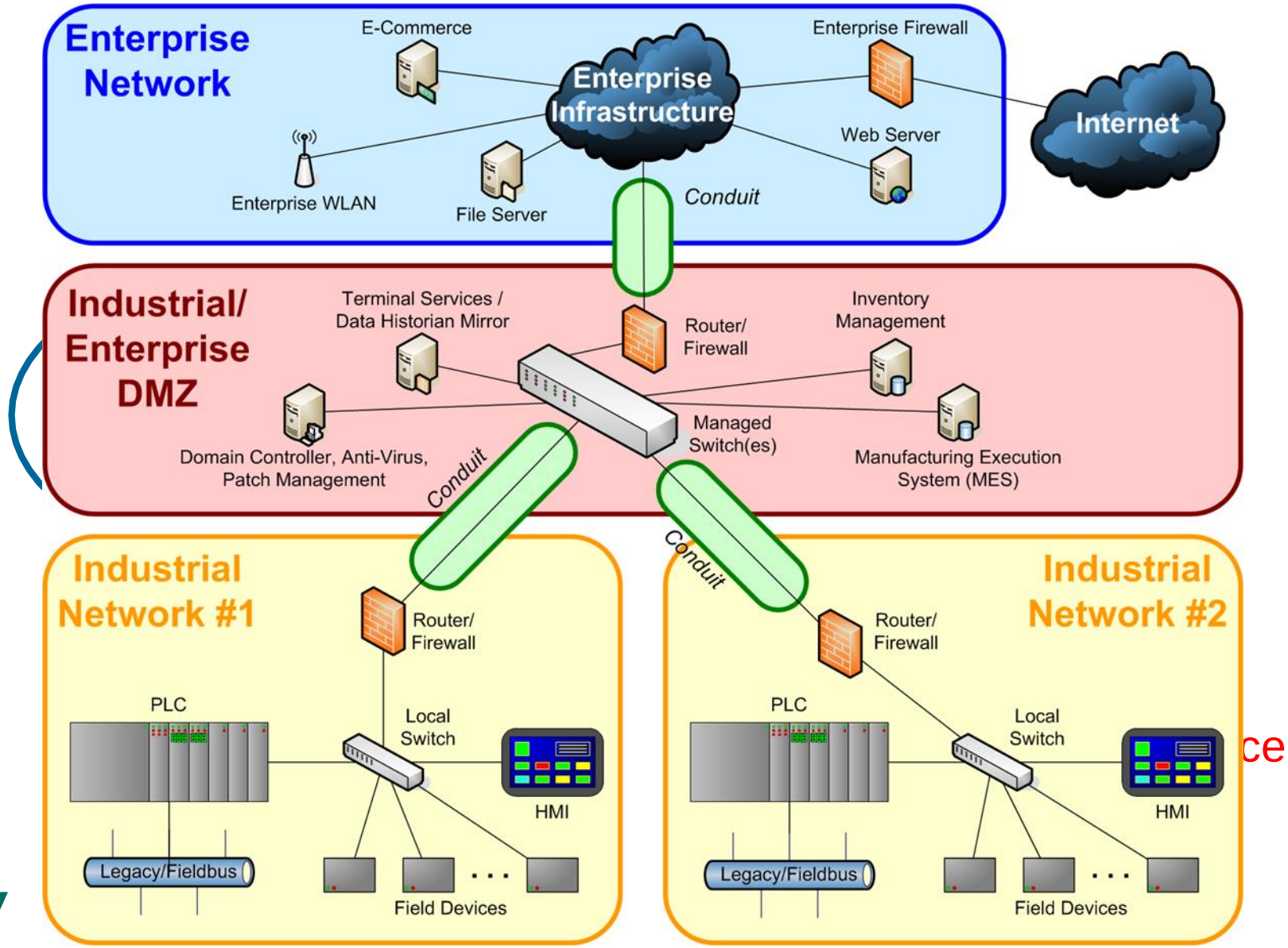
- Protecting only the perimeter of the OT network is not enough.
- There are lots of pathways inside the OT network that bypass perimeter security.
- It's necessary to protect the factory floor with modern and in-depth defense technologies where problems in one area are not allowed to migrate to another area.
- The Solution is the use of security zones, as defined in ISA-IEC62443 standard.



kaspersky

munio SECURITY

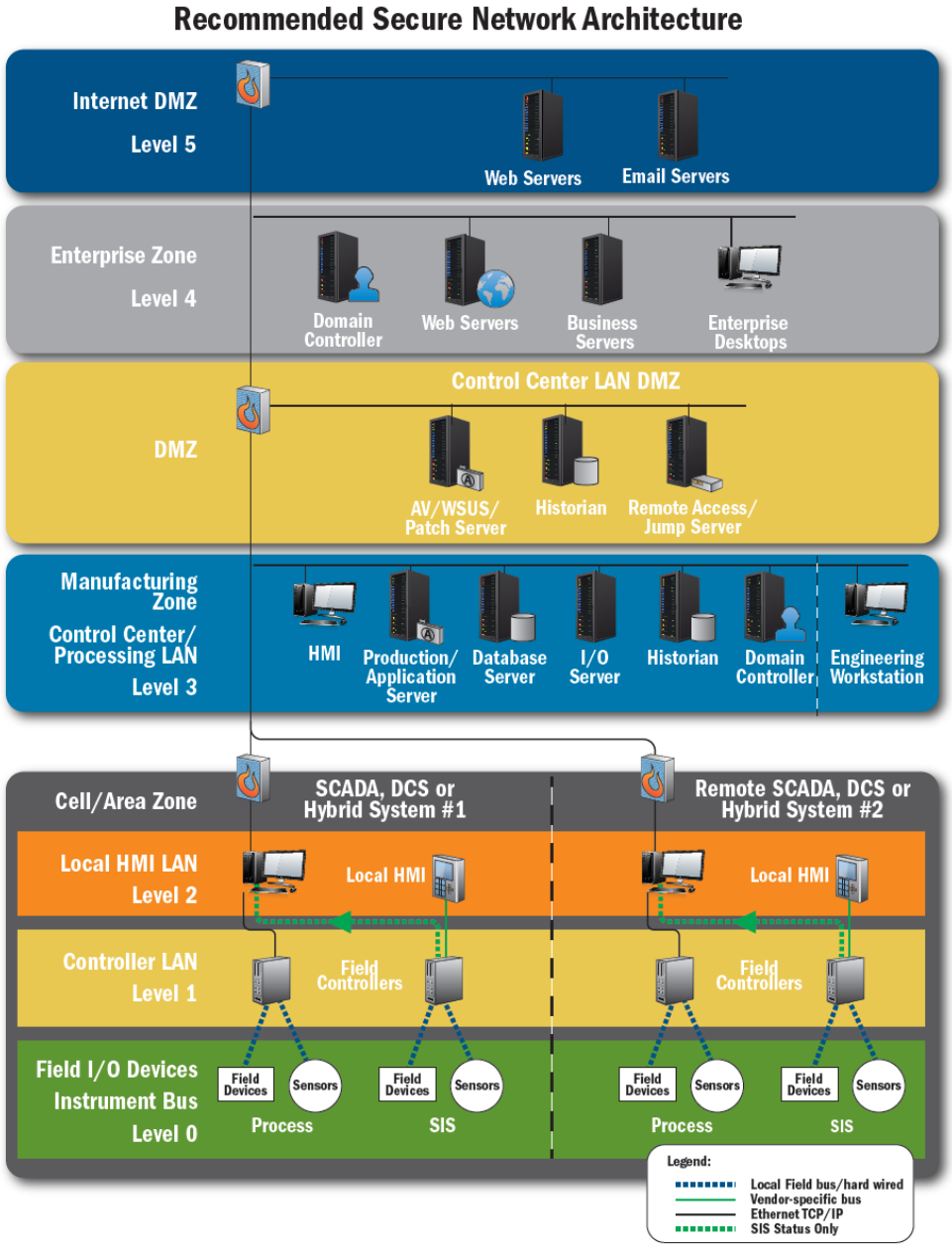
2 - ISA/IEC 62443 – The Zones and Conduits Model



kaspersky

munio SECURITY

2 – Defense in Depth



Source

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016

kaspersky

munio SECURITY

3 - Asset Management / Risk Management

Automatic Discovery of Industrial Assets

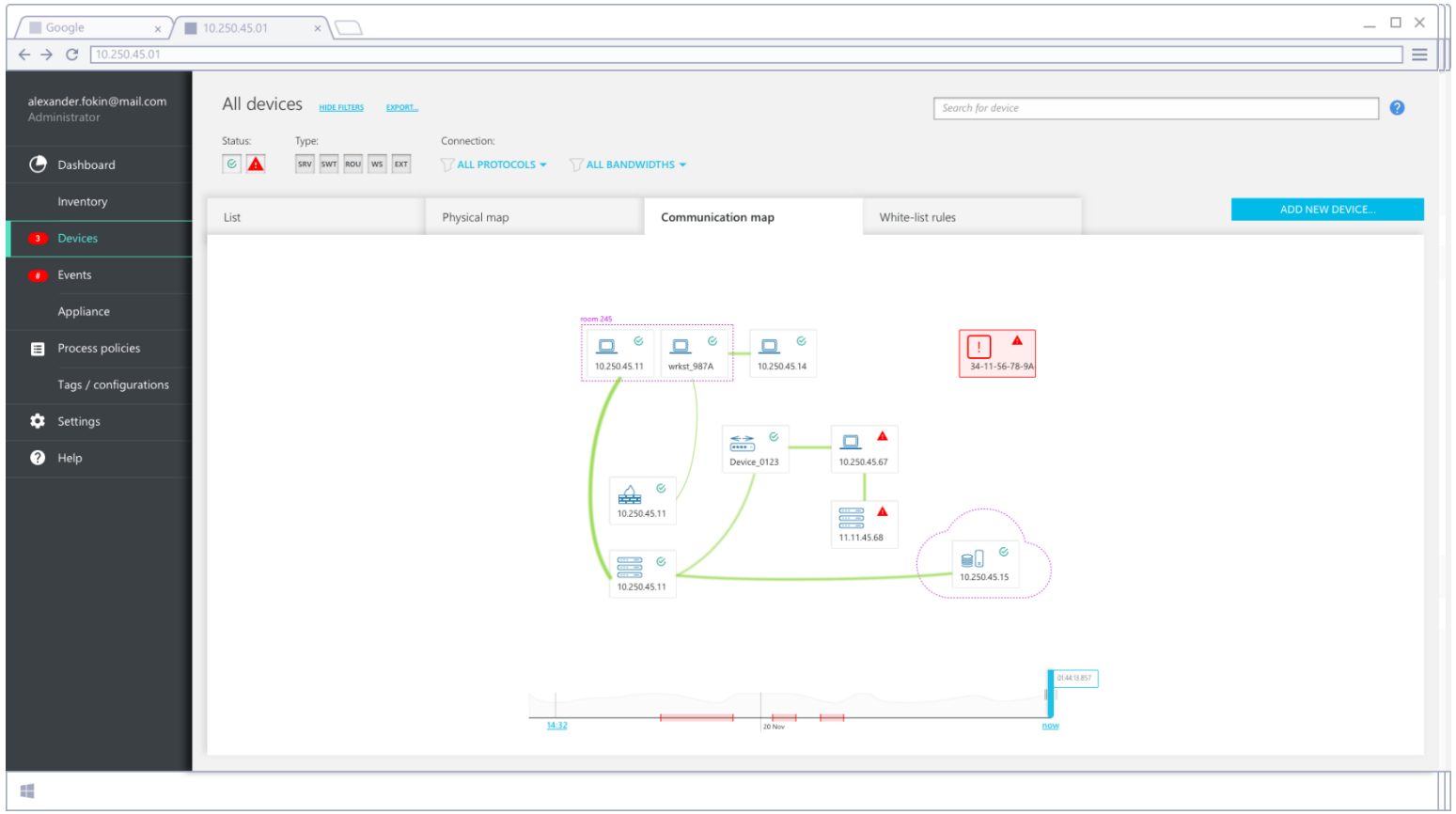
Discover Current Devices (PCs, Servers, Laptops, PLCs, Routers)

Current Map of the Communication Network

View existing network communications in connection with detected assets

Configure network map and DPI rules in one easy to use interface

The Time Machine feature allows the security officer to forensically search any network activity over various time dimensions.



kaspersky

munio SECURITY

It´s necessary to monitor and manage equipments 24x7x365 to respond to cyber attacks without causing a production outage.

We did it through our OT-SOC

Munio Security OT-SOC integrates cybersecurity functions with industrial processes monitoring to prevent and respond to cyber attacks against critical infrastructures.

munio SECURITY

4. Monitor and maintain - Log sources for OT-SOC

Active Directory	Firewall	Industrial Firewalls	Network Services such as DNS, DHCP, etc
SCADA	Industrial IDS	Network events from Switches and Firewalls (Physical and virtuals)	Netflow and Jflow
Layer 7 Packet Analisys	Proxy Servers	Operating Systems Events (Linux / UNIX / Windows)	Physical Security Systems

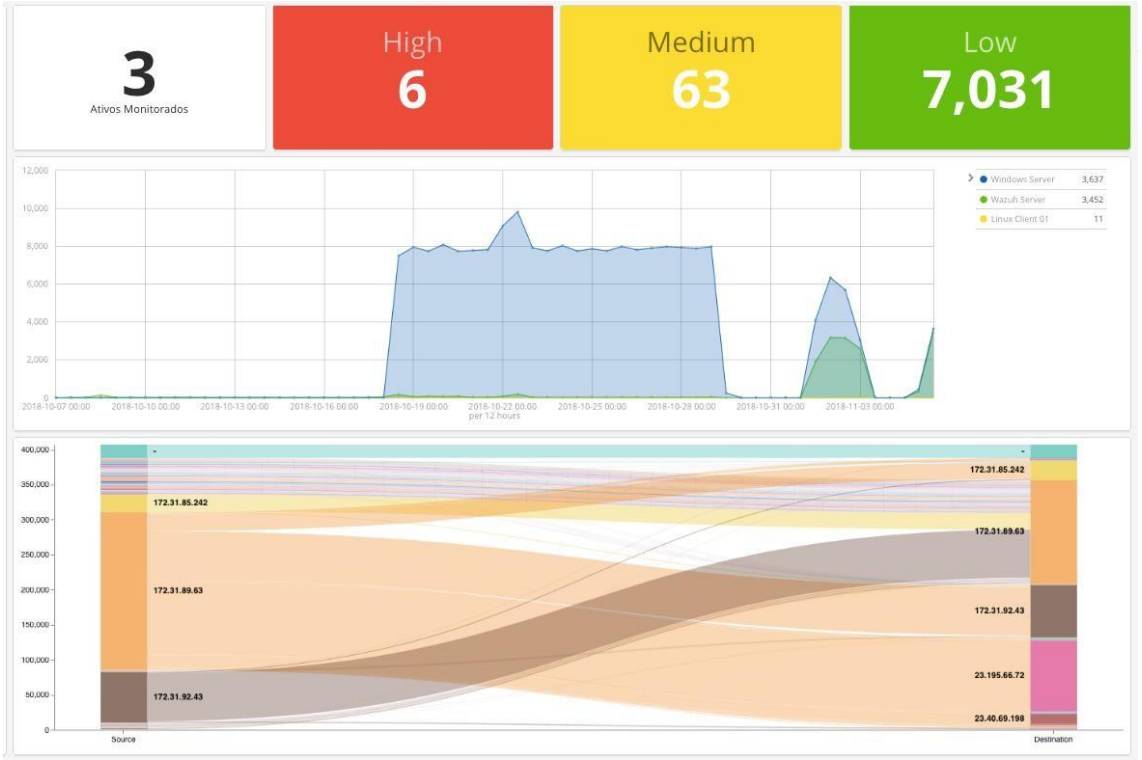
kaspersky

munio SECURITY

4. Monitor and maintain the OT Network

OT SIEM – Event Management for the Electrical Sector

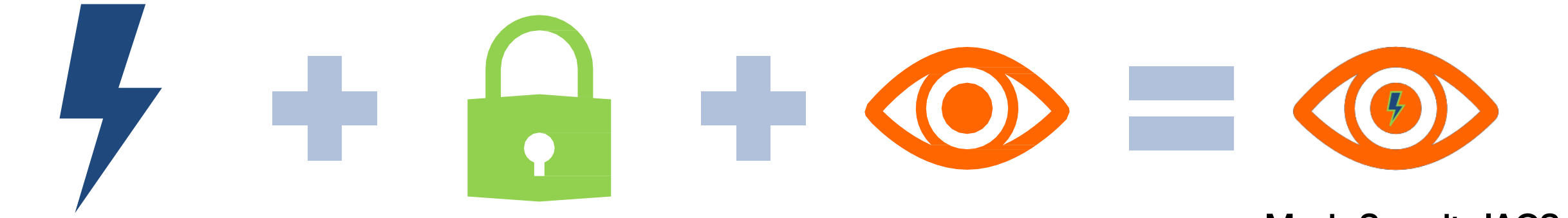
- Security intelligence platform with unified architecture to collect, store, analyze and structure data of events (logs), network flows, threats, vulnerabilities and risks of electrical energy environments: generation, transmission and distribution.
- Event correlation activities are performed on a single screen, with the possibility of clear incident identification, flow telemetry, risk modeling, and impact analysis.
- Modular and scalable structure that allows you to manage the security of environments of all types and sizes.
- Platform established in partnership with leading technology of big data andanalytics.
- Integrated cyber security dashboards and operating information, including information on Modbus,ICCP, DNP-3, IEC 60870-5-104, Siemens S7 protocols, among others specific to power.



kaspersky

munio SECURITY

A new joint product



Energy Clients + Kaspersky Kics + Munio Security OT-SOC = Munio Security IACS Cybersecurity for Energy

kaspersky

munio SECURITY

Munio Security Cybersecurity for Energy

Cybersecurity policies	Edge Security with Next Generation Firewall	Secure Remote Access
Visibility – Kics Networks	Zones and Conduits Segmentation and Defense in Depth	Vulnerability Monitoring
Malware protection and Control – Kics Nodes	Continuous monitoring by Munio Security OT-SOC	4-eyed Auditing and Management

kaspersky

munio SECURITY

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

munio SECURITY

Thank you!

kaspersky.com

muniosecurity.com


kaspersky


munio
SECURITY