

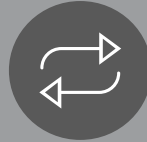
a little understanding of

who we are



software developer

of the SCADA Panorama Software Suite



transverse approach

in order to address many sectors Safety/Security, Energy Efficiency, Industrial SCADA, Building, etc.



French SMB

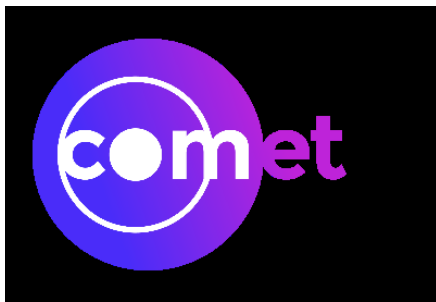
100 employees

13.5M€ of SR (**8%** export)




they trust us
our clients





why and how to secure a SCADA System

a Panorama overview story

- 
- .01** what's a SCADA system ?
 - .02** understanding SCADA risk impacts
 - .03** building a SCADA cybersecurity framework
 - .04** the basics
 - .05** CODRA's cyber strategy



SCADA system

Definition

0

1

what is a

SCADA system ?



SCADA is the acronym for **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition

Part of the Industrial Control System (ICS)

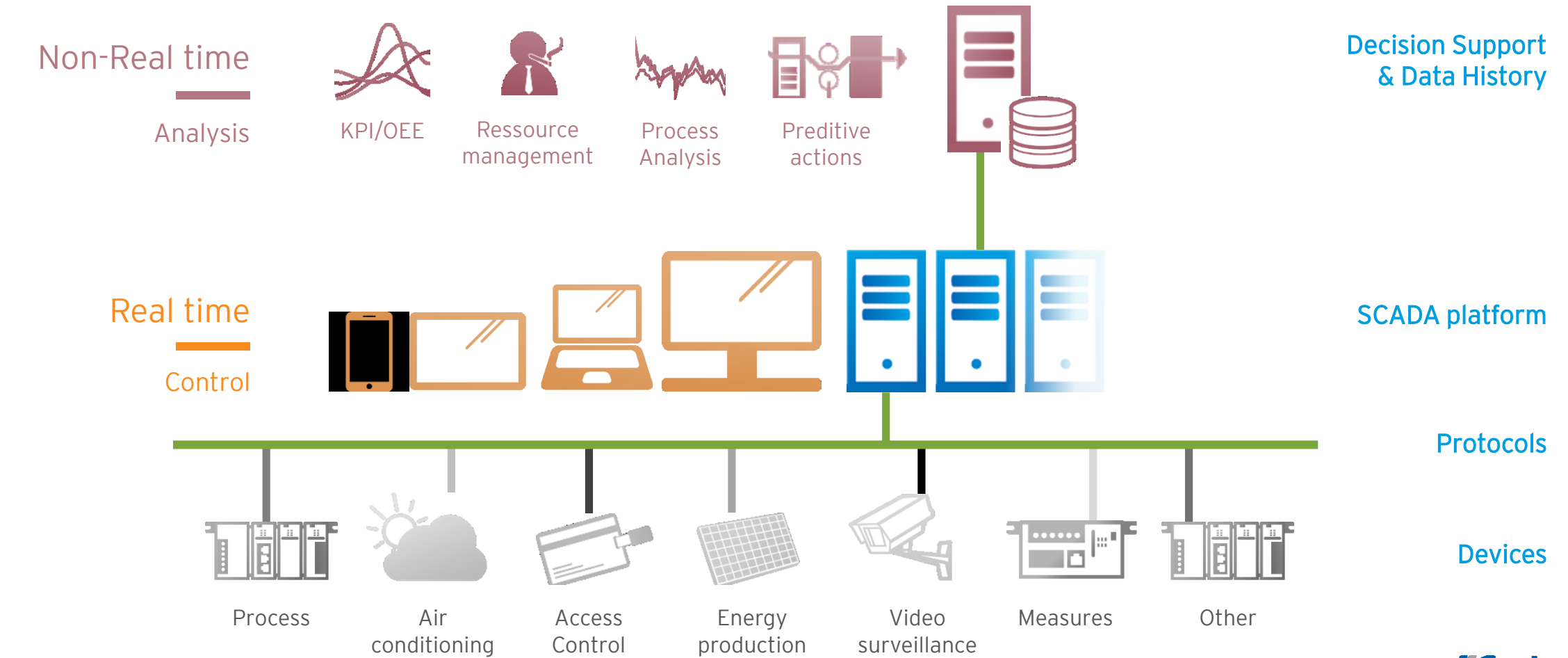
Used to monitor and control a plant or equipment in many fields : industrial, infrastructure or facility.

Control industrial processes locally or at remote locations

Monitor, gather, and process real-time data

global scheme

SCADA system





SCADA cybersecurity risks

02

facts

a real threat !

Because of the importance of SCADA systems, they have become a target for those wishing to create significant harm.

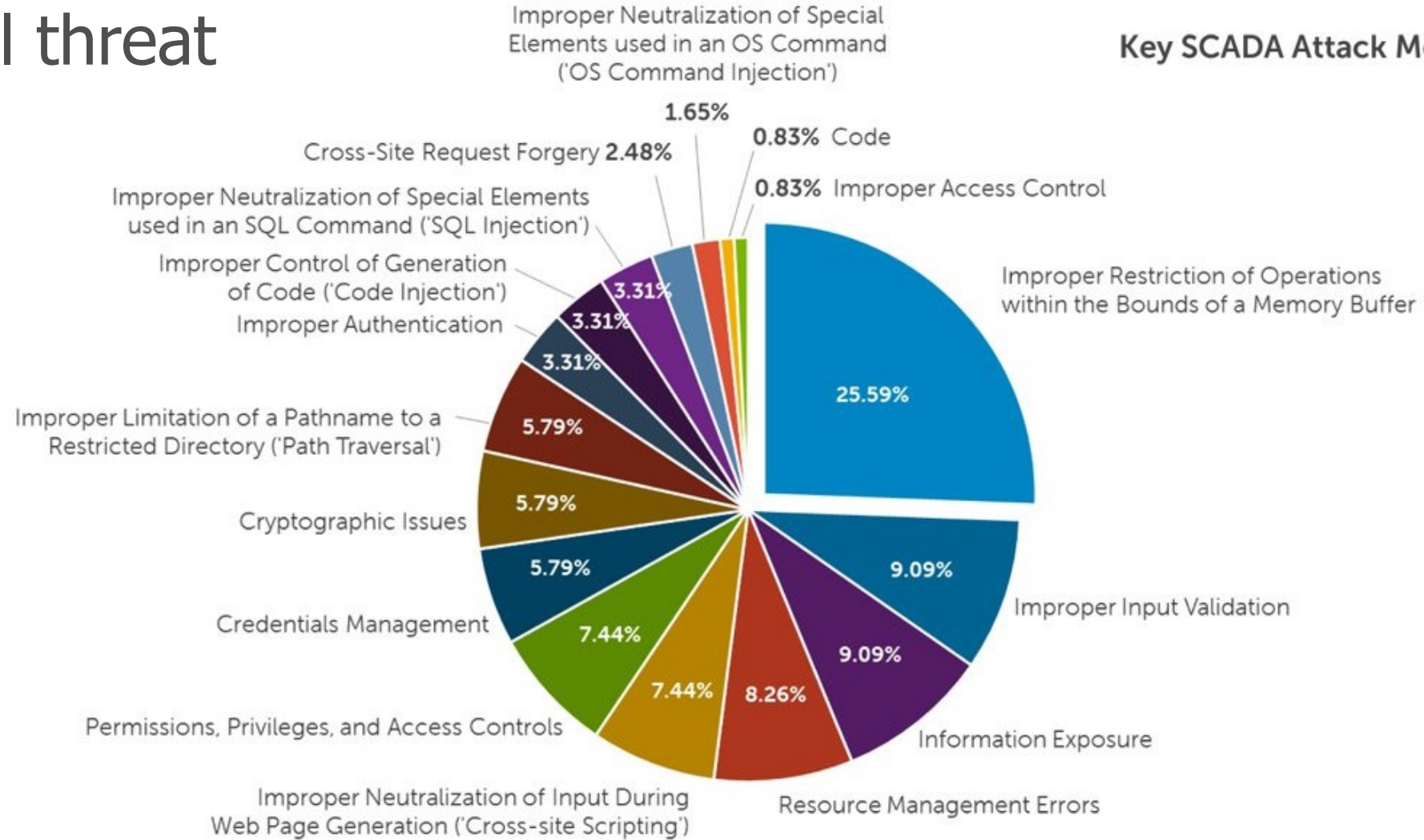
- **2000** – Maroochy Shire (QLD) Sewage Spill
- **2003** – Zotob Worm and Chrysler
- **2010** – Stuxnet
- **2014** – Dell SonicWall said “SCADA attacks increase from 91.676 in 2012, to 163.228 in 2013, up to 675.186 in 2014.
- **2017** – WannaCry ...



facts

a real threat

Key SCADA Attack Methods



Dell SonicWall - 2015

why SCADA's are impacted ?

greater openness

1. Previously SCADA **were** specifically **isolated** and separated from IT environment
2. Throughout years SCADA systems are changing from **traditional proprietary** protocols to **Internet Protocol (IP)** based systems
3. We have entered a **convergence** phase between OT (Operational Technology) and IT (Information Technology)
4. **Connectivity** is increasing
5. Modern IP-based SCADA systems are now **inheriting** all the vulnerabilities associated with IP

understanding SCADA cyber risks

Category	SCADA	Corporate IT
Confidentiality	Low	High (where determined by data classification)
Integrity	Very High	Low to Very High (depending on specific system)
Availability	<ul style="list-style-type: none"> • Rebooting and momentary downtime usually not acceptable • Operates on philosophy of seven nines (99.99999 % uptime) 	<ul style="list-style-type: none"> • Rebooting acceptable in specified time windows. • Outages may be tolerated (as determined by business impact)
Impact of System Failure	Regulatory noncompliance, environment, loss of life or serious injury, production or service delivery failure affecting the territory served	Business Operations (as determined by Business Impact Assessments related to the specific system)
Time-Criticality	Response to human interaction and emergency situations is critical	System-dependent, but generally less time critical
Performance	<ul style="list-style-type: none"> • Must be “real-time” • Latency and jitter are not acceptable • Moderate throughput 	<ul style="list-style-type: none"> • Must be consistent • Latency and jitter may be acceptable • High throughput may be required
Prioritising Risk Controls	<ul style="list-style-type: none"> • Safety always takes priority • Process protection (integrity and availability) are the next primary factors • Fault tolerance is essential 	<ul style="list-style-type: none"> • Protecting data confidentiality and integrity are primary • Fault tolerance less important



building a SCADA

cybersecurity framework

03

Security principles

1. Availability
2. Integrity
3. Authentication
4. Confidentiality
5. Traceability



global approach

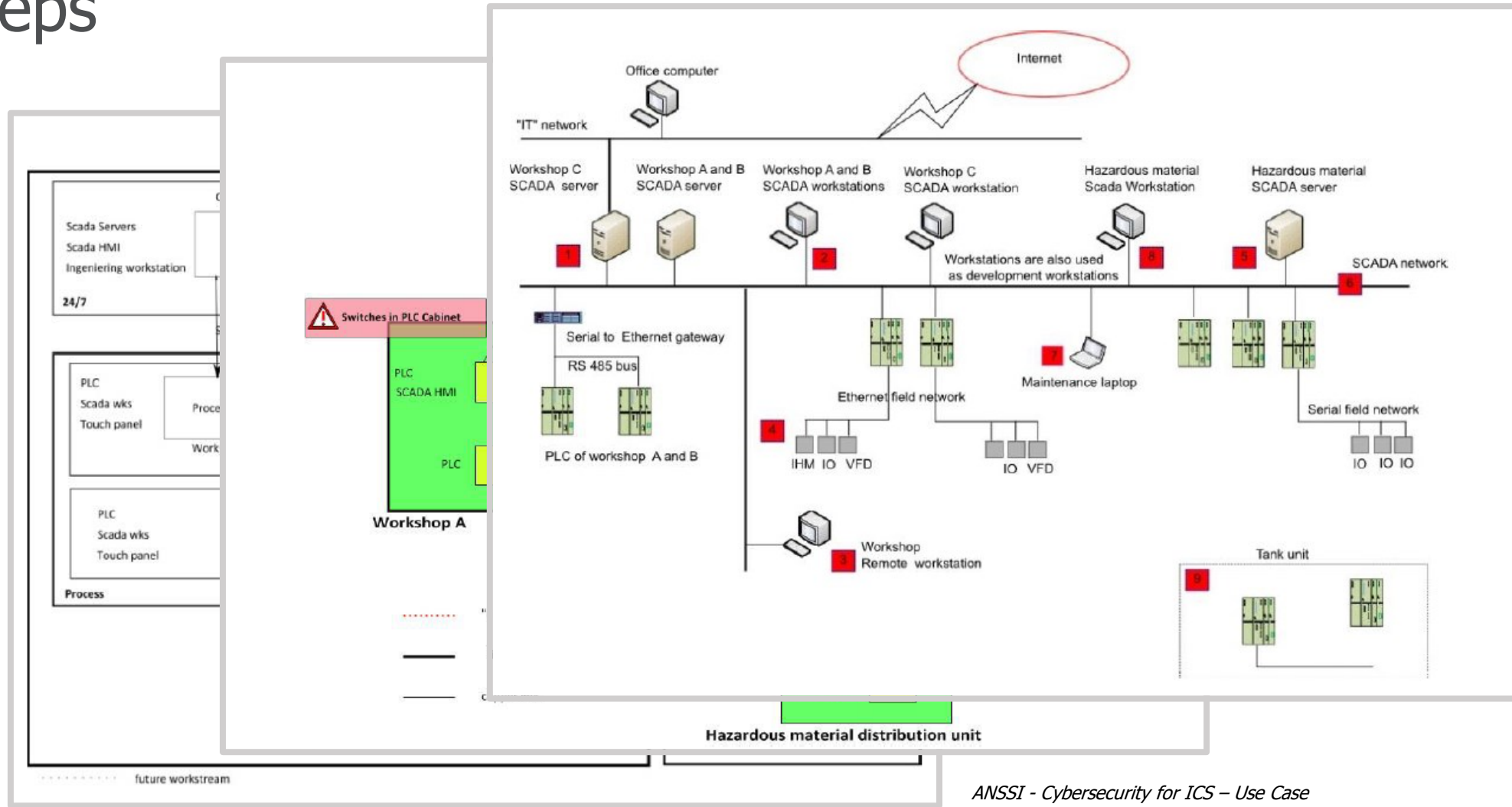
3 steps

- 1. Assemble** a physical and logical mapping of plant and the data streams and then establish level of criticality for each one
 - Understand business needs
 - Take inventory of devices and services
- 2. Evaluate** of sensitivity levels and initial analysis of existing vulnerabilities
- 3. Analysing** the new requirements would allow to identify the necessary security measures (technical and organisational) to reduce discrepancies and the potential impacts on the plant.



global approach

3 steps

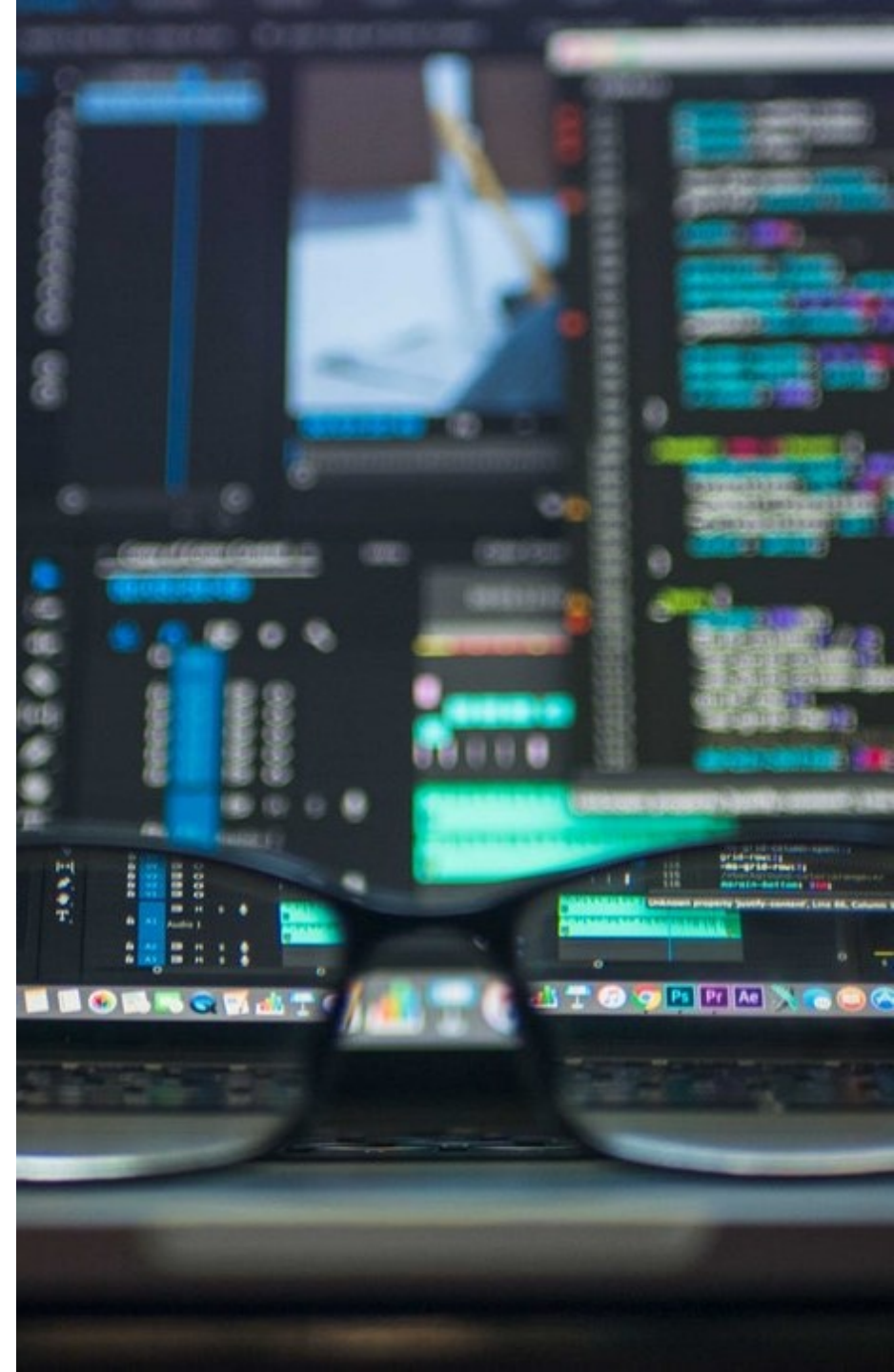


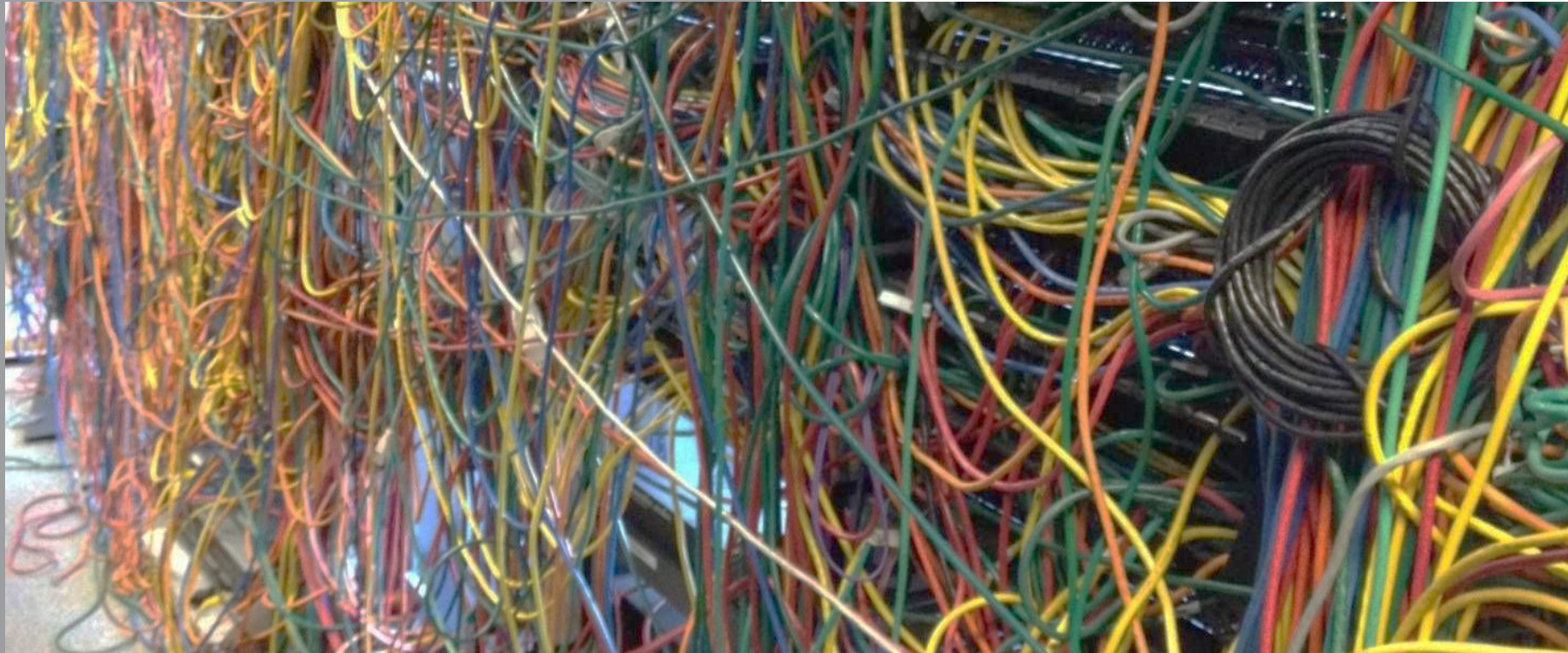
ANSSI - Cybersecurity for ICS – Use Case

target

ideal SCADA security framework

- Comprehensive and evolving to meet a changing threat profile
- Meets the availability requirements of SCADA systems
- Meets the risk management and performance requirements typical of SCADA systems
- Scalable to meet different standards and regulations as applicable

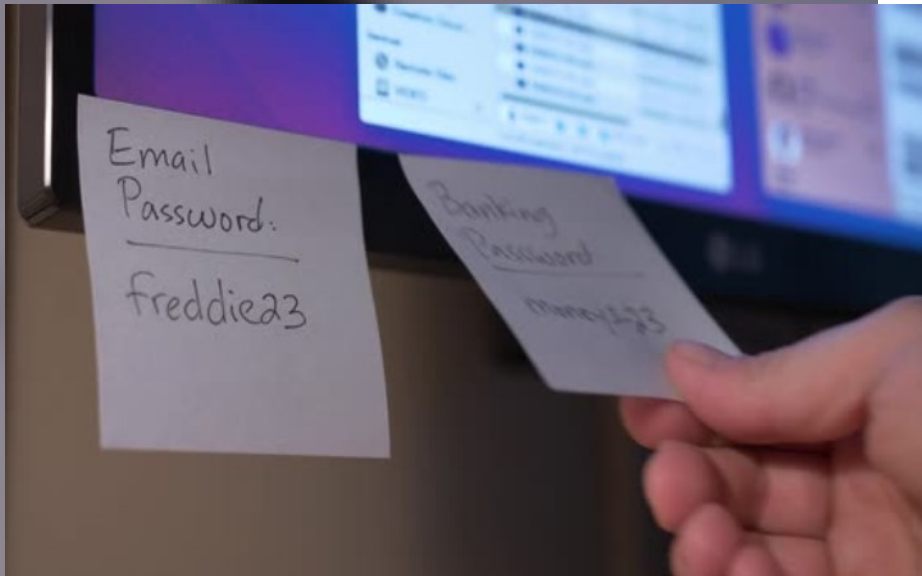




the basics

04

SCADA most common threats



1. Denial of service
 1. Sending incorrect requests
 2. Using a corrupted configuration file
2. Alteration of the streams
3. Corruption of the configuration
4. Identity theft

basics for a clean SCADA infrastructure

the basics

1. Up to date operating system
2. Policy, standards and exceptions : a smart and real configured domain directory
3. Access to the SCADA machines must be restricted
4. Set up a system log monitoring policy



defining the right

SCADA application roles recommendation

5 profiles

Developer

Design,
development and
application
maintenance

Operator

Application user

Backup operator

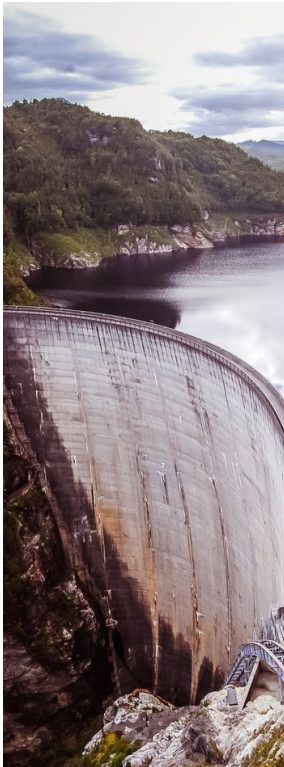
Backup
application data

Administrator

Application
machines
administration :
SCADA product
and DataBase
installation

Domain Administrator

AD groups and
users
management

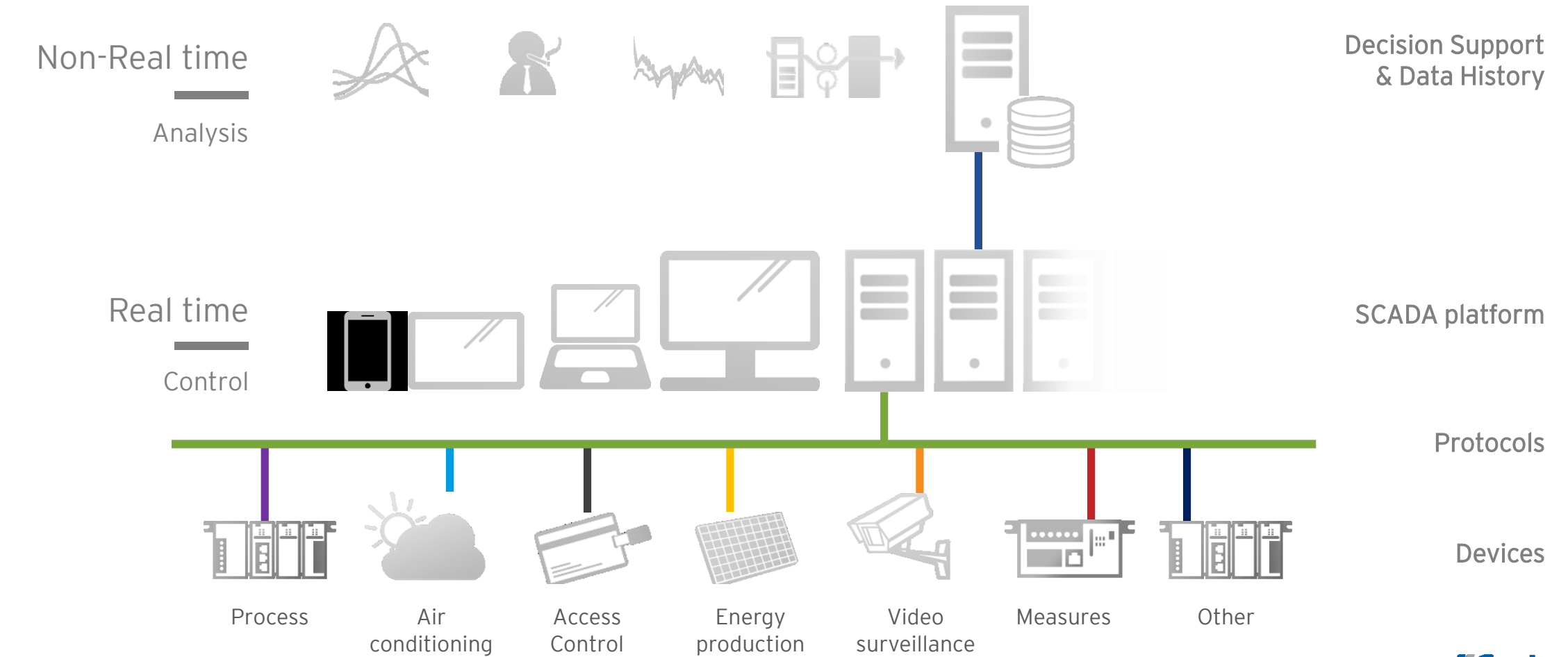


the SCADA streams

- Industrial specific protocols (Profibus, CAN, DeviceNet, ...)
- Ethernet protocols (Modbus TCP, BACNet, IEC61850, ...)
- Web Services
- OPC UA DA (web services, DCOM,...)
- Wifi
- ...

global scheme

SCADA system streams



focus on a secure protocol

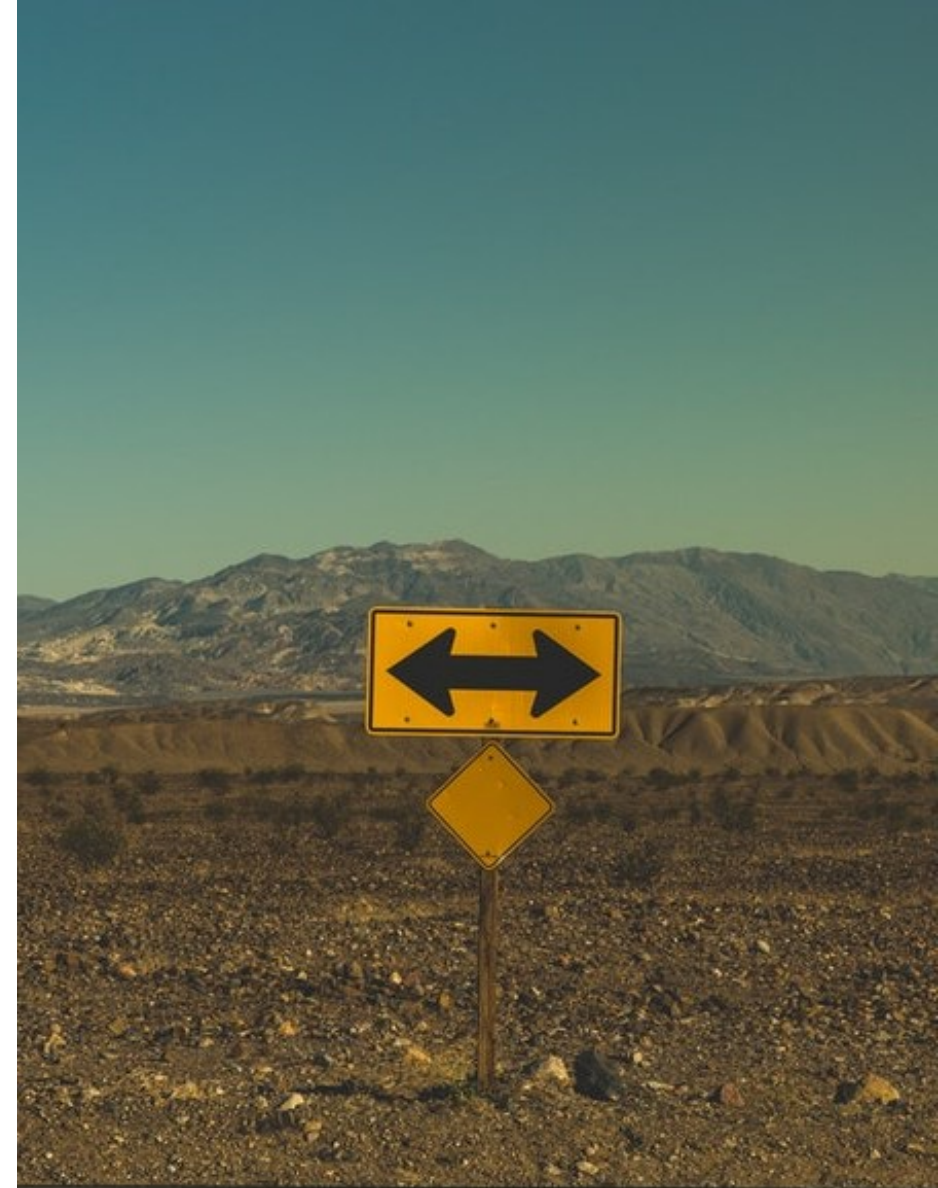
OPC Unified Architecture

1. Link securization
2. Application Authentication
3. User Authentication
4. User Authorization
5. Server Availability
6. System Auditability



methodology

- Dedicated and isolated testing platform from the SCADA network :
 - Develop the application
 - Test the application
 - Enable application security
- On site :
 - Install the SCADA solution
 - Secure the machines
 - Secure exchanges between machines
 - Deploy the application on site



reducing surface attacks

summary

1. Network partitioning (DMZ, ...)
2. Hardware limitations (get rid of USB key,...)
3. Hardening Windows
4. Crypto Certificate management (EKCM)
5. Deep defense
6. Action processes in case of attack
7. Continuity plan
8. Software management



CODRA

'cyber-strategy'

US

cybersecurity

Concerns us all !

Editor

Systems infrastructure
SCADA & Automation
R&D process

Integrators

Profile management
Application design
Development process

Customers

Security of access
Directory management
Operating process





is working with ANSSI*

to qualify our Industrial Supervision solution

*"Qualification is a process that certifies the **robustness** level of a product or service and the level of **confidence** in a product or service supplier"*
(ANSSI 274/ANSSI/SDA QUAL-PROD-PROCESS/1.0)

