Cybersecurity Institute
Univ. Grenoble Alpes

Cybersecurity of industrial systems. Open problems and some ideas.

Stéphane Mocanu,
Laboratoire d'Informatique de Grenoble/INRIA
CTRL-A
stephane.mocanu@inria.fr

LIG

Inria
INVENTEURS DU MONDE NUMÉRIQUE

A cross-disciplinary viewpoint

- process
- control system
- computer science

INDUSTRIAL CONTROL SYSTEMS (SCADA)

Cyberphysical Systems

IT

Remote connections

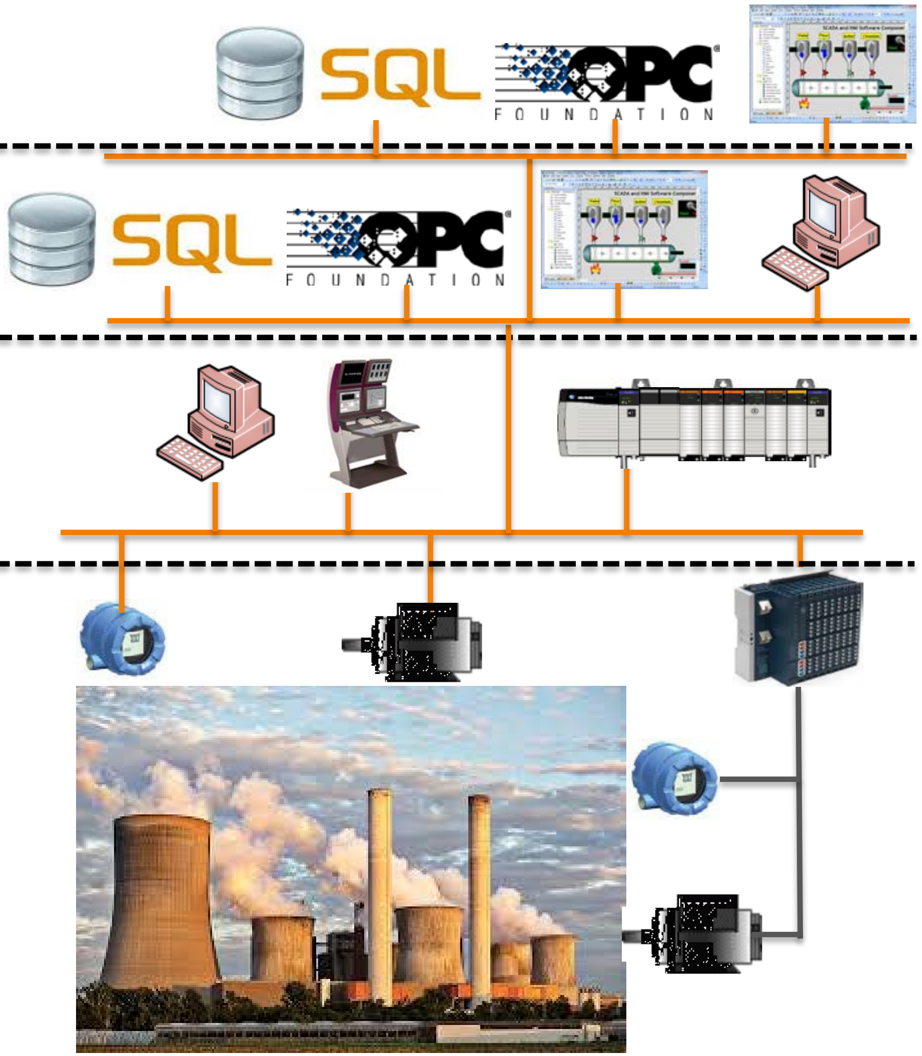
Supervisory and journaling
No real-time

OT
Operational Technology

Controllers
Soft real-time communication

Intelligent sensors and actuators
Hard real time communication

Main asset : the physique plant



SOME DEFINITIONS AND FACTS

- **Cybersecurity triad revisited**
  - **Availability is paramount (keep running under attack)**
  - **Non-repudiation may be crucial (emergency stop)**
  - **Real-time properties are important**
  - **Reaction time to attacks is very short**
- **Attacks targets the physical process**
  - **Stuxnet, BlackEnergy, Industroyer, ….**
- **Behavioral classification**
  - **Event-based : sequential systems (aka Manufacturing) PLC controlled**
    - All manufacturing systems
  - **Time-based : continuous systems (aka Process)**
    - Feedback control based processes
    - Electrical transport and distribution (hybrid)

THREATS 2019

- **Primary attacks (Source BSI-CS005E Top 10 Threats and Countermeasures 2019)**

Top 10 Threats	Trend since 2016
Infiltration of Malware via Removable Media and External Hardware	↗
Malware Infection via Internet and Intranet	↗
Human Error and Sabotage	↑
Compromising of Extranet and Cloud Components	↑
Social Engineering and Phishing	↘
(D)Dos Attacks	↑
Control Components Connected to the Internet	→
Intrusion via Remote Access	→
Technical Malfunctions and Force Majeure	↘
Compromising of Smartphones in the Production Environment	→

- **Secondary attacks**
  - ▶ **Privilege escalation**
  - ▶ **Unauthorized access to internal systems**
  - ▶ **Manipulation of fieldbus communication**
  - ▶ **Manipulation of network components**

Important remark

Recent mediatic events are Big Game Hunting

- Norsk Hydro
- Southwire
- Altran
- CHU Rouen
- Bouygues Construction

60% RDP attacks

RAAS is today golden mine

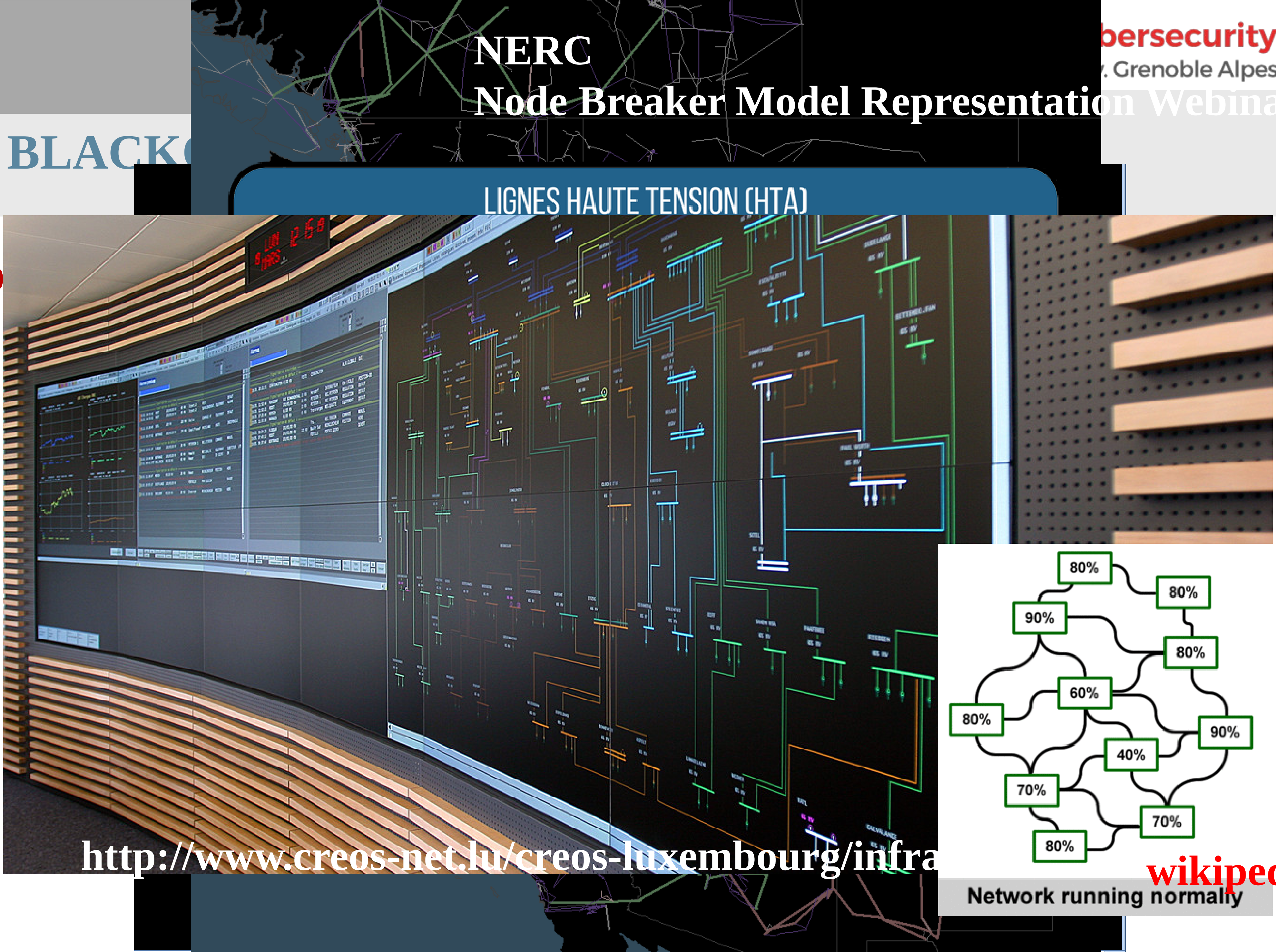
Source ANSSI CERTFR-2020-CTI-001

BEYOND RANSOMWARE ATTACKS

- **Process oriented attacks**
  - **Malicious controls sent to the process (actuators) using legal frames**
  - **Injection of false data sensors using legal frames**
  - **Exploitation of IT/OT and physical process vulnerabilities**
- **Leads to**
  - **Loss of view**
  - **Loss of control**
  - **Physical process damage**
- **Proof of concept**
  - **“Aurora vulnerability” (thunderbolt-like effect attack) – Idaho National Laboratory**
    - Current spikes on the secondary circuit of a generator, faster that the protections relay timing
  - **Stuxnet**
  - **Blackout 2003**

U.S. BLACKO

■ 200



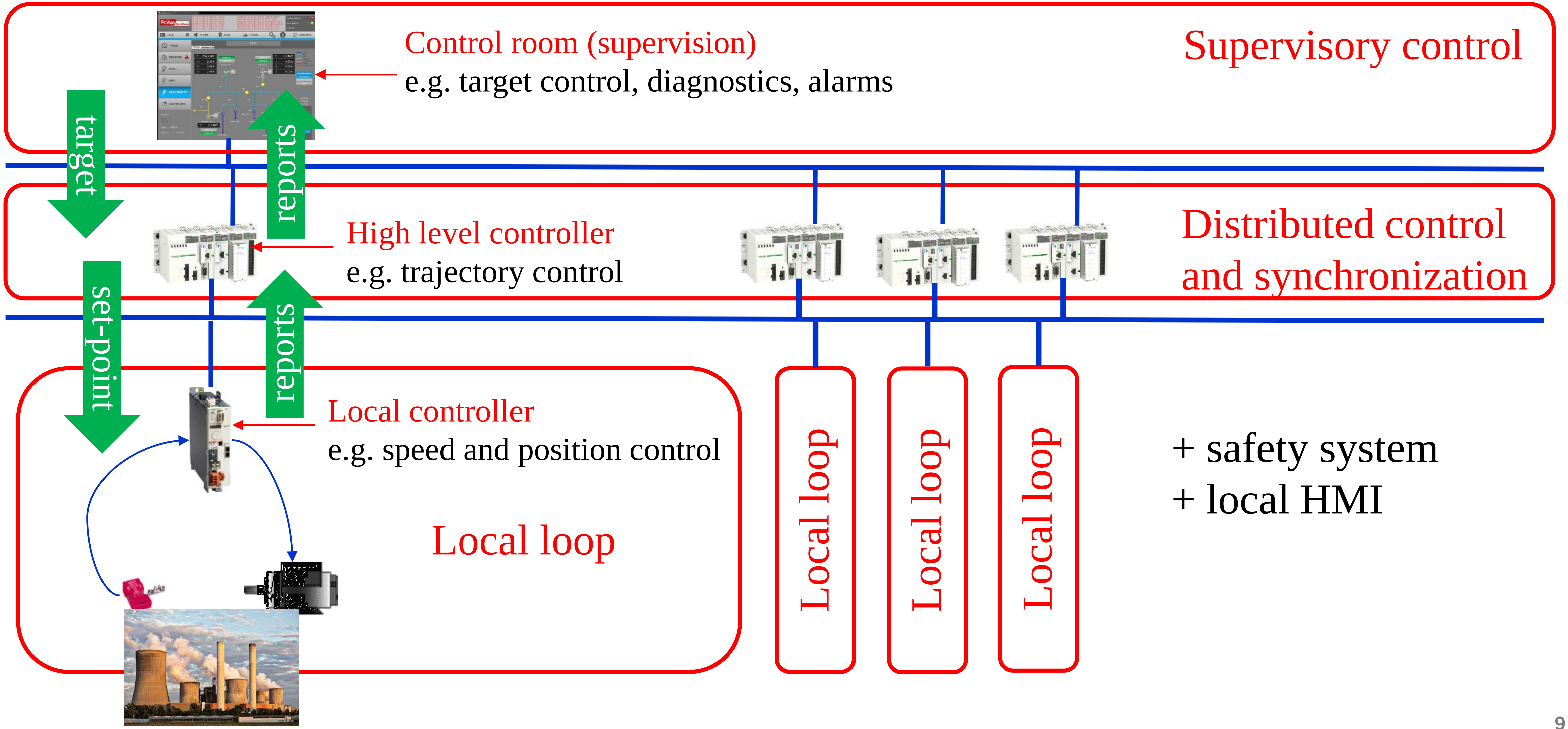
wikipedia

BLACKOUT 2003

- Starting event : (accidental) false sensor data injection
- Exploits cyber et physical system vulnerabilities
- Loss of view (false supervisory view)
- Loss of control
- Physical system damage
- Human causalities (collateral)

- No protocol syntax or semantics violation

THE SYSTEM APPROACH



SYSTEM APPROACH

- **Everything, including communication system is part of the control function**
  - Communication protocols are control oriented
- **There is strong interdependence between control elements**
  - Some control functions are distributed
- **Security deployment has to be global**
  - System oriented not global oriented
- **The final target of the control function is the physical process integrity**
  - Physical process model has to be taken into account

LAST DECADE TECHNICAL ADVANCEMENT

- **Lots of ICS cybersecurity standards (IEC 61443, IEC 62351, etc)**
- **Improved device security**
  - Signed firmwares
  - Some secured communication protocols
  - Logging systems
- **Device and system access control**
  - RBAC
- **IDS**
  - Flow inspection based
- **Industrial protocols support in firewalls**
  - Is this realistic ?
- **Data diodes**

AND SOME MYTHS

Controller side

- **Secured industrial communication protocols**
  - Not interoperable
  - Initial exchanges still using unsecured Ethertype communications
- **Certified PLC**
  - Control devices heavily relay on time synchronization
  - Interoperability
- **Certified SCADA**
  - Support for legacy (unsecured protocols) is unavoidable

Countermeasure side

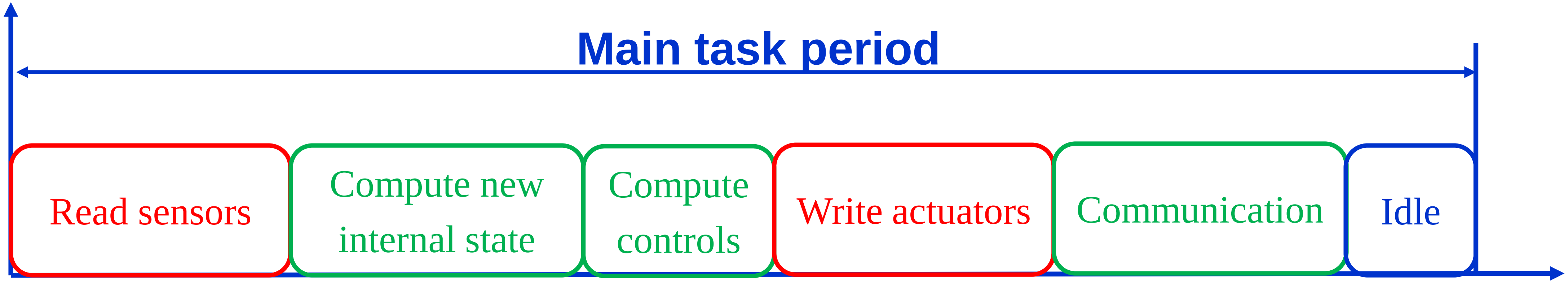
- **Learn control model from (5 minutes) traffic aka “all by AI legend”**
  - Transients may take hours
  - Controllers are intended to compensate perturbations
    - Abrupt changes in control values are normal

Some open problems : a personal view

From controller to system

CONTROLLER : (CYBER)-SAFE PROGRAMMING LANGUAGES ?

- **Controller periodic task**



- **Programming languages**
  - **5 normalized (IEC 61131)**
    - Sequential Function Chart (SFC)
    - Instruction Logic (IL)
    - Structured Text (ST)
    - Function Block Diagram (FBD)
    - Ladder (LD)
  - **A non-standard one : Continuous Function Chart (CFC)**

HOW RESILIENT IS PLC PROGRAMMING ?

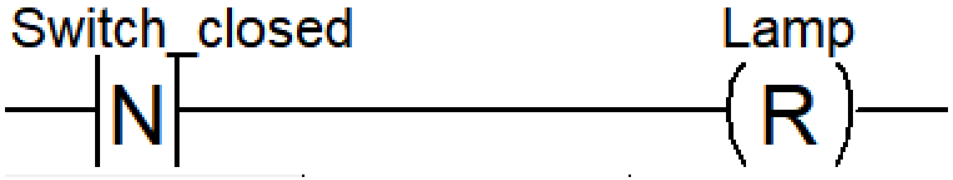
- **A simple control program**

Reads : if the switch is closed activate the lamp for one cycle

Implicit action : if the switch is open do not activate the lamp

- **Alternative program**

Reads : on a raising edge of the switch set the lamp on (permanently)

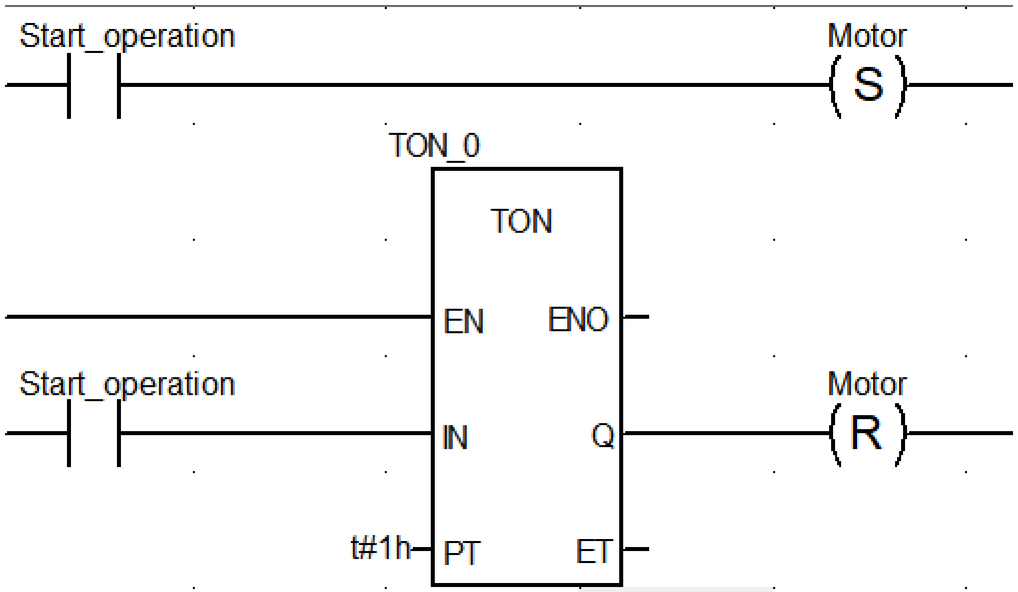


Reads : on a falling edge of the switch set the lamp off (permanently)

- **First solution is more resilient to cyberattacks than the second one !**
- **Open problem : evaluate the 61131 programming languages and define cybersecure programming patterns**

WRITE YOUR VARIABLES EVERY CYCLE ?

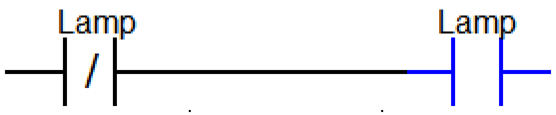
- **Not always possible**
- **What about timed operations ?**



Reads : Start a motor and a timer
At timeout : stop the motor

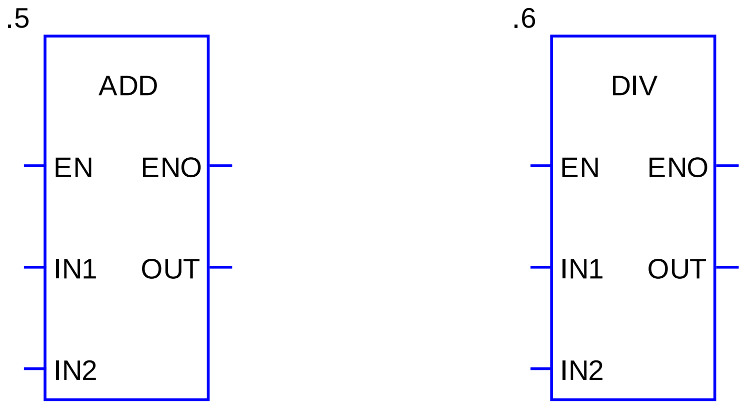
Between “Start” and TON.Q variable Motor is never refreshed !

- **Homework : is the following program safe ?**



IF IS NOT BOOLEAN THEN IS A FUNCTION !

- Traditional PLC programming languages (LD, IL) are digital logic based
- Everything else (e.g. mathematical operations) are (graphical) function calls



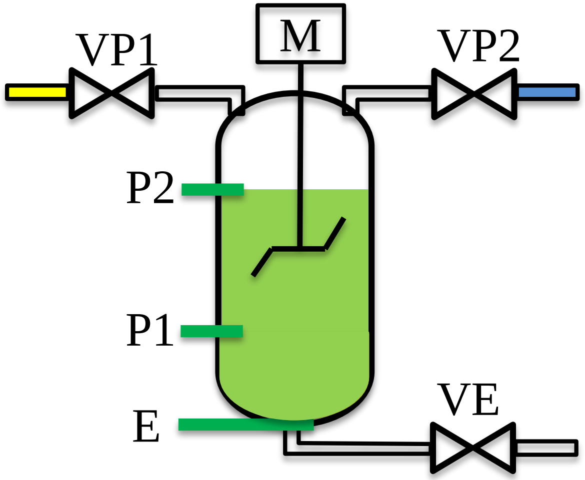
- Decompilation shows that parameter values are not checked but types are
  - overflow and divide by zero are possible, but apparently handled
- Open problem : tools for FB vulnerabilities check
  - Static analysis (decompilation) possible
  - Needs an execution platform for dynamic analysis
- Open problem : embedder OS vulnerabilities
  - often VxWorks (commercial version 7, PLC manufacturer version 3.10 or earlier)
  - development libraries may include old open source code (e.g. 2002 versions found in 2019)

NETWORK LEVEL : PROCESS-AWARE INTRUSION DETECTION

- Only network-based IDS are possible today
  - End devices are too loaded to support host-based IDS
- Network is part of the control function
  - Process-aware detection need to include the process model
- Open problem : cyber-physical models for intrusion detection
  - Sequential systems
  - Continuous systems
  - Control functions modeling
- Open problem : distributed detection
- Open problem : cross-domain correlation
  - Multiple attack surfaces
  - SCADA log correlation

CYBER-PHYSICAL MODELS: SEQUENTIAL SYSTEMS

- **Sequence attacks**



Normal behavior
T0: E↓, VP1↑
T1: P1↑, VP1↓, VP2↑
T2: P2↑, VP2↓, M1↑
T3: M1↓, VE↑
T4: P2↓
T5: P1↓
T6: VE↓

Qualitative Attack
VP2↑
VE↑

Quantitative Attack
M1↓
VE↓VE↑VE↓VE↑

- **PhD Oualid Koucham (co-supervised UGA/CentraleSupelec/DGA)**
  - ► Security patterns LTL (Dwyer) and MTL (Konrad)
  - ► Runtime monitoring
  - ► Cross-domain correlation (monitors and network activity)

CYBER-PHYSICAL MODELS :CONTINUOUS SYSTEMS

- **Which security properties**
  - Stability
  - Response-time
  - Boundedness
  - Static error
  - …..
- **Which formalism**
  - STL seems to be a good candidate
  - Monitorability of security properties
- **Handle the under-sampling problem**
  - At network level signals are sampled at a lower frequency than the controller
  - Degraded view of the dynamics
- **Correlation**
  - Correlate with diagnostic system (physical level system deviation detection)

CONTROL FUNCTIONS MODELLING

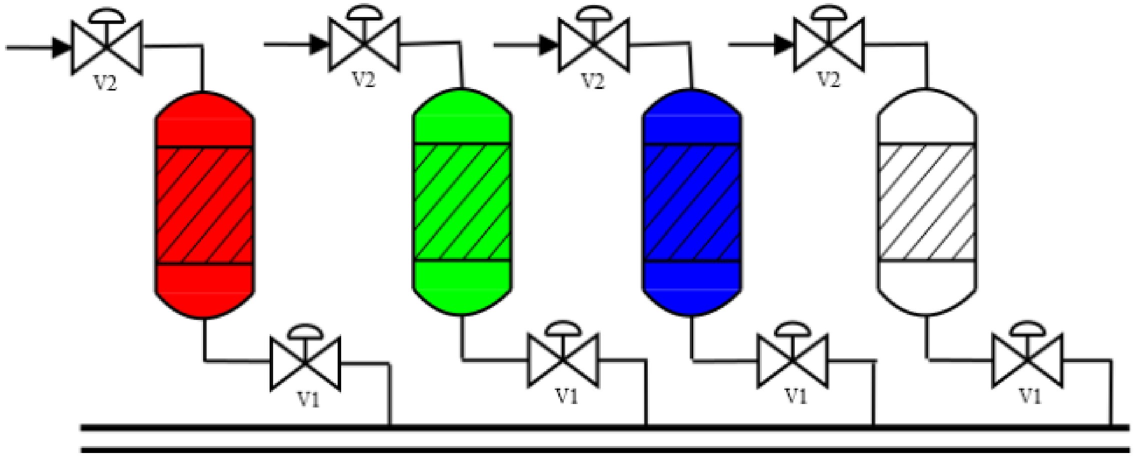
- **A general approach is difficult excepting for**
  - ▶ **Well known control functions (PID for instance)**
  - ▶ **Electrical grid protection functions**

RTE Substation Protection Automation and Control Systems IEC 61850 Model

- **Timed-hybrid system**
- **STL model or another logic ?**

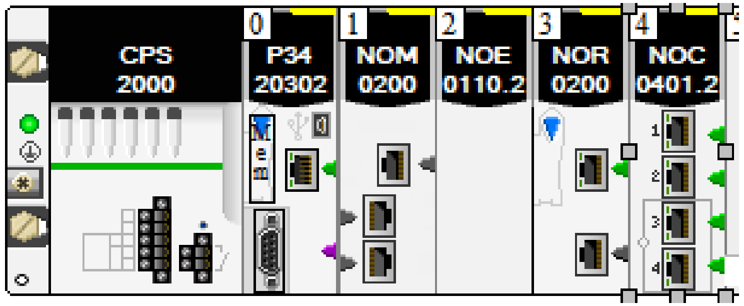
DISTRIBUTED DETECTION

- **In large systems distributed monitoring seems more reasonable**
  - Due to network segmentation
  - Large distances
  - A probe per local loop seems more reasonable
- **Some global security properties may not be decomposed in local properties**
  - “hierarchical detection” ?
- **Ex. Security property : “the four tank are not simultaneously empty” cannot pe locally decomposed.**



MULTIPLE ATTACK SURFACES

- **Modern devices are multi-network, and multi-protocol**



4 IP network interfaces
2 fieldbus interfaces
7 communication protocols

An internal variable may be accessed by different protocols at different addresses
In Modbus there are several different possible requests to write the same variable

Multinetwork-address normalization ?
Cross network attack scenarios ?

SYSTEM LEVEL: DSML

- Several configuration files available on devices
  - SCL, AutomationML, OpenPLC, etc
- Flow and network cartography, device configuration and versions

- Open problem: risk analysis oriented DSML
  - Automatic data extraction and architecture model construction
  - Risk assessment
  - Network and flow segmentation
  - IDS probes deployment policy

The end ?