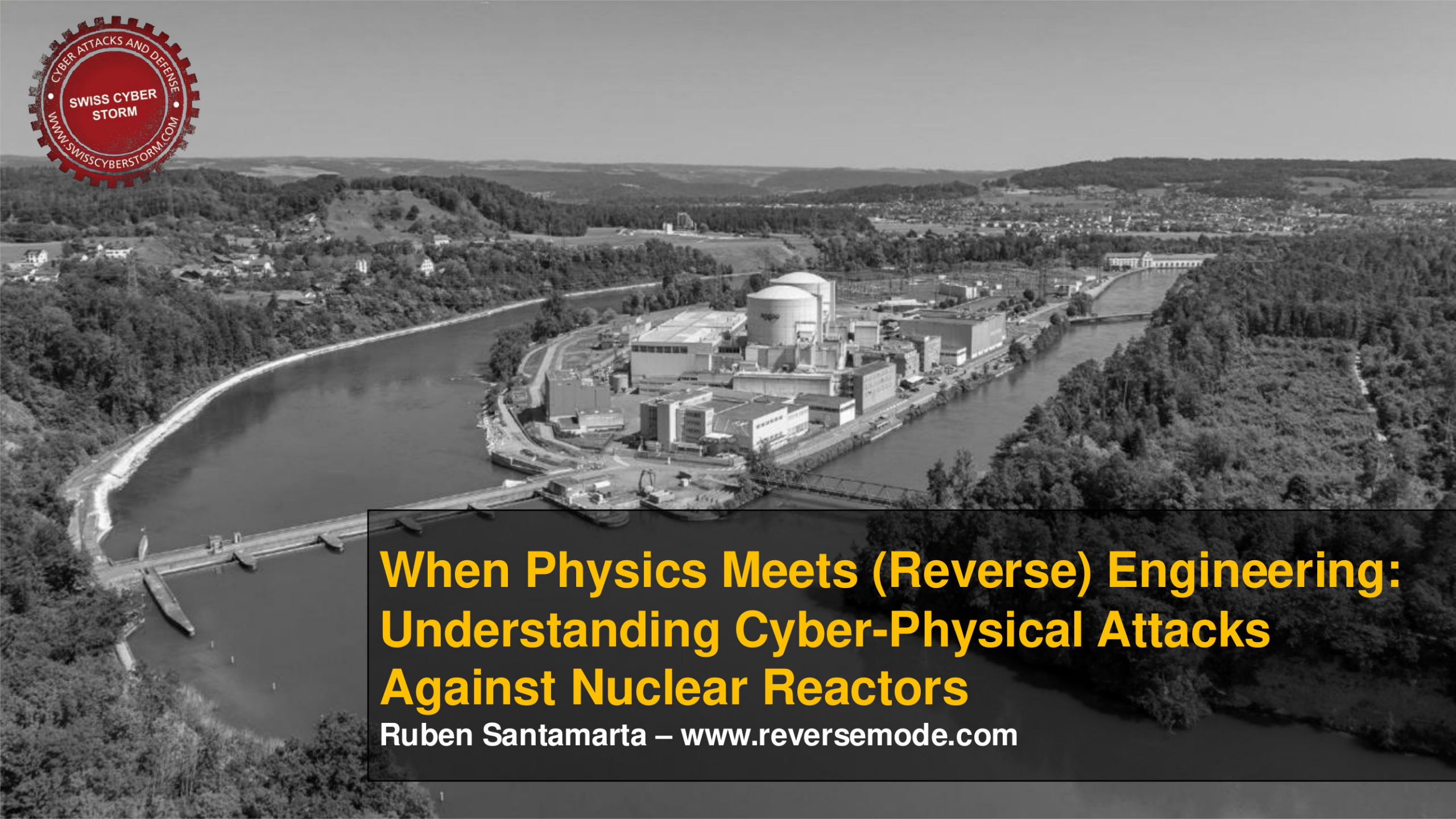


When Physics Meets (Reverse) Engineering: Understanding Cyber-Physical Attacks Against Nuclear Reactors

Ruben Santamarta – www.reversemode.com

OK Ruben, but what about AI?

Microsoft

Three Mile Island nuclear reactor to restart to power Microsoft AI operations

Google

Google to buy nuclear power for AI datacentres in 'world first' deal

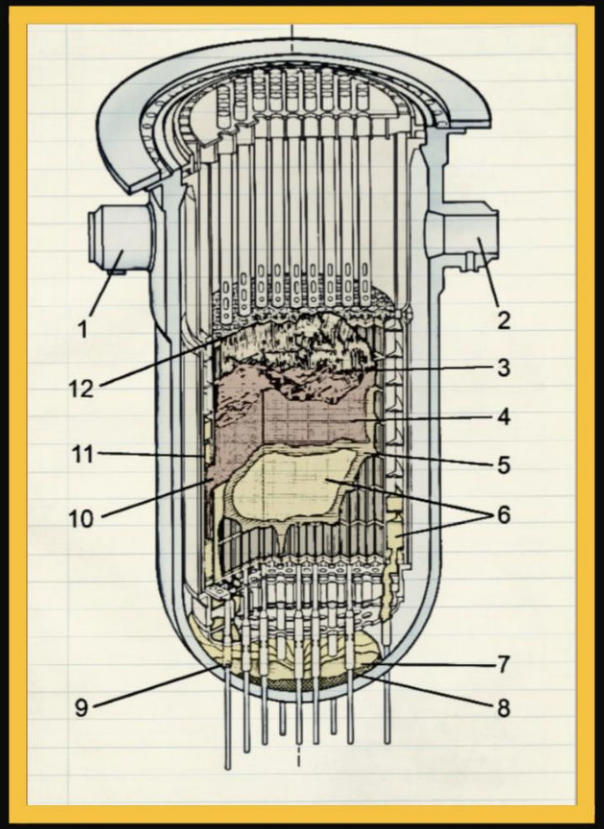
amazon

Amazon goes nuclear, to invest more than $500 million to develop small modular reactors

RESEARCH PAPER

- +130-Page
- Intro to Nuclear Physics And Nuclear Engineering
- Actors and Motivations
- Digital Instrumentation & Control System
  - Framatome's Teleperm XS (Safety)
- Cyber-Physical Attacks
  - Characterization
  - Implementation
  - Simulation

A Practical Analysis of Cyber-Physical Attacks Against Nuclear Reactors.



Ruben Santamarta
Security Research Services - www.reversemode.com

What is this talk about?

Hypothetical cyber-physical attacks targeting the safety systems of NPPs

INFORMATION

EDUCATION

NO FUD, NO DRAMA

WHAT ABOUT SWITZERLAND?

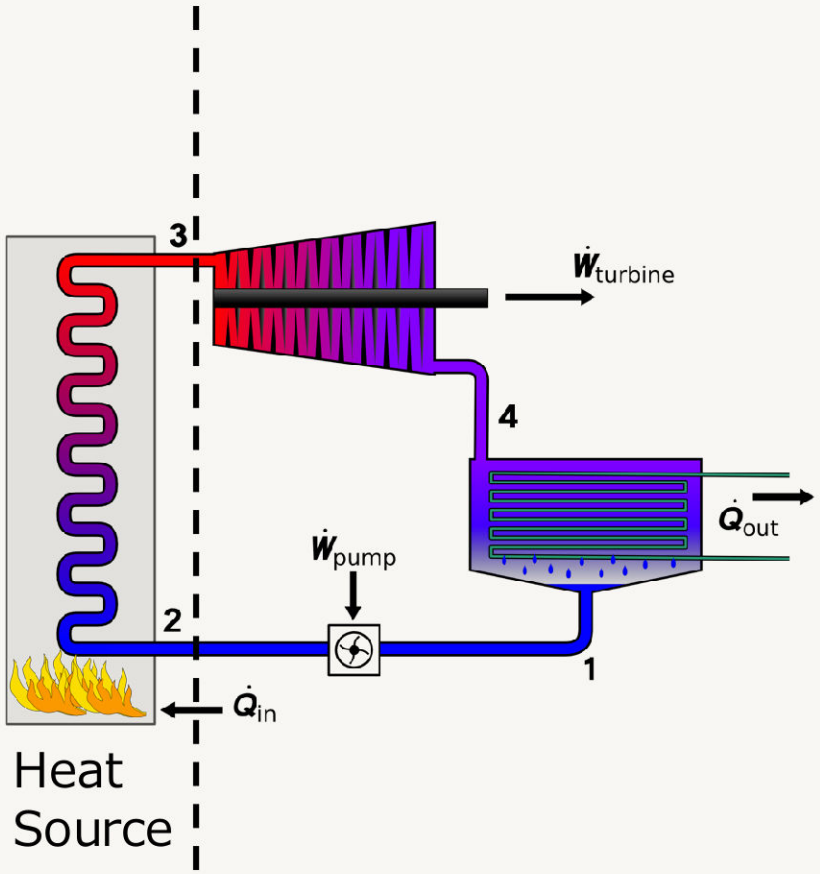
The RPS at **Gösgen** and **Beznau** is implemented using Teleperm XS.

Motivations

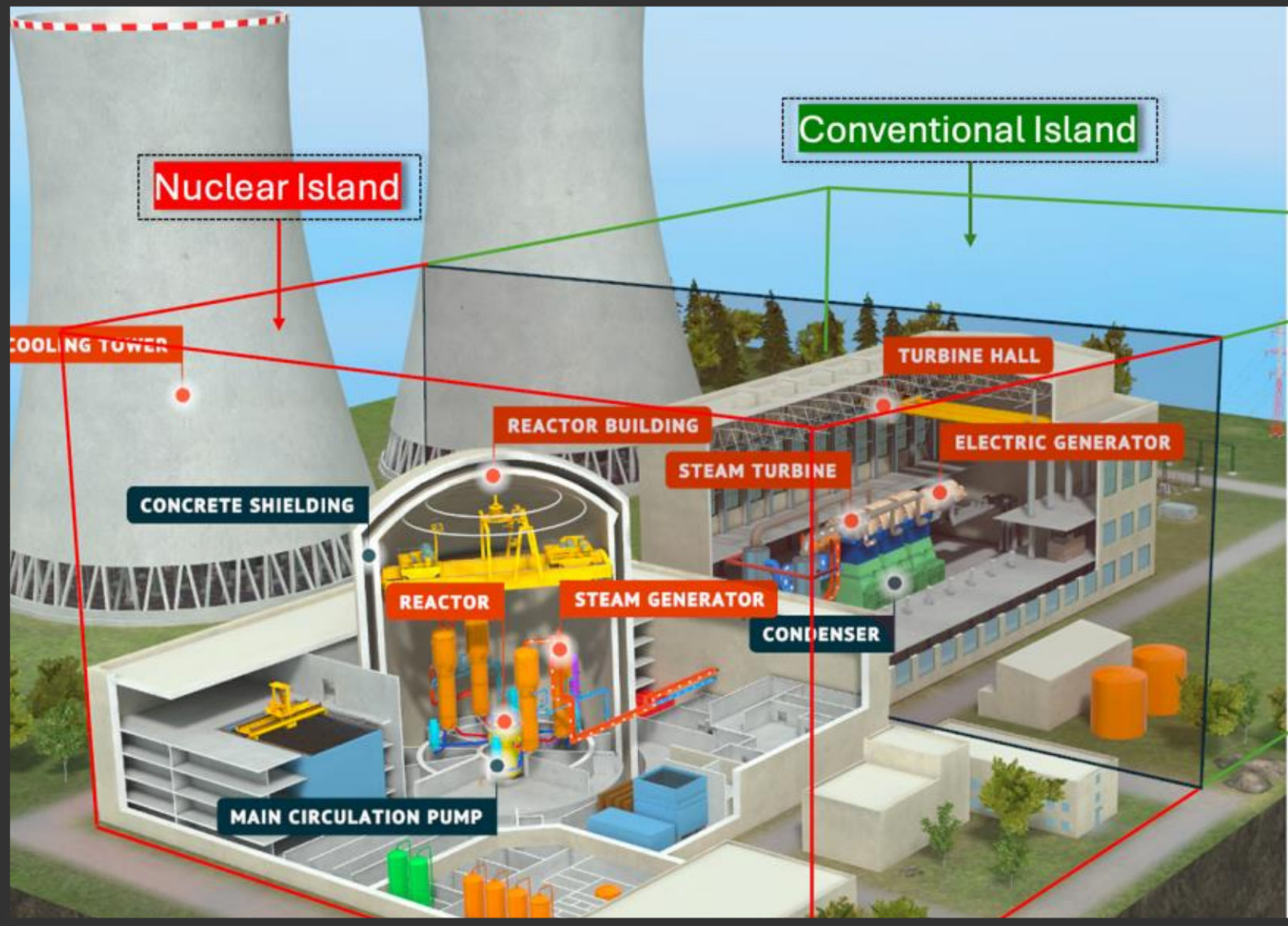
- **Potential for causing, through cyber means, widespread societal disruption, inflicting economic or military damage.**

- **The motivation to undertake such a massive effort needs to be proportional to the ability of its authors to deal with, or assume, the implications of this first-of-its-kind operation.**

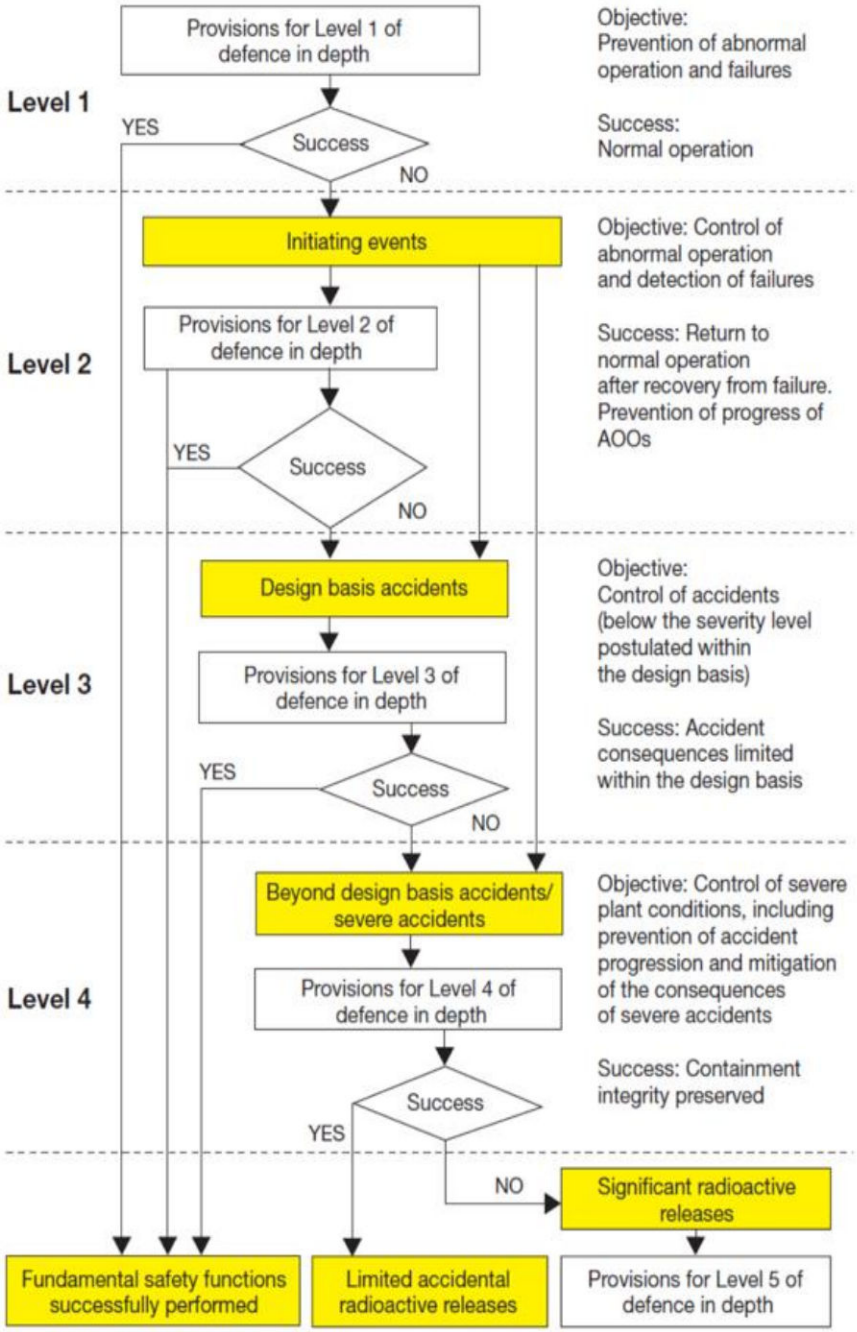
The Rankine Cycle

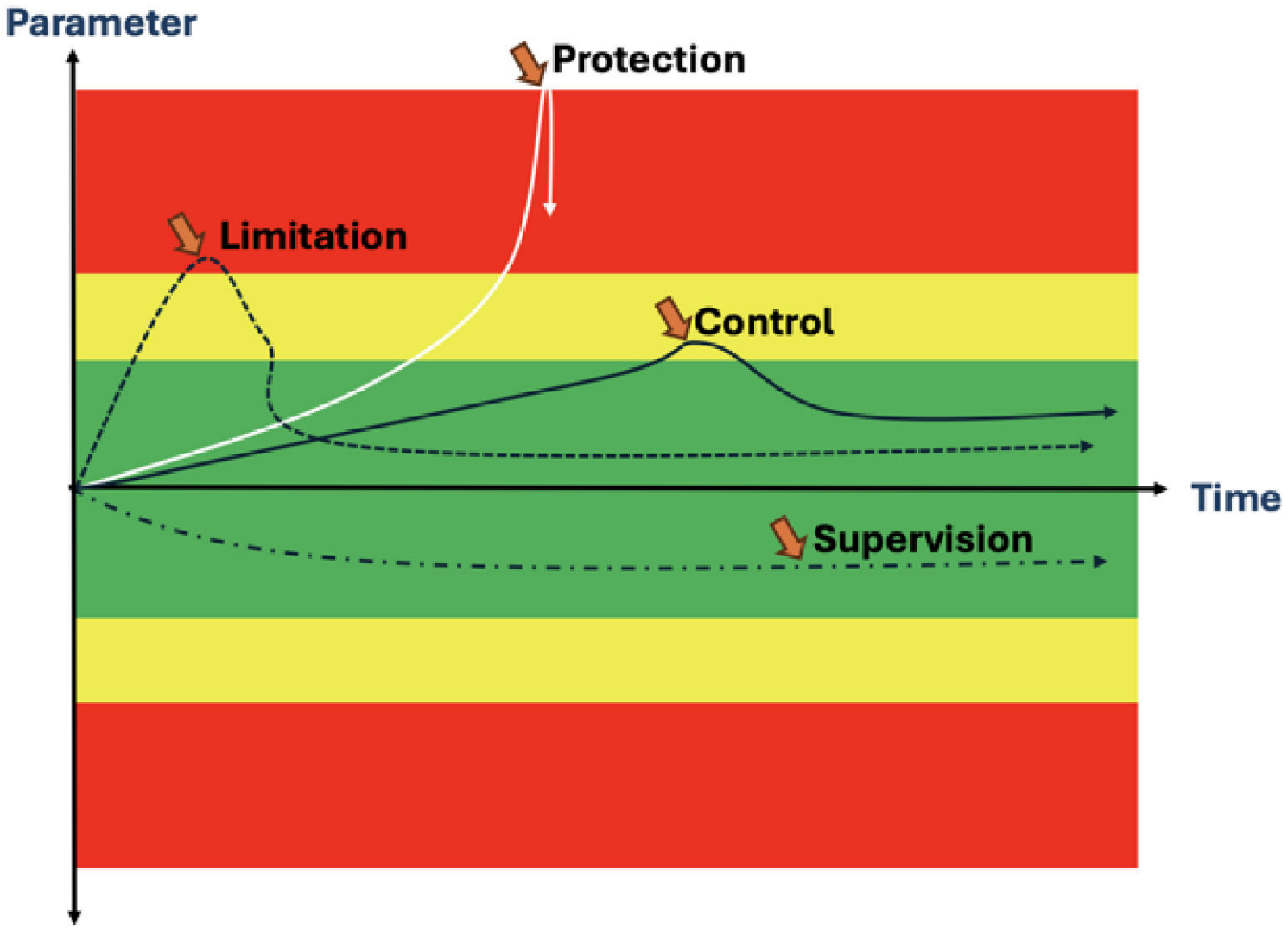


Nuclear Power Plant



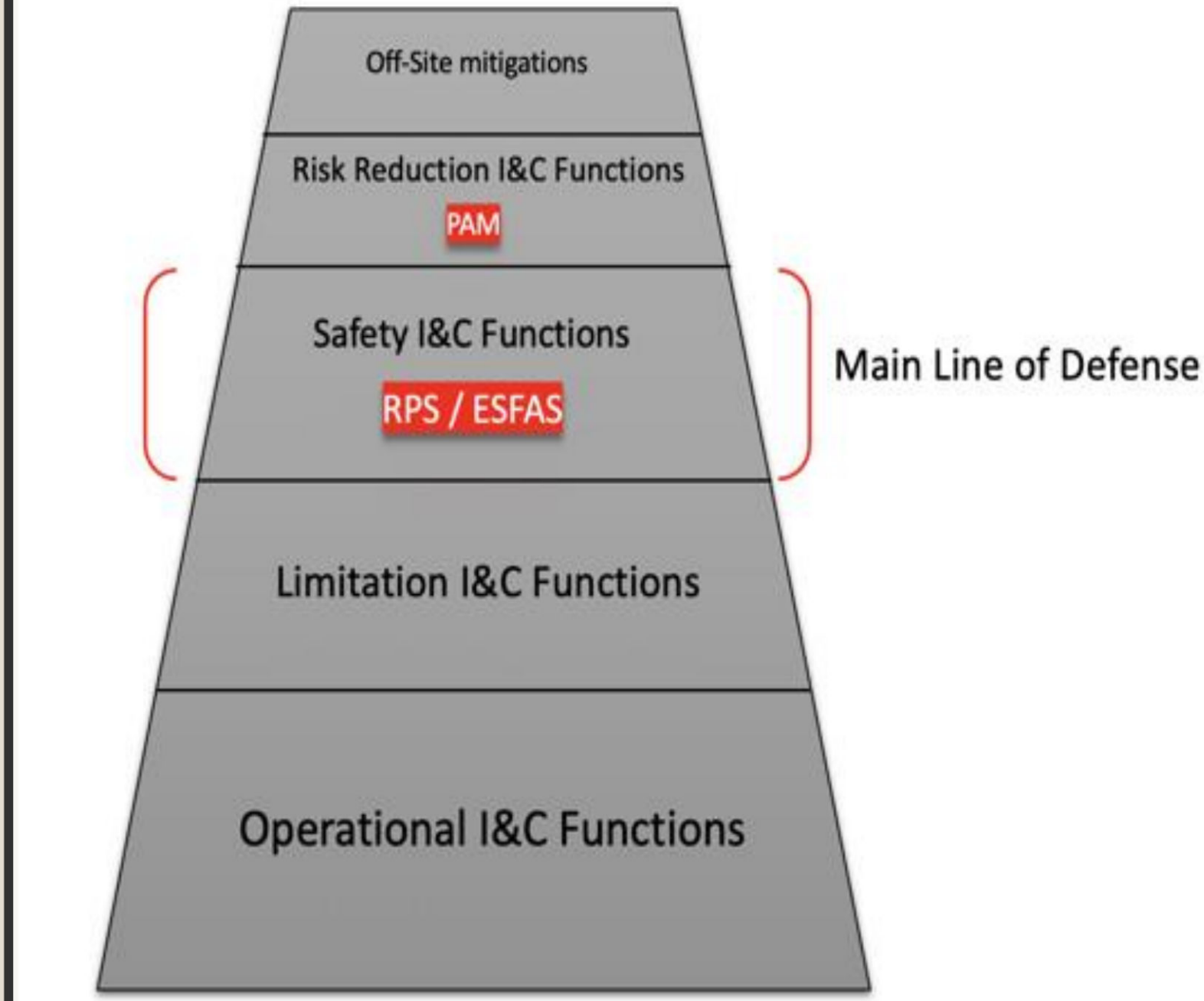
Defense in Depth and Diversity (D3)





Digital Instrumentation and Control Systems

TELEPERM XS


Off-Site mitigations
Risk Reduction I&C Functions
PAM
Safety I&C Functions
RPS / ESFAS
Main Line of Defense
Limitation I&C Functions
Operational I&C Functions

HOW IT STARTED

ebay Shop by category

teleperm xs

Category

All

Business & Industrial

PLC Processors

Other Automation Equipment

More +

Price

Under $350.00

$350.00 to $1,500.00

Over $1,500.00

$ Min to $ Max

85 results for teleperm xs

Save this search

All | Auction | Buy It Now | Condition | Delivery Options

Siemens Teleperm XS 6FK5206-8BE Safe

New (Other)

$3,165.24

or Best Offer

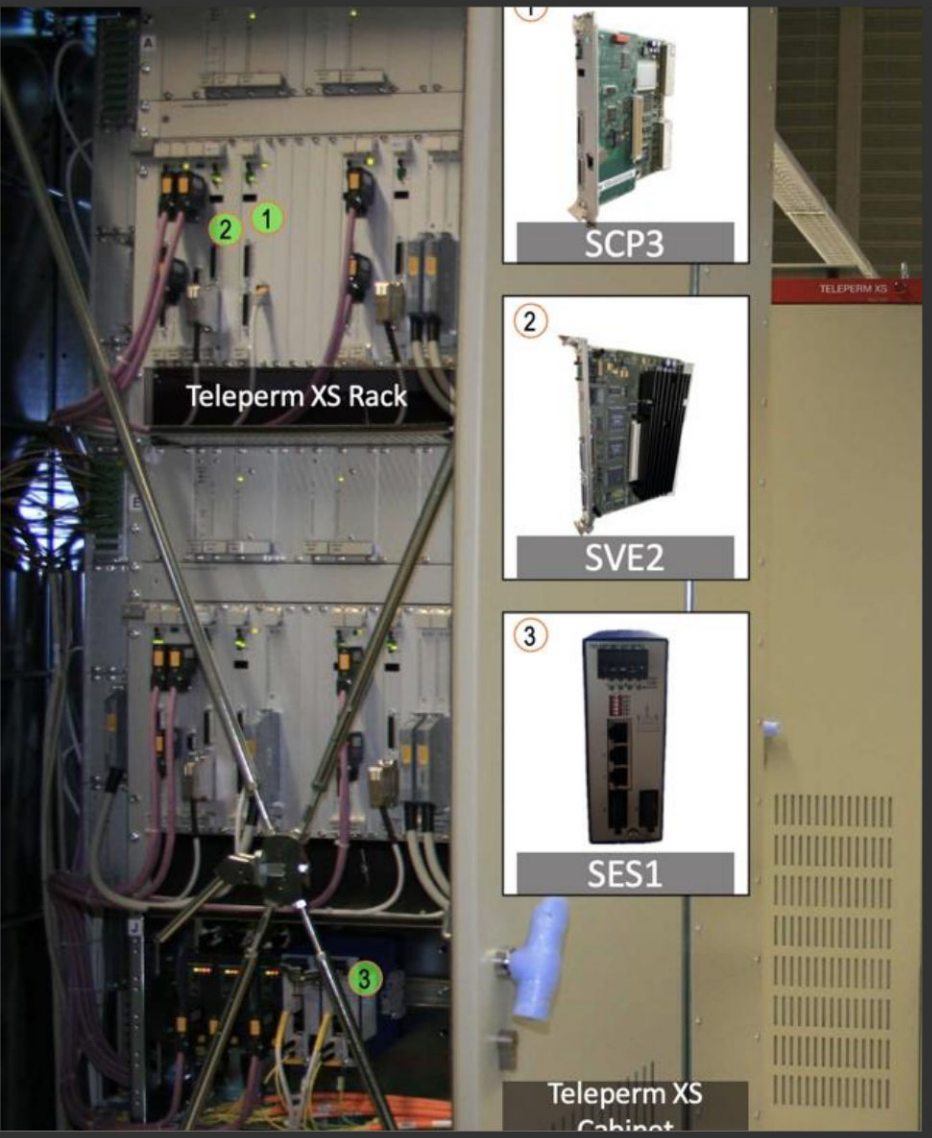
+$27.18 shipping

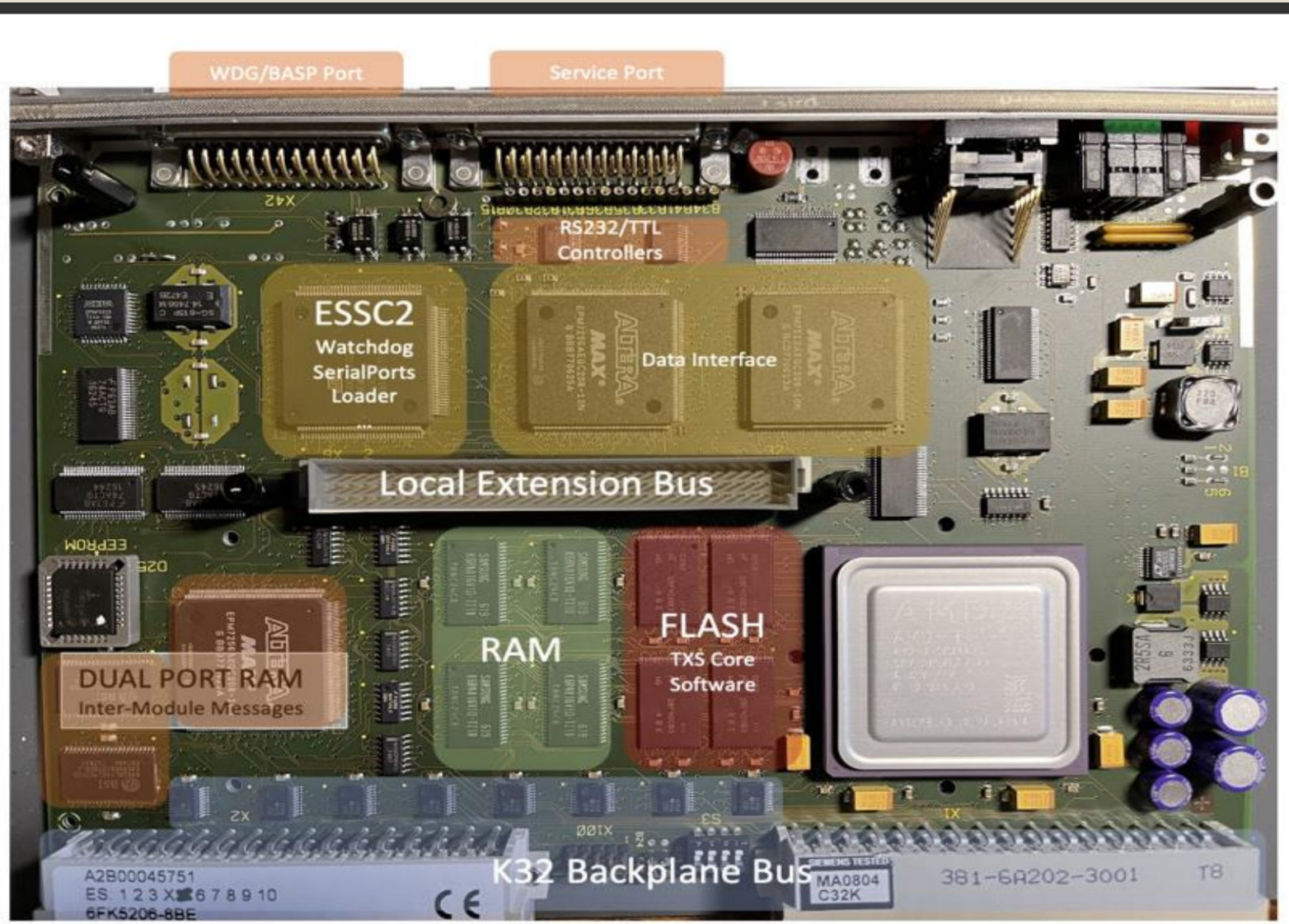
from Germany

wm-inc

Sponsored

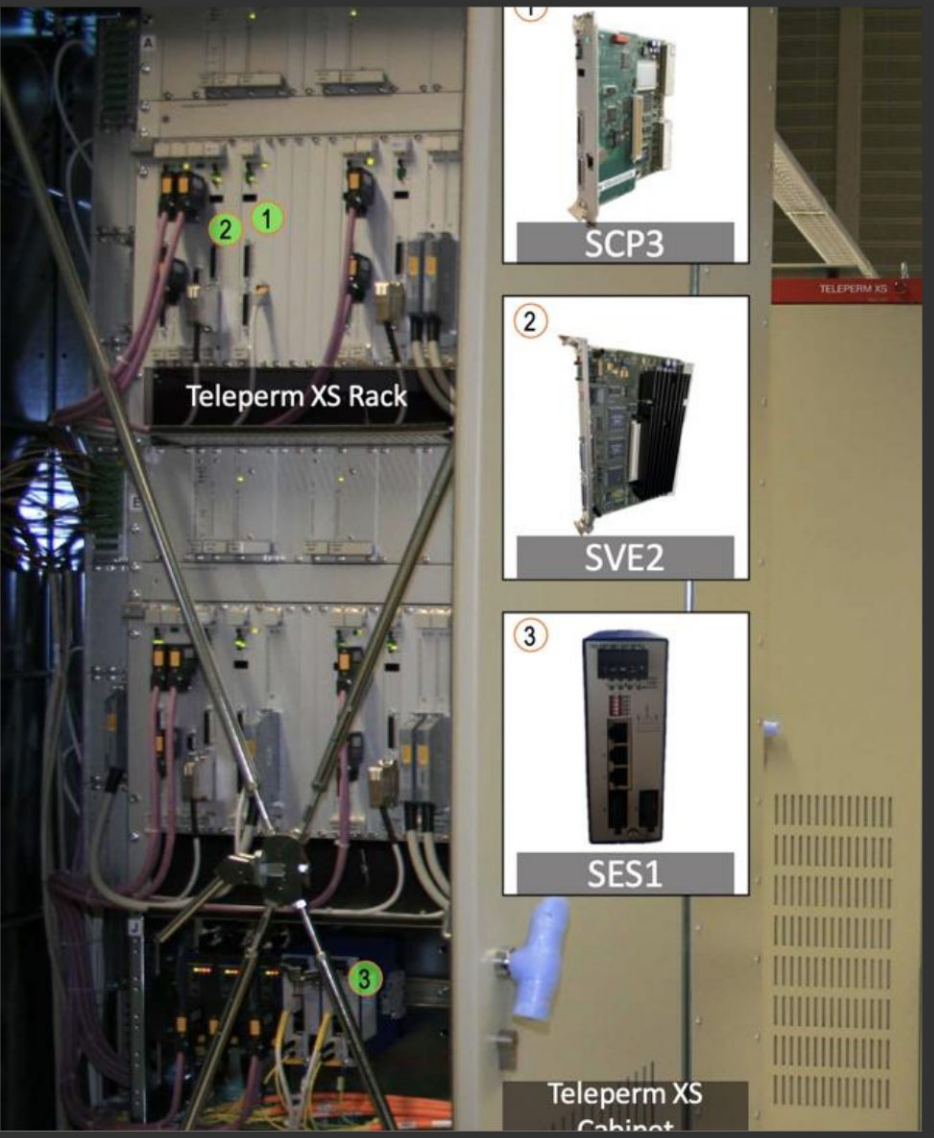
SVE2

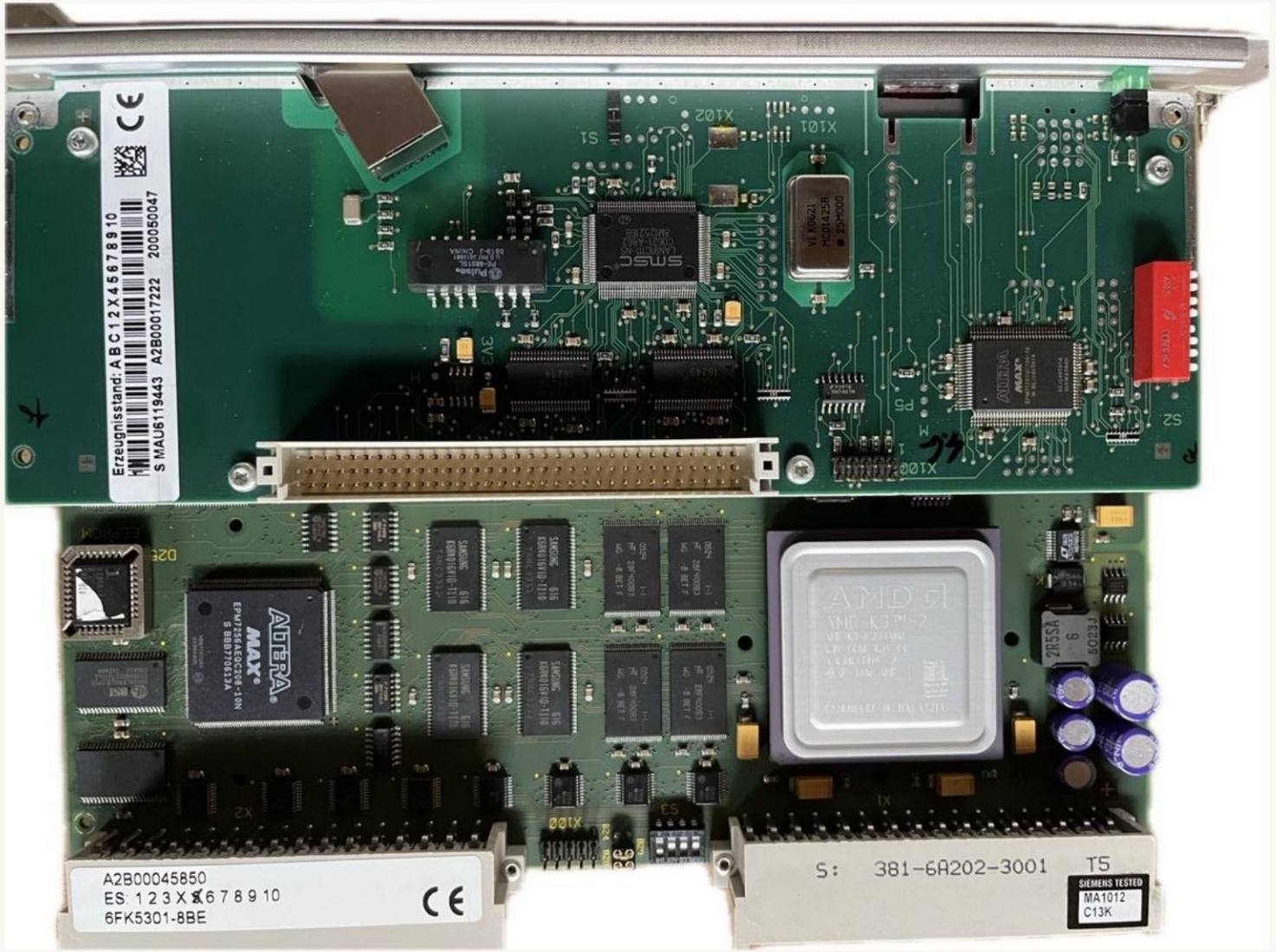




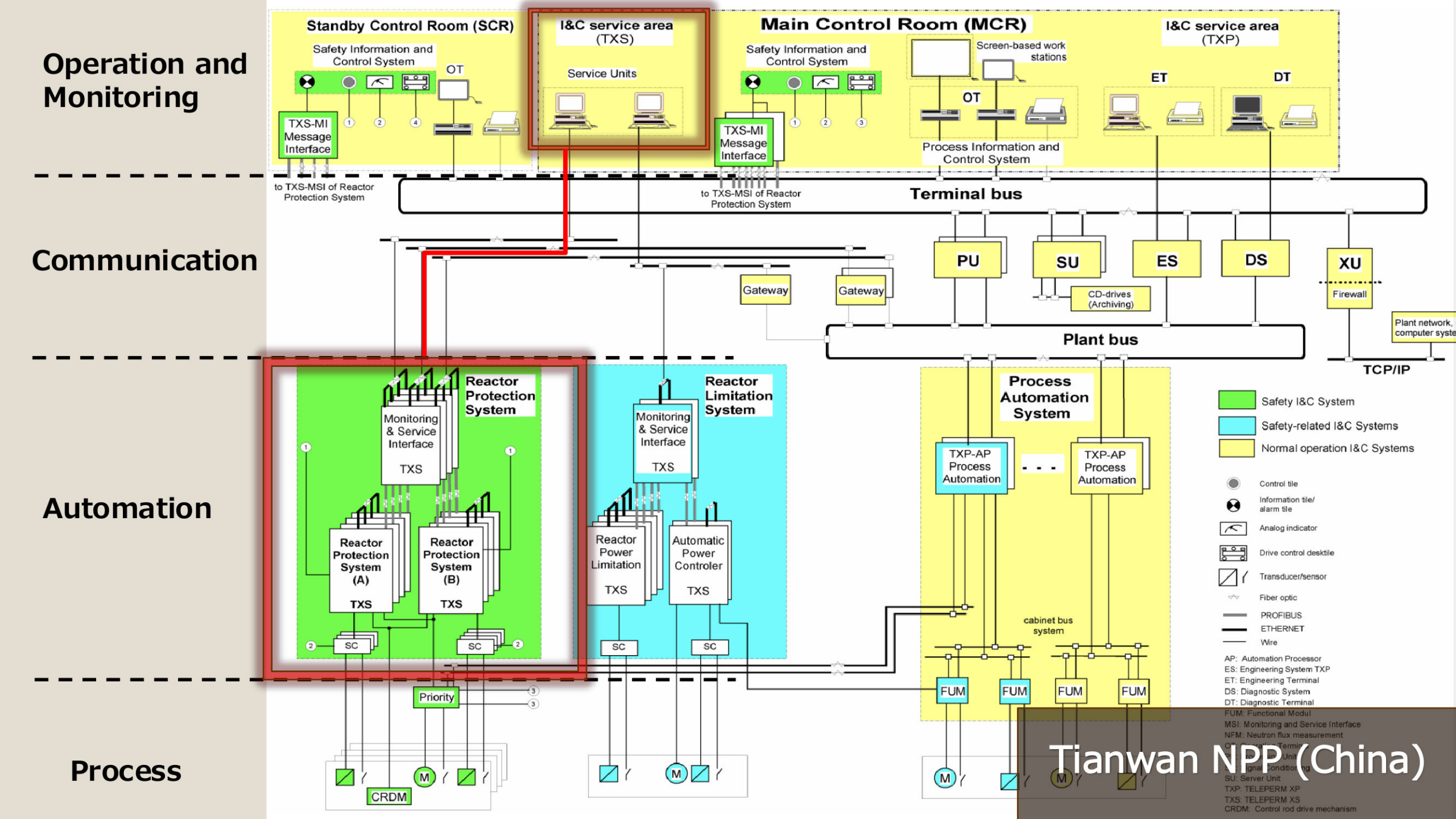
Main Processing Module – AMD K6-2

SCP3

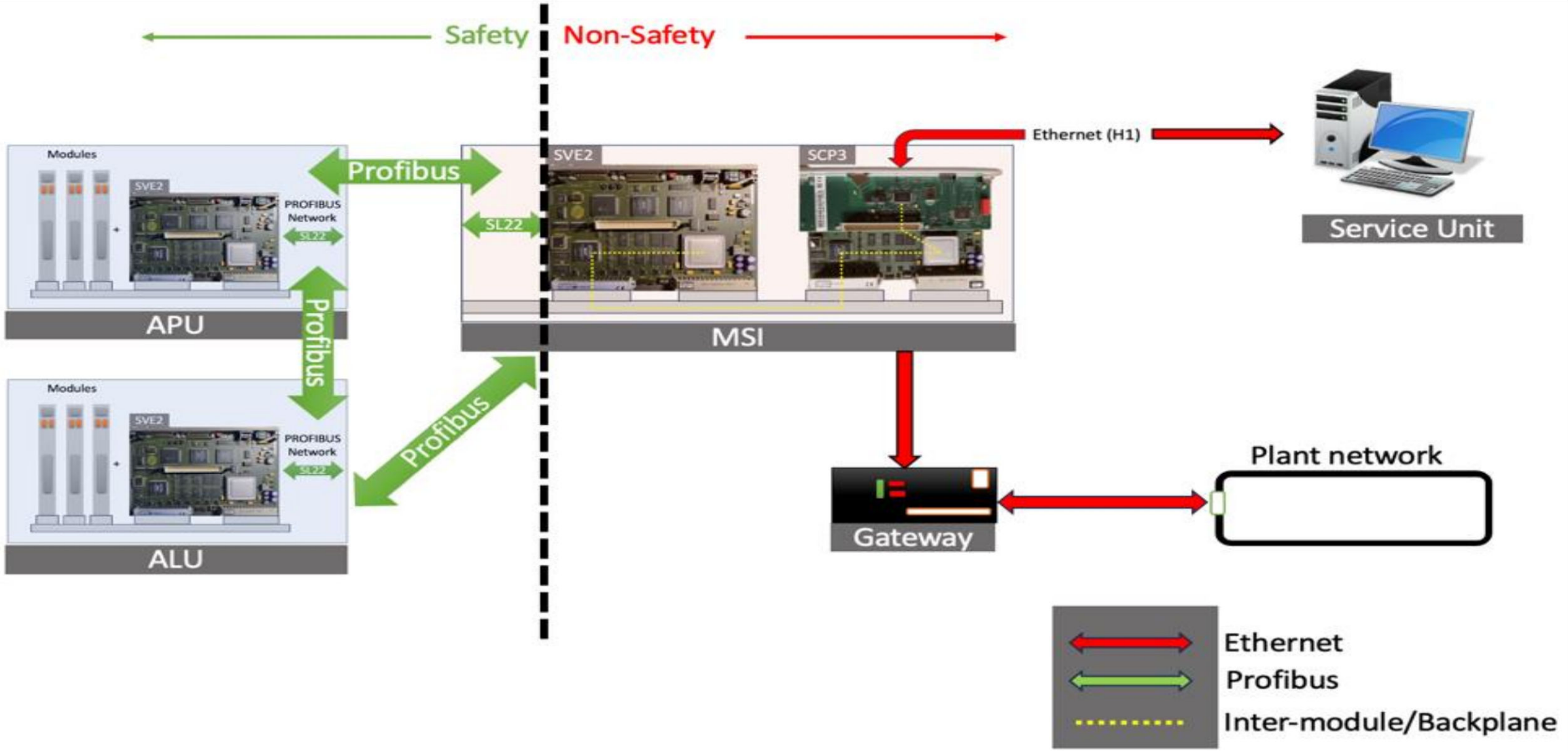




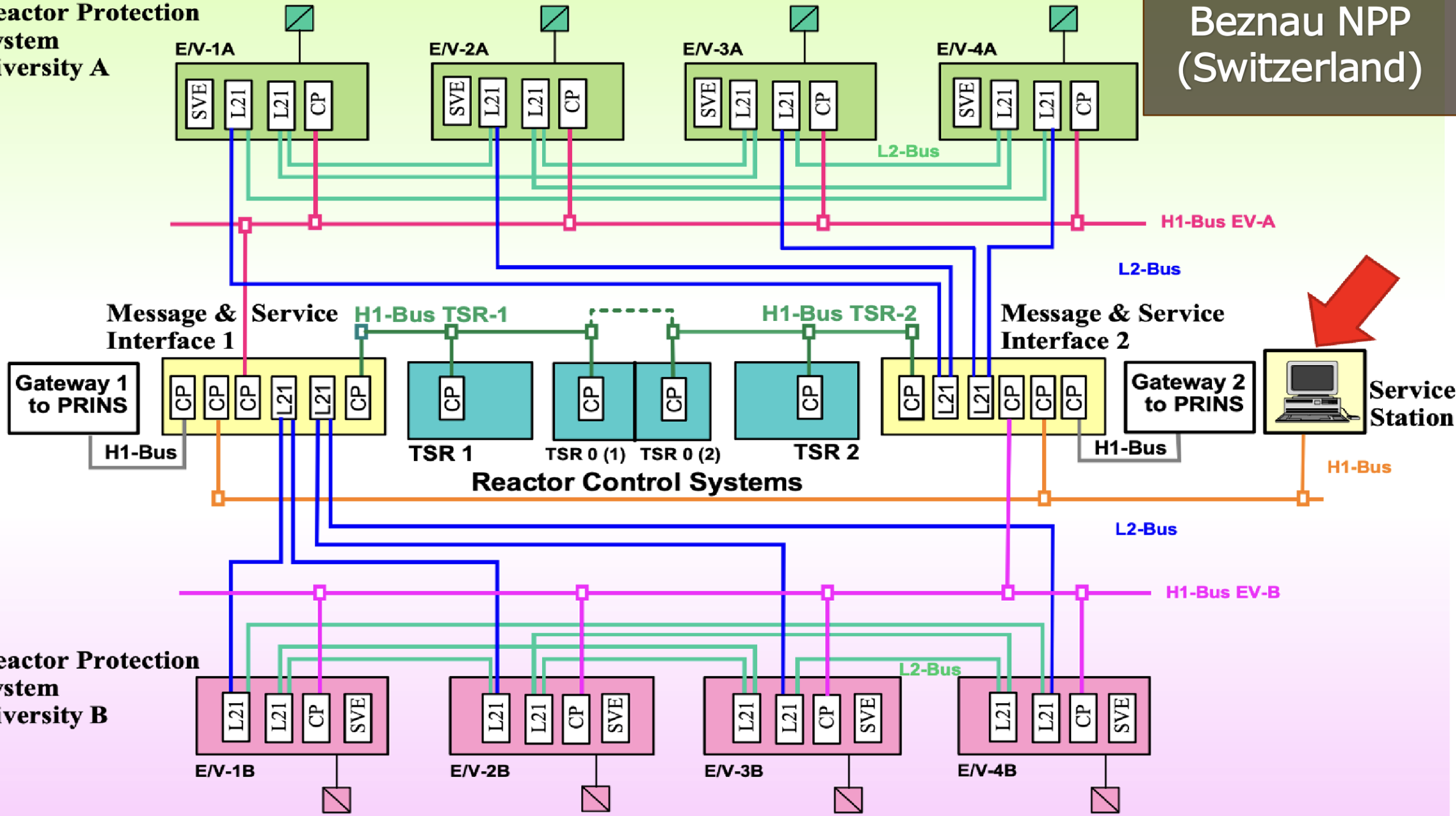
Communication Module (H1 - Ethernet)


Operation and Monitoring
Communication
Automation
Process
Standby Control Room (SCR)
Safety Information and Control System
OT
TXS-MI Message Interface
I&C service area (TXS)
Service Units
Main Control Room (MCR)
Safety Information and Control System
Screen-based work stations
OT
Process Information and Control System
I&C service area (TXP)
ET
DT
TXS-MI Message Interface
to TXS-MSI of Reactor Protection System
to TXS-MSI of Reactor Protection System
Terminal bus
Gateway
Gateway
PU
SU
CD-drives (Archiving)
ES
DS
XU
Firewall
Plant network, computer syste
Plant bus
TCP/IP
Reactor Protection System
Monitoring & Service Interface
TXS
Reactor Protection System (A)
TXS
Reactor Protection System (B)
TXS
SC
SC
Reactor Limitation System
Monitoring & Service Interface
TXS
Reactor Power Limitation
TXS
Automatic Power Controler
TXS
SC
SC
Process Automation System
TXP-AP Process Automation
TXP-AP Process Automation
cabinet bus system
FUM
FUM
FUM
FUM
Priority
CRDM
M
M
M
Safety I&C System
Safety-related I&C Systems
Normal operation I&C Systems
Control tile
Information tile/ alarm tile
Analog indicator
Drive control desktile
Transducer/sensor
Fiber optic
PROFIBUS
ETHERNET
Wire
AP: Automation Processor
ES: Engineering System TXP
ET: Engineering Terminal
DS: Diagnostic System
DT: Diagnostic Terminal
FUM: Functional Modul
MSI: Monitoring and Service Interface
NFM: Neutron flux measurement
SU: Server Unit
TXP: TELEPERM XP
TXS: TELEPERM XS
CRDM: Control rod drive mechanism
Tianwan NPP (China)

TXS – Functional units



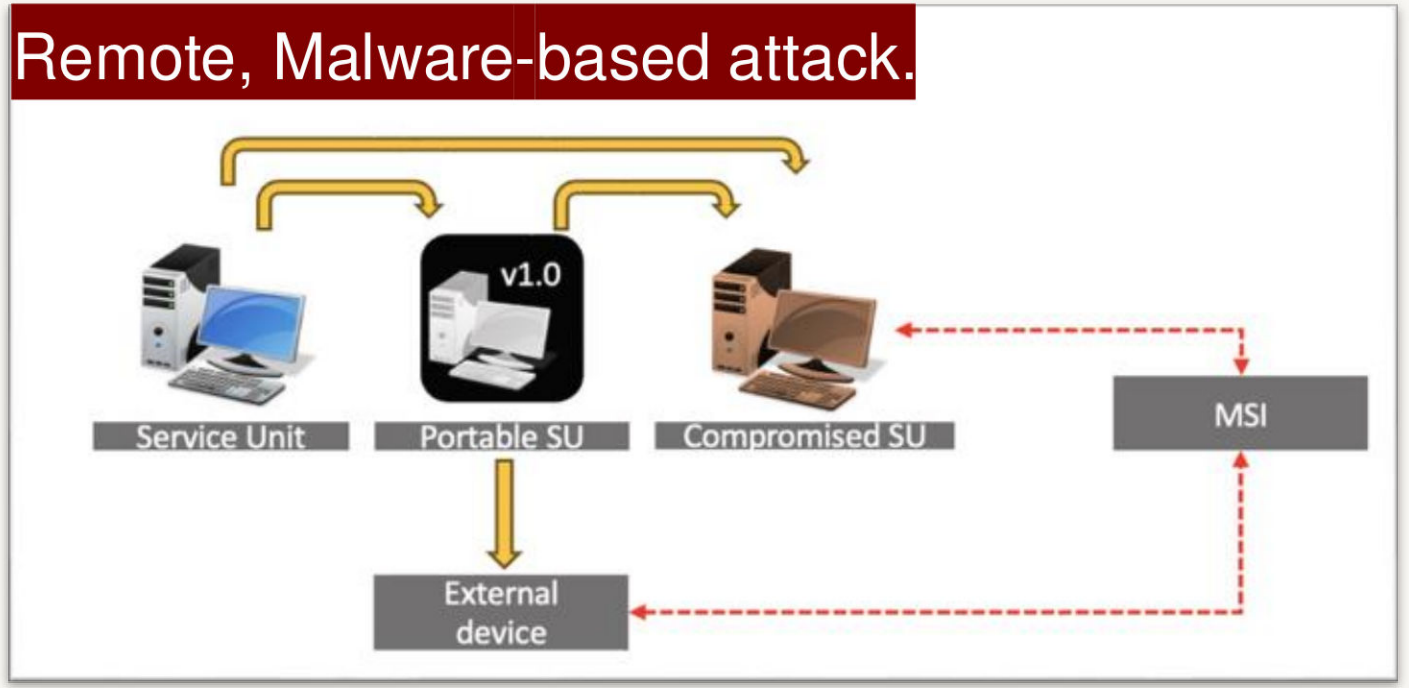
Beznau NPP (Switzerland)



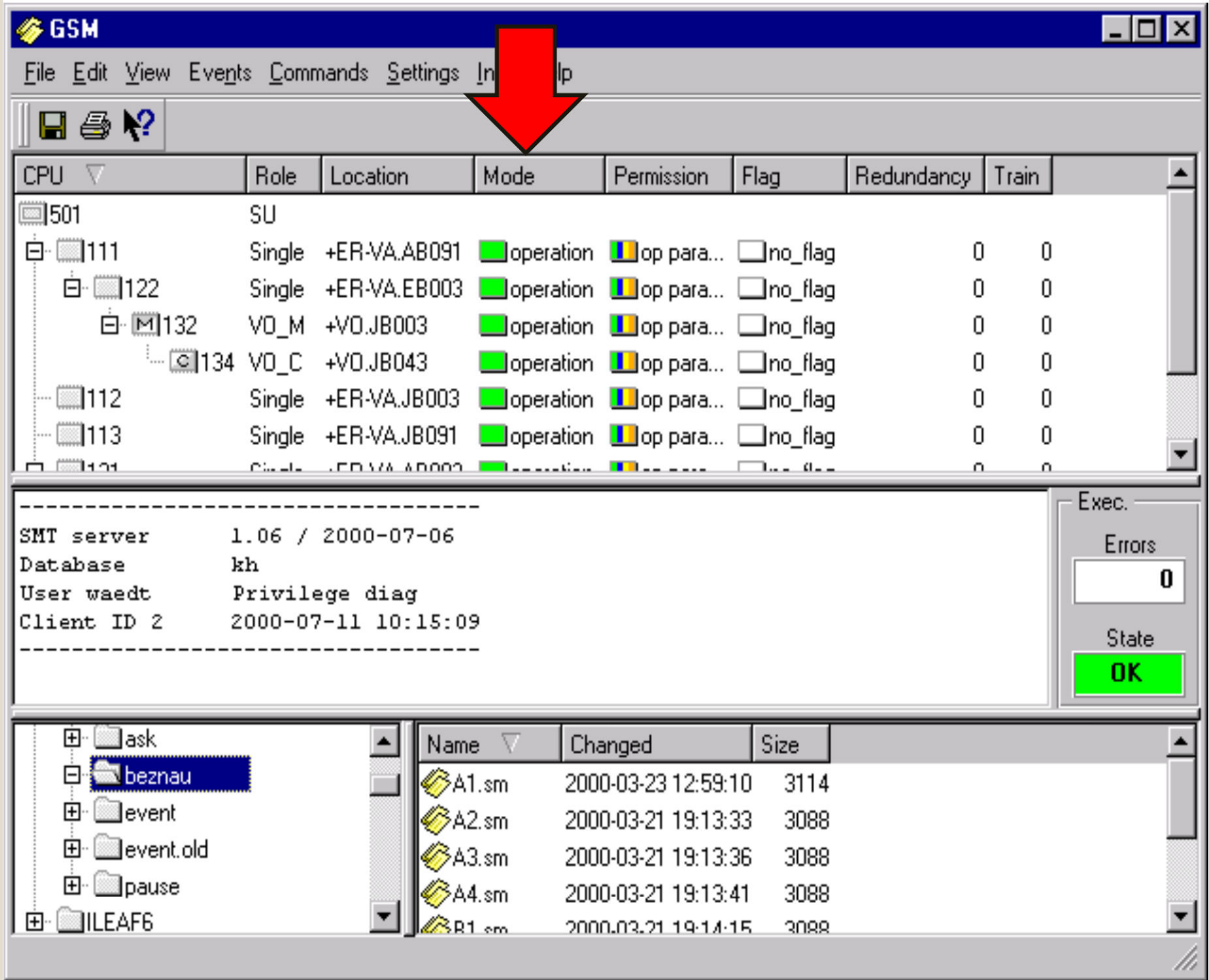
SERVICE UNIT

Primary Target

- COTS computer running SUSE Linux
- Diagnosis.
- Bi-directional communication with the MSI
- Monitoring the system functional status.
- Performing periodic tests of the system (e.g. triggering specific actuation sequences).
- Modifying the changeable software parameters (e.g. setpoints).
- Loading new software.



Service Unit



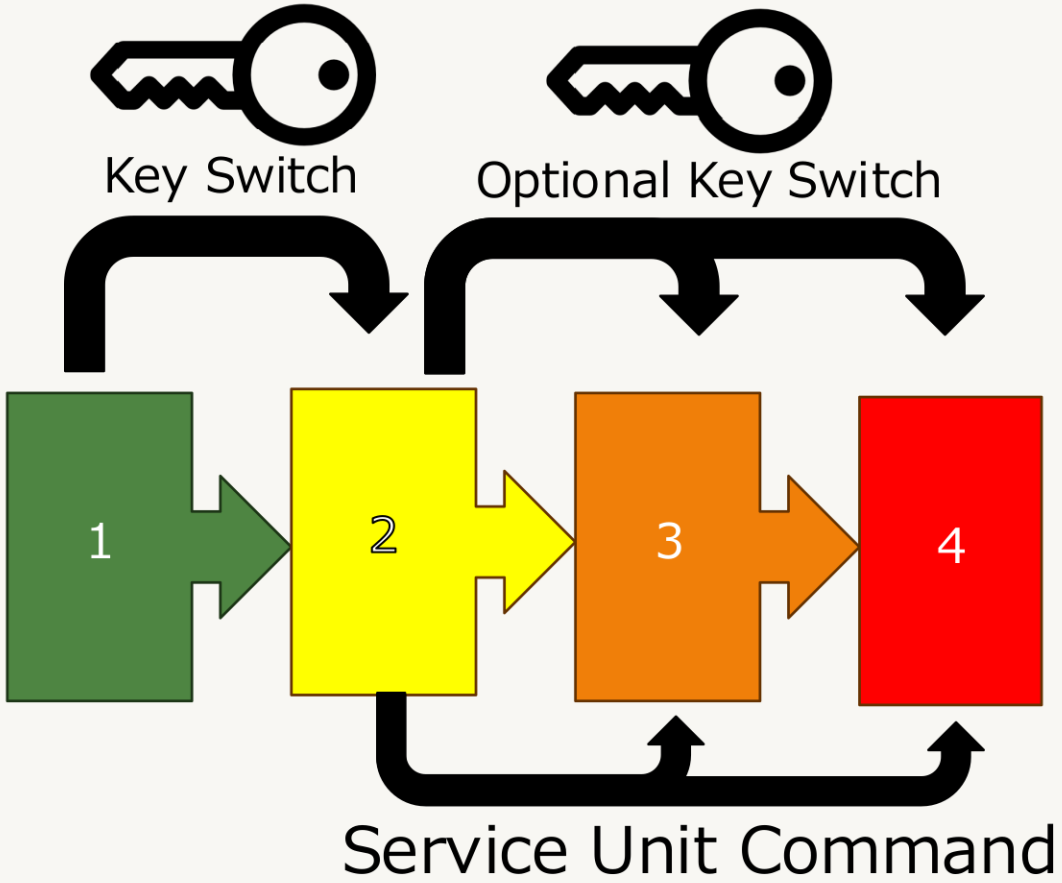

REMOTE
RUN
PROGRAM
STOP
-LOCAL-
TRICONEX
TRISIS
NO HARDWARE
INTERLOCKS

Teleperm XS

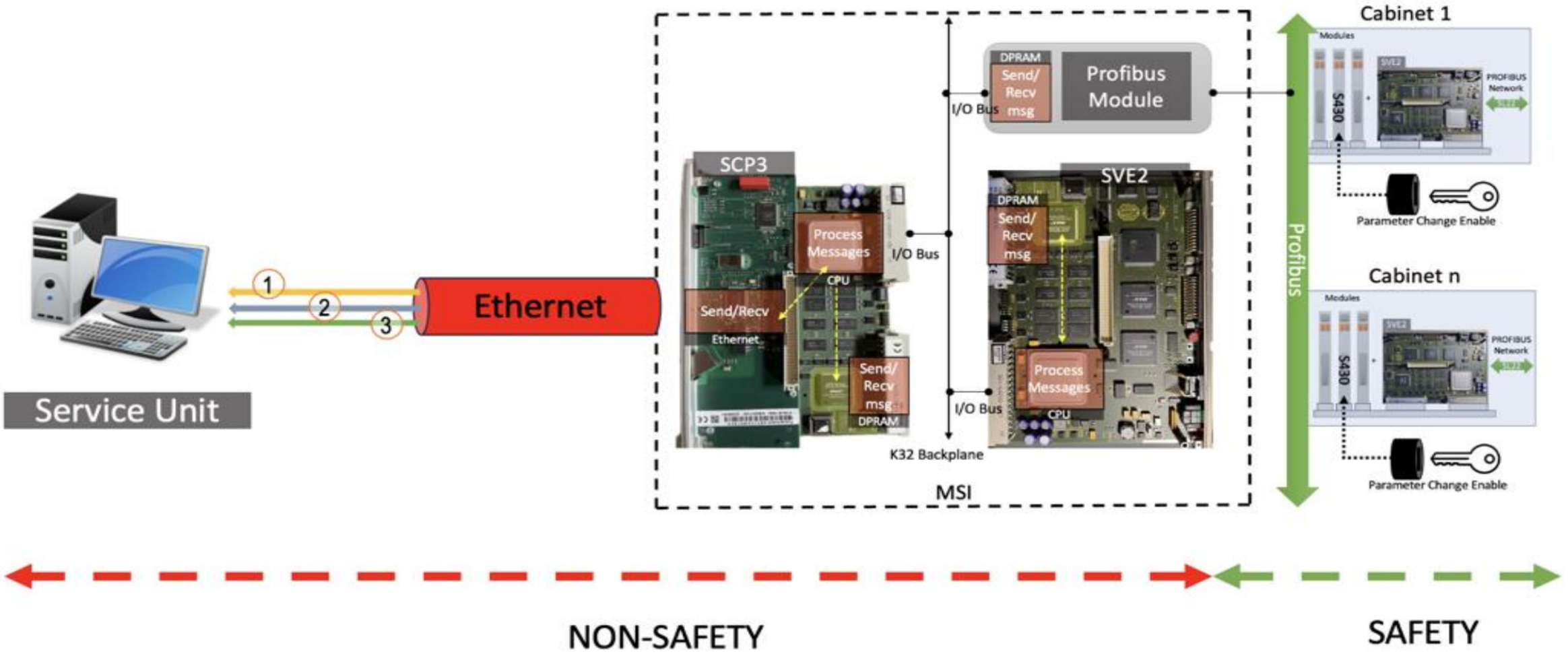
Operation Modes

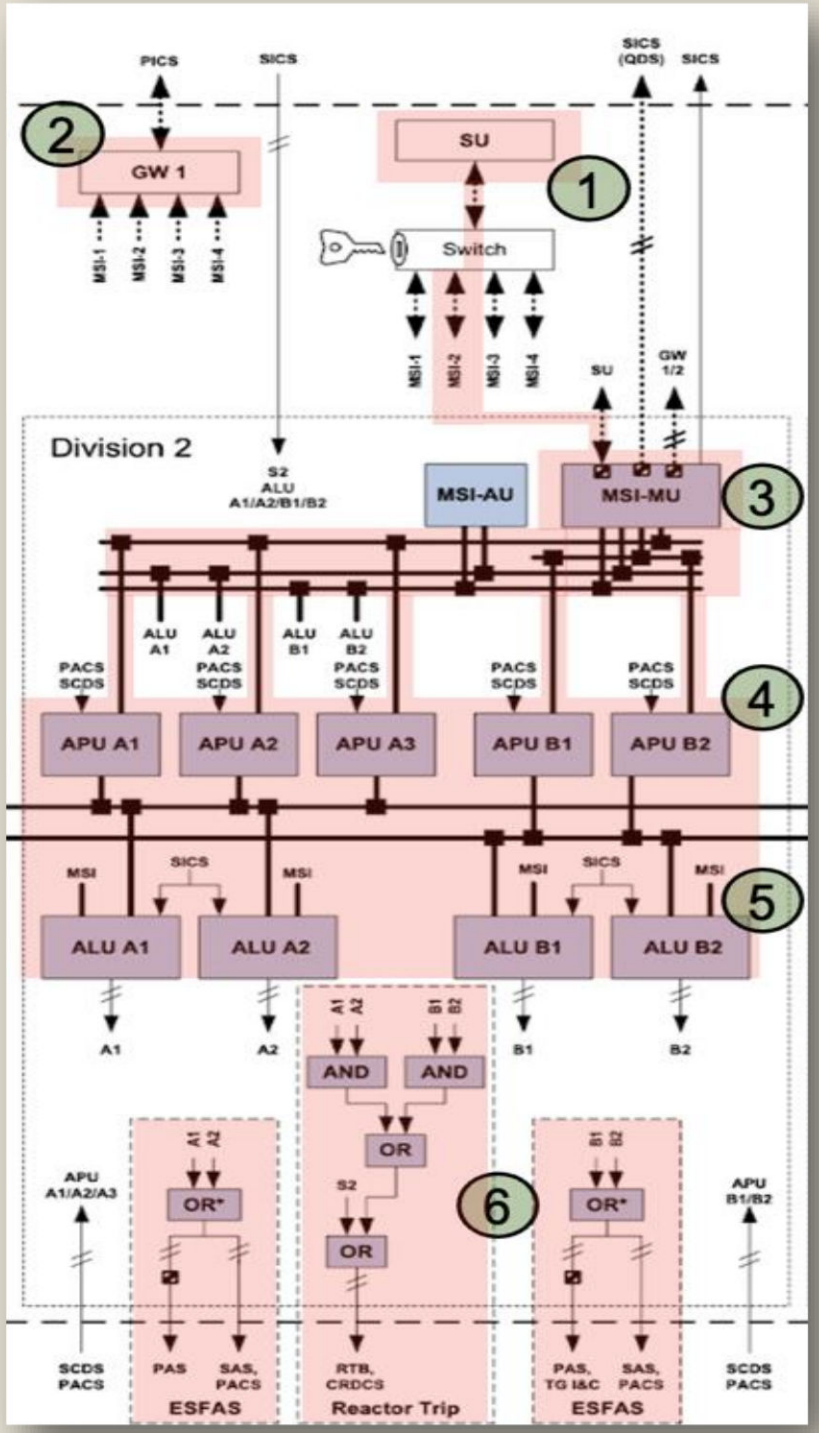
1. Operation (Running logic)
2. Parameterization (Running logic)
3. Test (No Logic)
4. Diagnosis (No Logic)

-Install new firmware / applications



TXS


Service Unit
1
2
3
Ethernet
SCP3
Process Messages
CPU
Send/Recv
Ethernet
Send/ Recv msg
DPRAM
I/O Bus
DPRAM
Send/ Recv msg
Profibus Module
I/O Bus
SVE2
DPRAM
Send/ Recv msg
Process Messages
CPU
I/O Bus
K32 Backplane
MSI
Profibus
Cabinet 1
Modules
S430
SVE2
PROFIBUS Network
Parameter Change Enable
Cabinet n
Modules
S430
SVE2
PROFIBUS Network
Parameter Change Enable
NON-SAFETY
SAFETY



1. Attackers' implant is positioned as an 'alternative' Service Unit
   - It waits for "Change Parameters Enable" permissive (interlock)

2. Ideally the gateway may have also been compromised
   - It allows the attackers to control the information the operators receive.

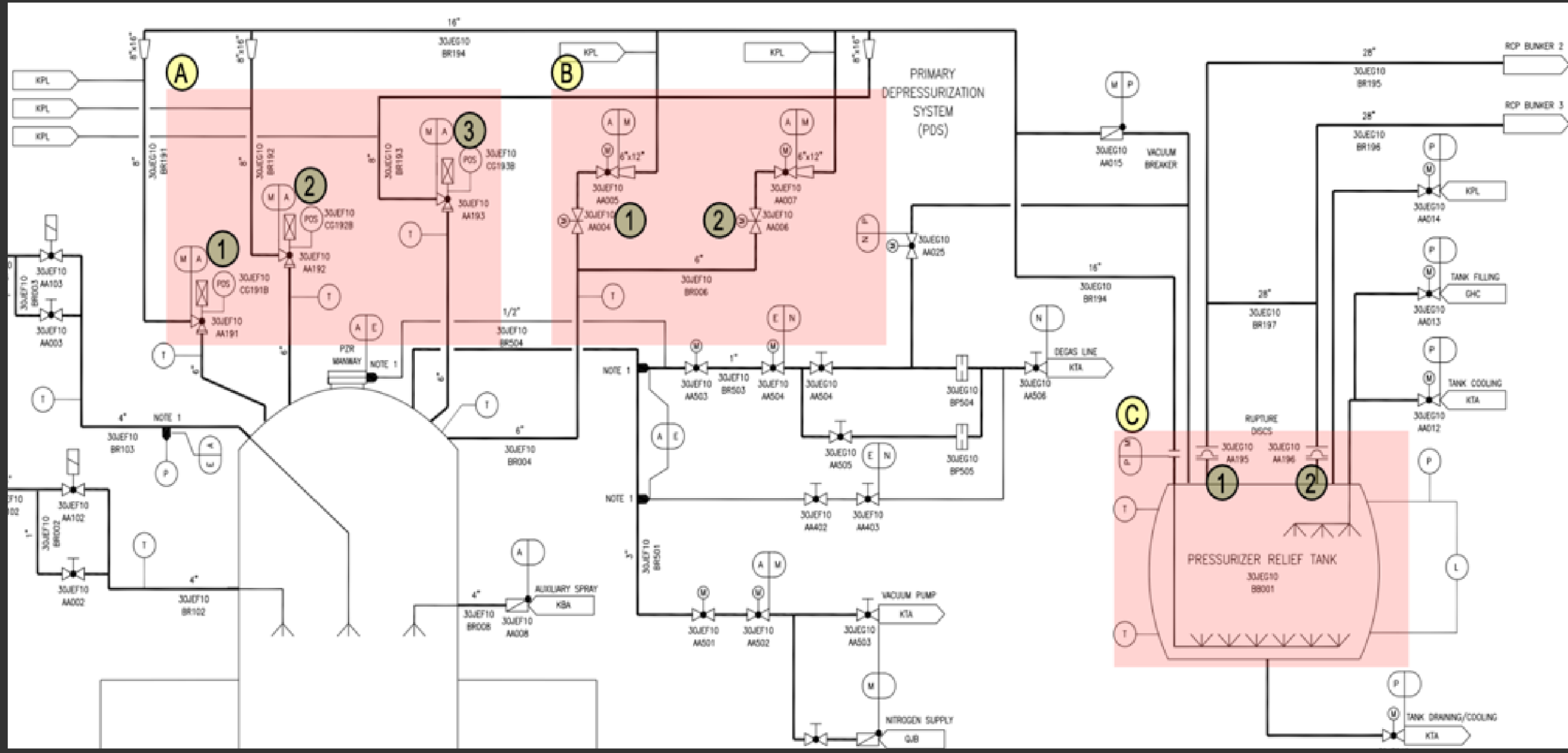
3. The MSI (main unit), by design, enables a logical bi-directional communication between the SU's implant and the safety network.

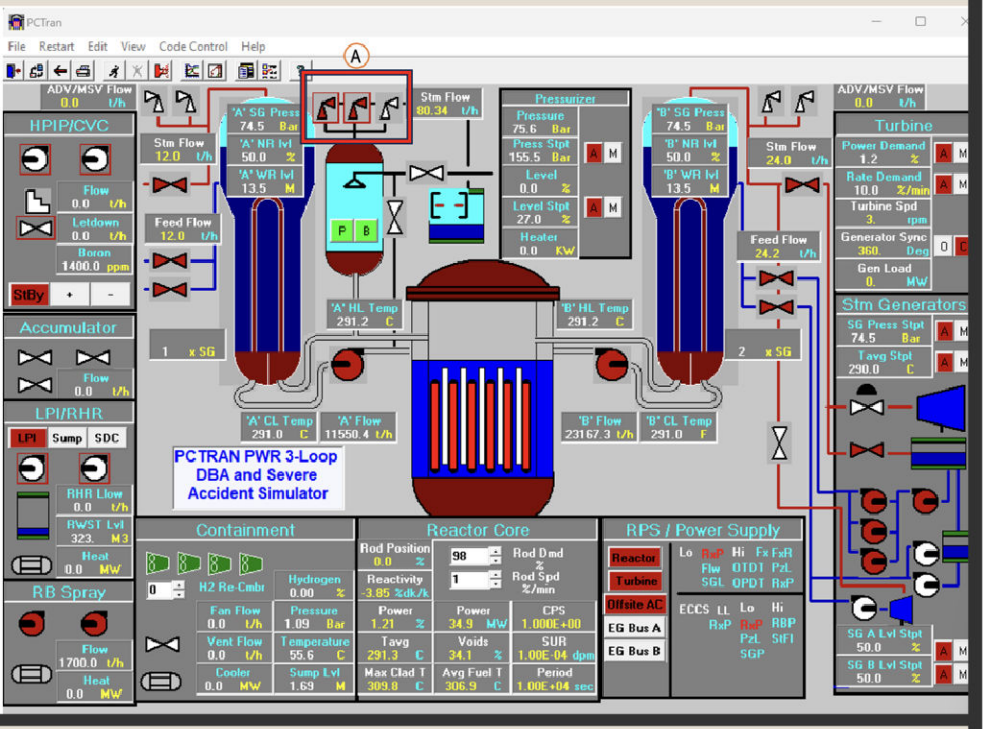
4. The APUs (Acquisition and Processing Unit) are plausibly compromised

5. The ALUs (Actuation Logic Unit) are plausibly compromised

   - Manual Controls that do not bypass the digital PS
   - Manual Controls that bypass the digital PS
   - Priority

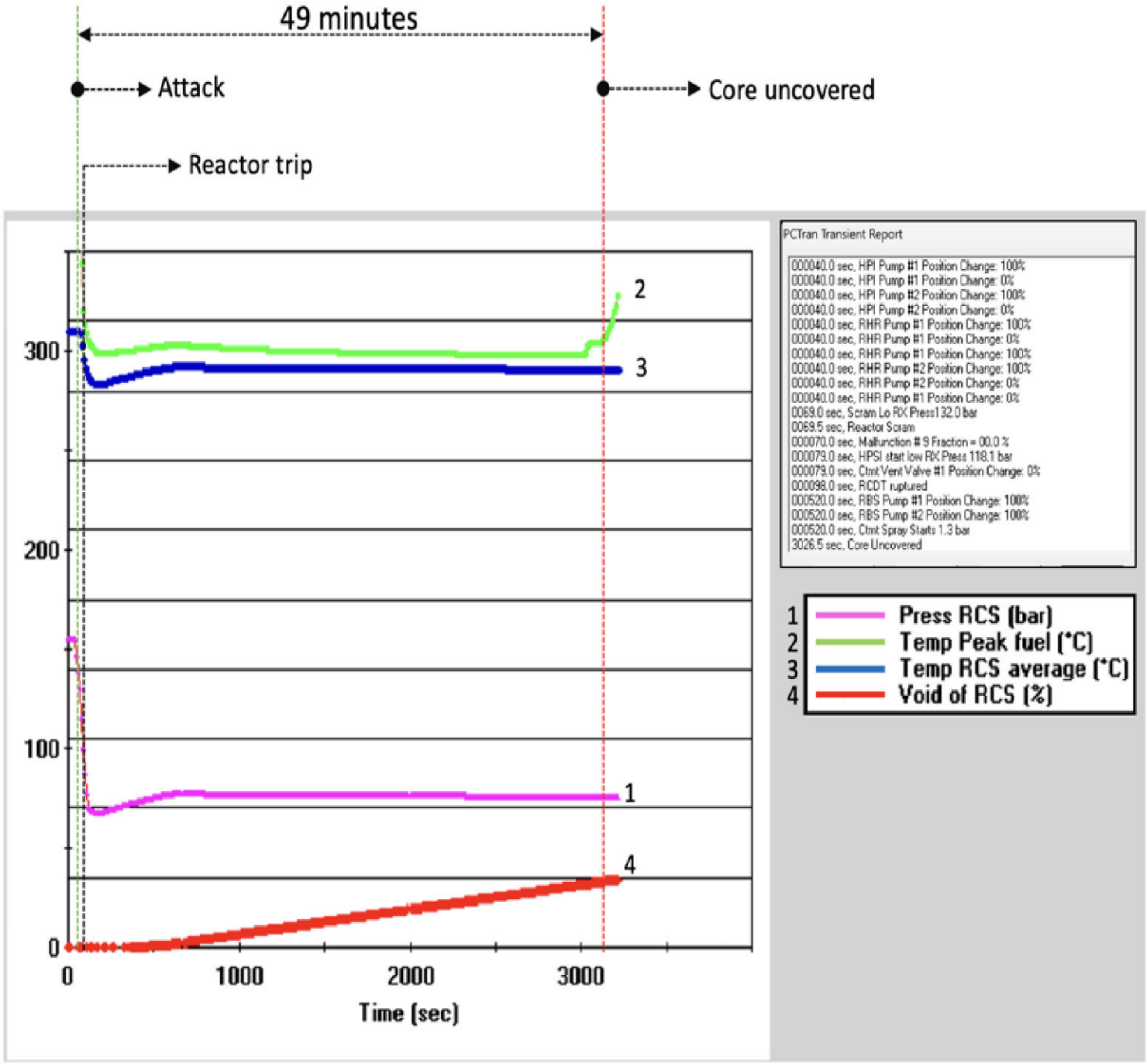
Small Loss Of Coolant Accident (SLOCA) via Pressurizer's PSRVs





Simulating the Cyber-Physical Attack

1. Two PSRVs stuck open
2. Inhibit Safety Injection and Residual Heat Removal systems
3. Coolant is continuously vented through the PSRVs (SLOCA)
4. Core uncovered after 49 minutes.
5. Core melt



Conclusions

Education and transparency are vital tools to dispel myths and foster a greater public understanding of nuclear technology (including cyber).

Small Modular Reactors (SMRs) will be assets to protect in the near future.

Nuclear Power Plants are complex, but valuable targets during (or in preparation for) armed conflicts or profound geopolitical confrontations.

We must be prepared to identify potential cyber-related nuclear incidents. (e.g. Radiation Spikes - Chernobyl Exclusion Zone’22)


CYBER ATTACKS AND DEFENSE
SWISS CYBER STORM
WWW.SWISSCYBERSTORM.COM


RS
Ruben Santamarta
Security Research Services
www.reversemode.com

THANK YOU!