THE ASHERAH NUCLEAR POWER PLANT SIMULATOR (ANS) AS A TRAINING TOOL AT THE BRAZILIAN CYBER GUARDIAN EXERCISE (EGC 2.0)

Rodney Busquim e Silva
Diego Alves Correa
Felipe Antunes
Francisco Carlos Salles Souza
José Roberto Castilho Piqueira
Ricardo Paulino Marques

#ICONS2020

IAEA, Vienna, Austria

EGC 2.0

ACTIVITIES

SCENARIOS

EVALUATION

Brazilian Cyber Guardian Exercise (EGC): support and improve the prevention, detection and response to cyber security incidents involving Brazil´s critical infrastructure.

- ✓ EGC 1.0 (2018): 115 participants from 23 organizations from finance, nuclear, and defense sectors.

- ✓ EGC 2.0 (2019):
  - 260 participants 39 private and public organization, more than 260 participants.
  - Finance, Electricity, Nuclear, Defense and Telecommunications.
  - IAEA CRP J2008 USP/MB team: 2 days activities
  - IAEA observer attended the EGC 2.0.
  - Asherah NPP Simulator: main exercise tool.

ipen

Eletrobras
Eletronuclear

CNEN
Comissão Nacional
de Energia Nuclear

MARINHA DO BRASIL

INB
INDÚSTRIAS NUCLEARES DO BRASIL

Table Top:

Testing the organizations emergency plan deal with emergency situations.

Use of Request Tracker Tool

Study Group:

"Establishing a roadmap for implementing a nuclear computer security regulatory framework in Brazil".

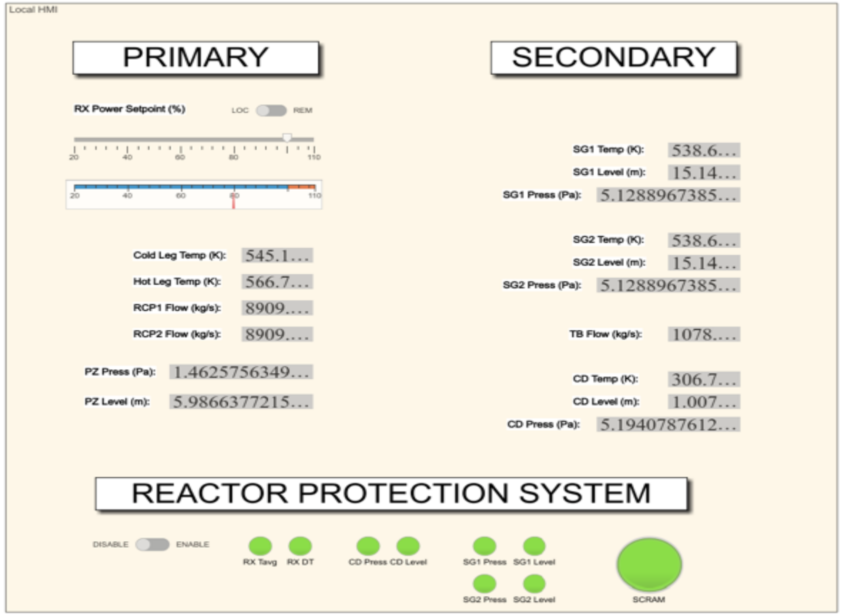
Hands On:

Network and Process Baseline/Attack.

Computer and Operators working together.

BR EGC 2.0 Nuclear Sector Schooling Activities

Asherah NPP Simulator ANS



Local HMI

PRIMARY

RX Power Setpoint (%) LOC REM

Cold Leg Temp (K): 545.1...

Hot Leg Temp (K): 566.7...

RCP1 Flow (kg/s): 8909....

RCP2 Flow (kg/s): 8909....

PZ Press (Pa): 1.4625756349...

PZ Level (m): 5.9866377215...

SECONDARY

SG1 Temp (K): 538.6...

SG1 Level (m): 15.14...

SG1 Press (Pa): 5.1288967385...

SG2 Temp (K): 538.6...

SG2 Level (m): 15.14...

SG2 Press (Pa): 5.1288967385...

TB Flow (kg/s): 1078....

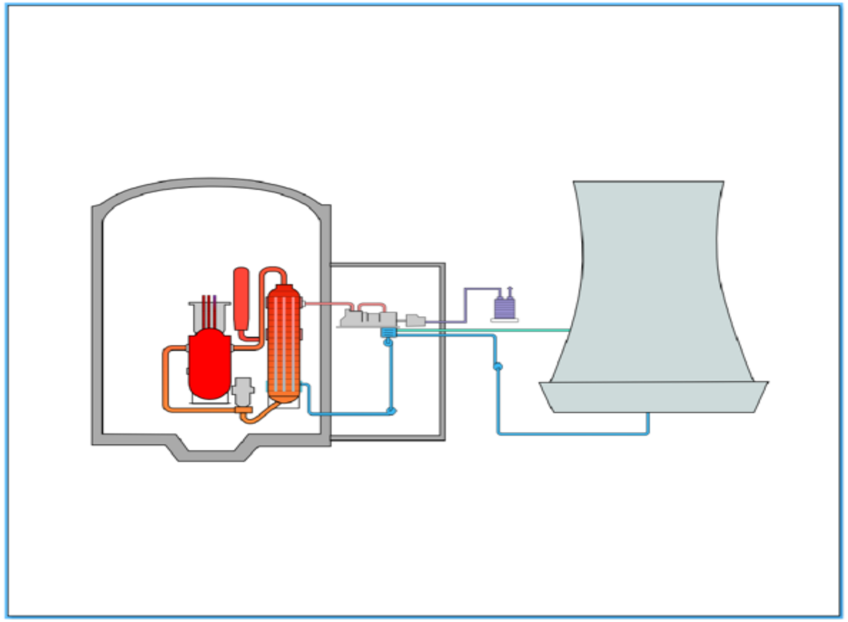
CD Temp (K): 306.7...

CD Level (m): 1.007...

CD Press (Pa): 5.1940787612...

REACTOR PROTECTION SYSTEM

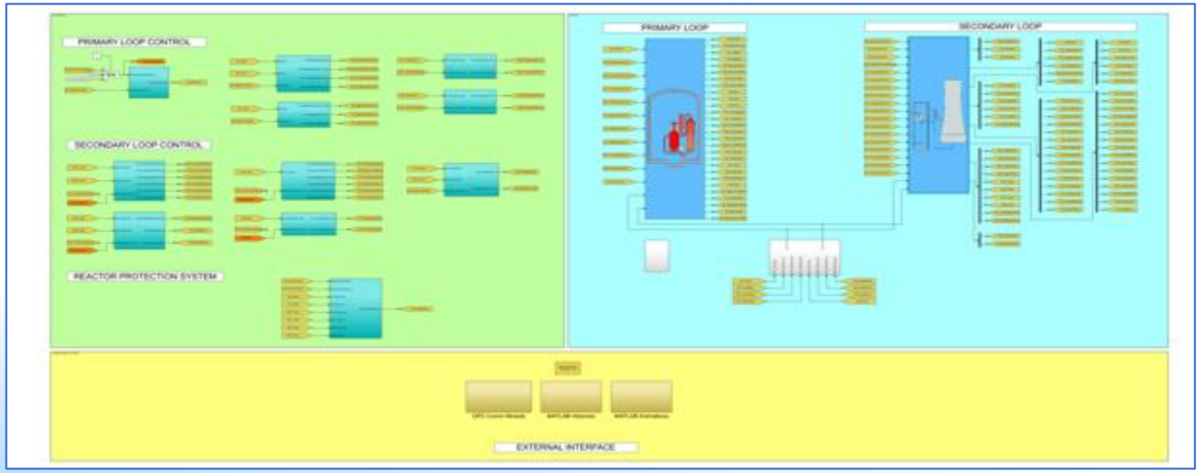
LOCAL HMI



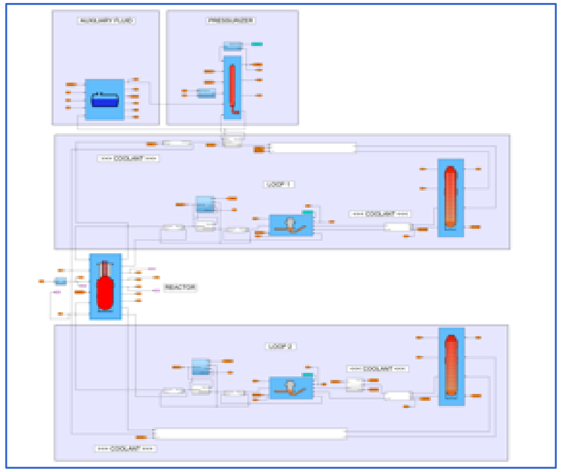
ASHERAH NPP

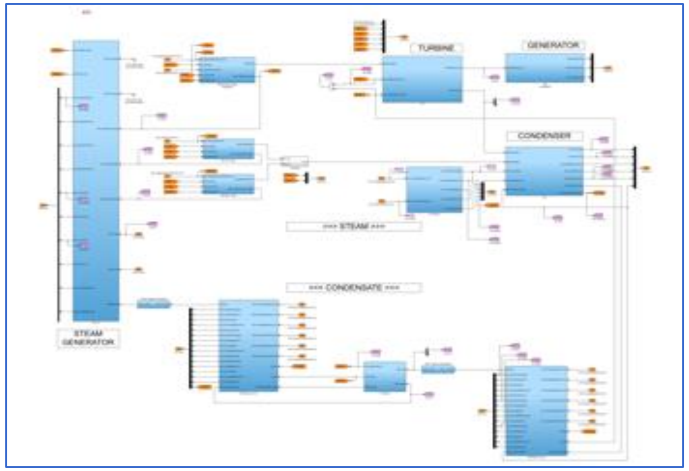
BR EGC 2.0: 1st time ANS was used as a training tool

IAEA ITC ROK: 2nd time ANS was used as a training tool (November, 2019)

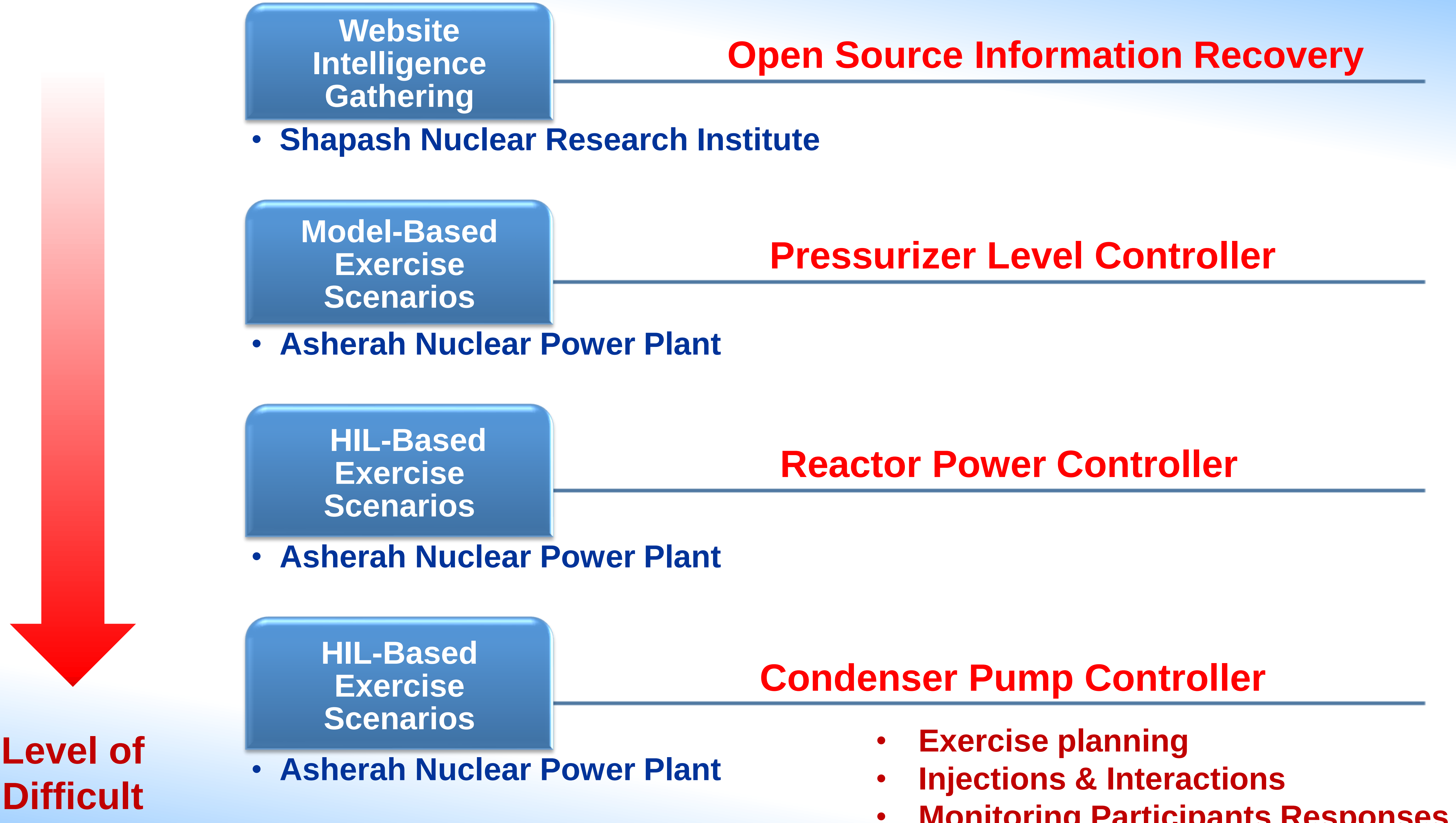


Controllers & Comm Modules





Primary, Secondary & Tertiary



Website Intelligence Gathering

Open Source Information Recovery

- Shapash Nuclear Research Institute

Model-Based Exercise Scenarios

Pressurizer Level Controller

- Asherah Nuclear Power Plant

HIL-Based Exercise Scenarios

Reactor Power Controller

- Asherah Nuclear Power Plant

HIL-Based Exercise Scenarios

Condenser Pump Controller

- Asherah Nuclear Power Plant

- Exercise planning
- Injections & Interactions
- Monitoring Participants Responses

Level of Difficult

INCOGNITUS

Intelligence Gathering

- Shapash Nuclear Research Institut

Ope

Model-Based Exercise Scenarios

- Asherah Nuclear Power Plant

P

HIL-Based Exercise Scenarios

- Asherah Nuclear Power Plant

Reactor Lev

HIL-Based Exercise Scenarios

- Asherah Nuclear Power Plant

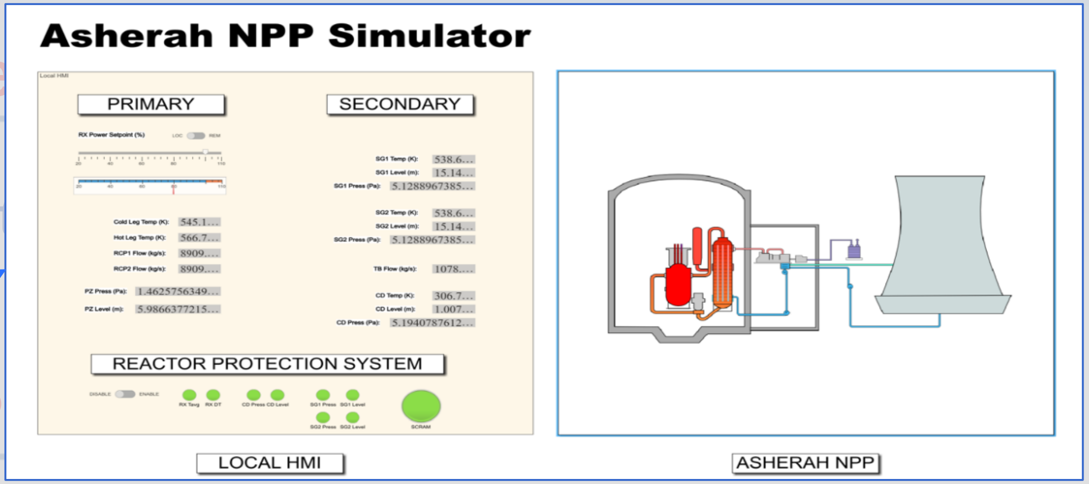
Condenser Pump Controller

rcise planning

ctions & Interactions

Monitoring Participants Responses

Level of Difficult



Asherah NPP Simulator

Local HMI

PRIMARY

RX Power Setpoint (%) LOC REM

Cold Leg Temp (K): 545.1...
Hot Leg Temp (K): 566.7...
RCP1 Flow (kg/s): 8909....
RCP2 Flow (kg/s): 8909....
PZ Press (Pa): 1.4625756349...
PZ Level (m): 5.9866377215...

SECONDARY

SG1 Temp (K): 538.6...
SG1 Level (m): 15.14...
SG1 Press (Pa): 5.1288967385...
SG2 Temp (K): 538.6...
SG2 Level (m): 15.14...
SG2 Press (Pa): 5.1288967385...
TB Flow (kg/s): 1078....
CD Temp (K): 306.7...
CD Level (m): 1.007...
CD Press (Pa): 5.1940787612...

REACTOR PROTECTION SYSTEM

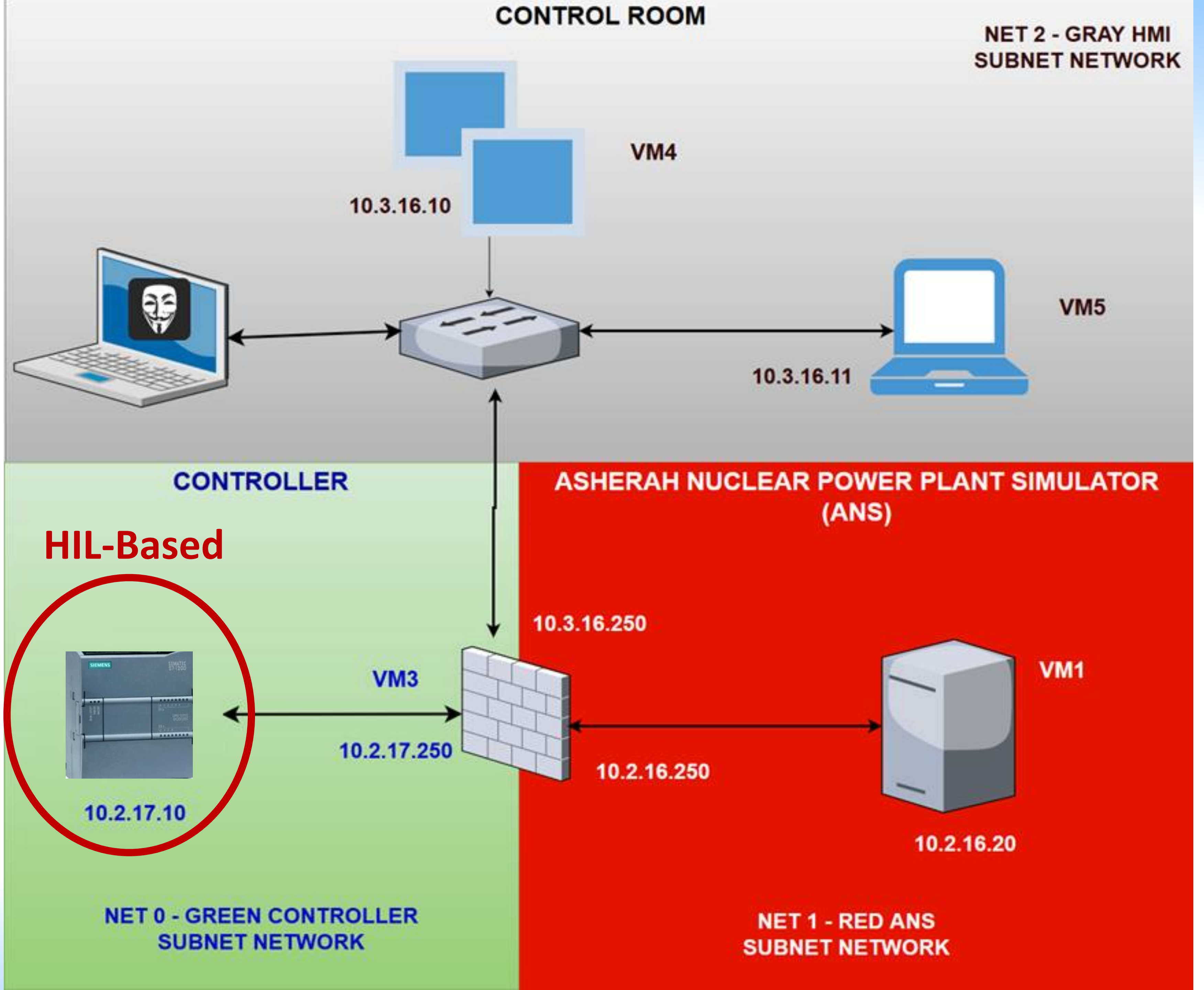
DISABLE ENABLE

LOCAL HMI

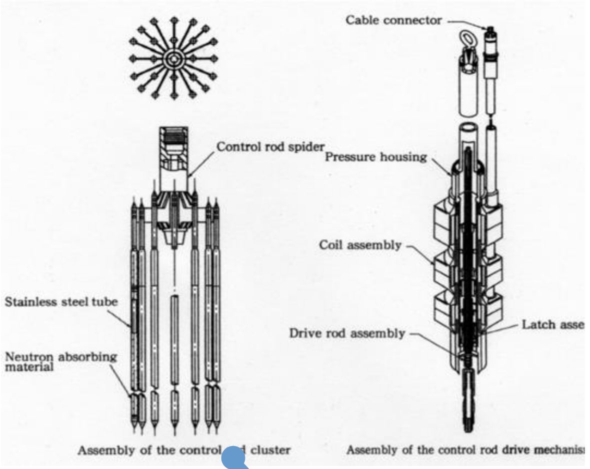
ASHERAH NPP

ANS Network & Process Baseline

VM1	=	ANS (Win7)
VM2	=	PLC S7 1200
VM3	=	IPFire Firewall (Linux)
VM4	=	ScadaBR (Win7)
VM5	=	Engineering Workstation (Win7)

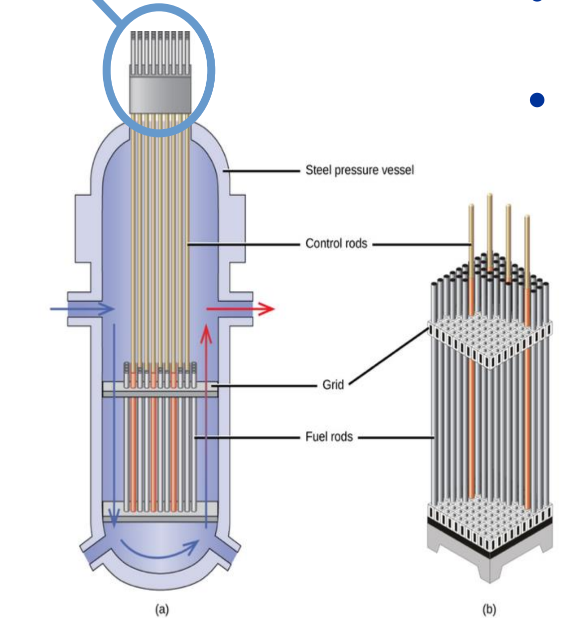

CONTROL ROOM
NET 2 - GRAY HMI SUBNET NETWORK
VM4
10.3.16.10
VM5
10.3.16.11
CONTROLLER
HIL-Based
ASHERAH NUCLEAR POWER PLANT SIMULATOR (ANS)
10.3.16.250
VM3
10.2.17.250
10.2.16.250
VM1
10.2.16.20
10.2.17.10
NET 0 - GREEN CONTROLLER SUBNET NETWORK
NET 1 - RED ANS SUBNET NETWORK

Asherah Reactor Power Controller



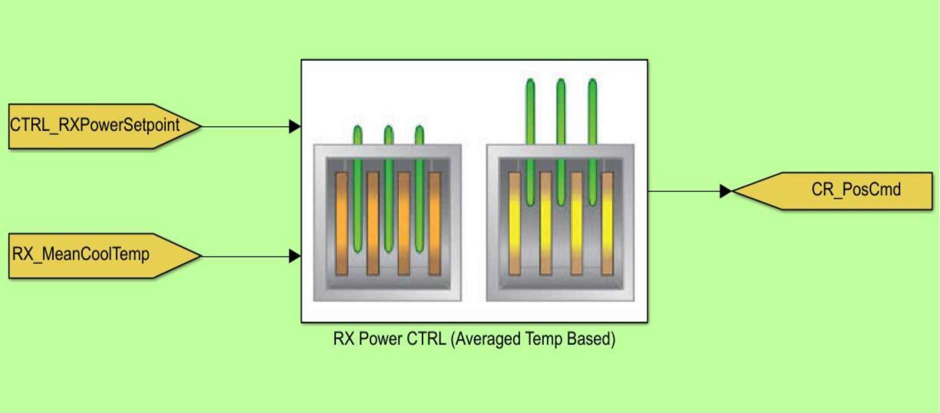
- **Main functions:**
  - **Controls the reactor core neutron flux/reactivity during normal operation.**
  - **Reactor shutdown for maintenance.**

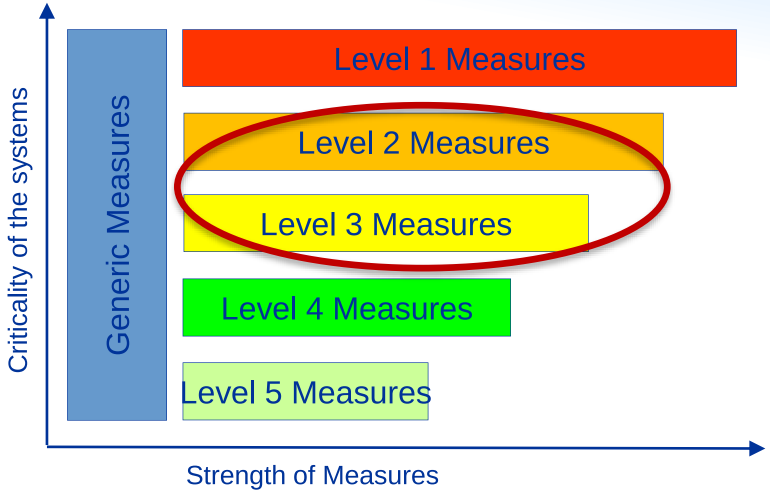
- **CRDM Controller (PLC, digital based):**
  - **Inserts control rods into the core: decreases power**
  - **Removes control rods from the core: increases power**



Control rods are rods that contain a neutron absorbing material, such as boron, that is used to control the power of a nuclear reactor

Asherah Reactor Power Controller





1. *Incognitus* uses OSINT to identify a third party potential insider.

2. Spear phishing: gain access to third party maintenance laptop John Doe (Unknowing Accomplice).

3. *Incognitus* install a malware at the maintenance laptop: scan for Siemens data on IT/OT equipment and copy them (EthernalBlue SMB exploit).

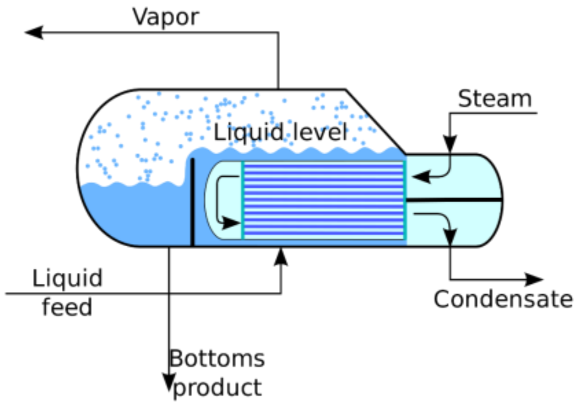
4. John Doe accesses CR network for maintenance.

Asherah Reactor Power Controller

6. The malware copies S7 1200 web server configuration backup files and OT network architecture.
7. John Doe connects his laptop to the Internet: the malware sends data captured to a remote server.
8. Using TIA portal, *Incognitus* prepares a new S7 1200 configuration file, that “stuck” the control rods in a certain position (“all rods out”).
9. During a new CR maintenance, SL2 remote maintenance access (from SL3) was allowed (case-by-case access and for a short defined working period).
10. The new PLC S7 1200 configuration file is uploaded.
11. The reactor power controller is compromised.

CD Pressure & Level Controllers

- **Main functions:**
  - – Condensation of the turbine exhaust steam into water
  - – Maintain vacuum to maximize turbine efficiency

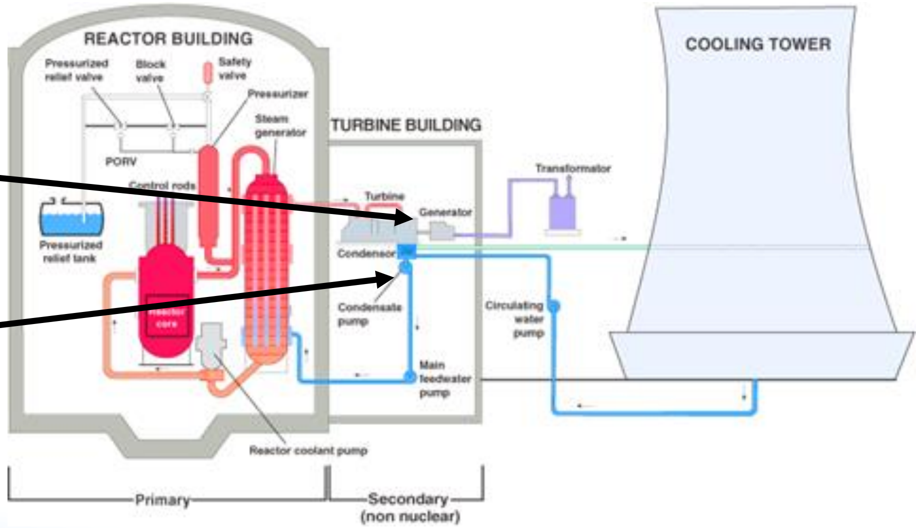


CD Level Controller (PLC, digital based):

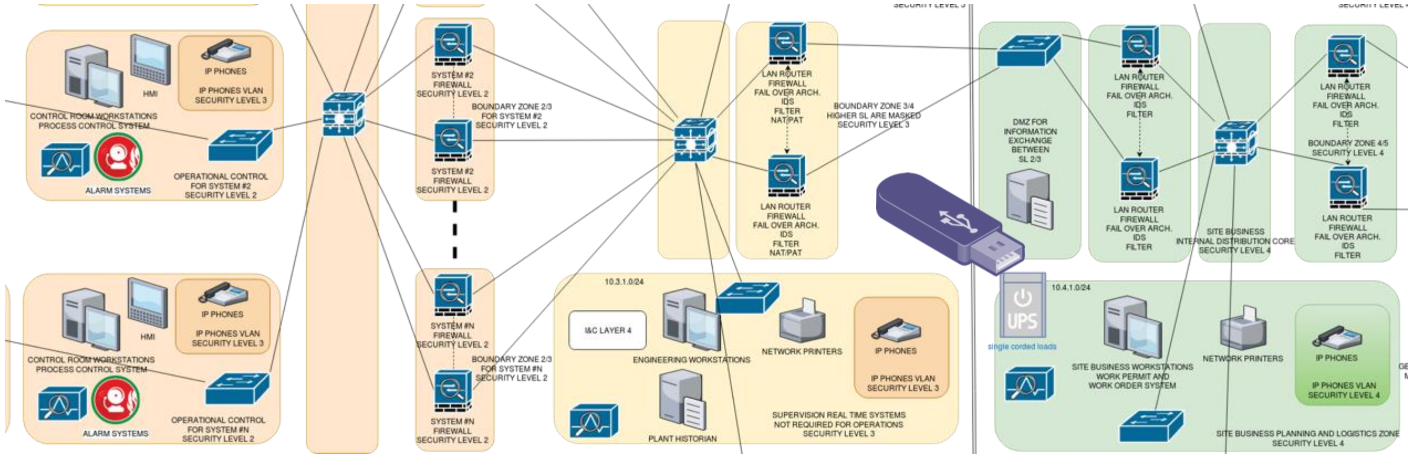
Condensate Extraction Pump

CD Pressure Controller (PLC, digital based):

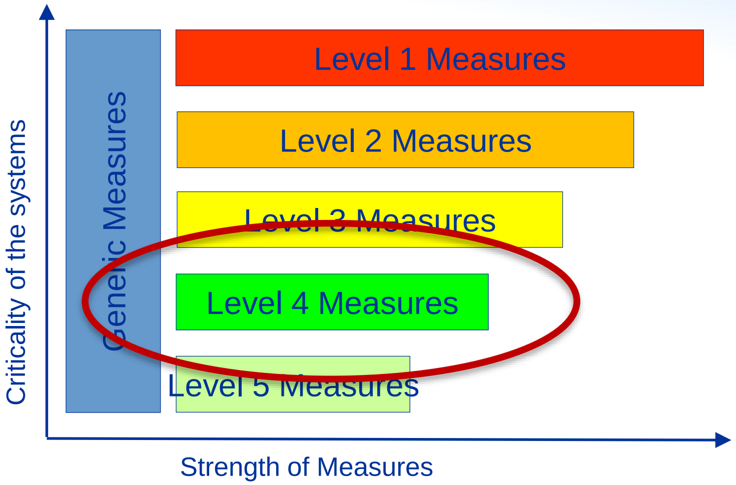
Condensate Cooling Pump



CD Pressure & Level Controllers


IP PHONES
IP PHONES VLAN SECURITY LEVEL 3
HMI
CONTROL ROOM WORKSTATIONS PROCESS CONTROL SYSTEM
ALARM SYSTEMS
OPERATIONAL CONTROL FOR SYSTEM #2 SECURITY LEVEL 2
SYSTEM #2 FIREWALL SECURITY LEVEL 2
BOUNDARY ZONE 2/3 FOR SYSTEM #2 SECURITY LEVEL 2
SYSTEM #2 FIREWALL SECURITY LEVEL 2
IP PHONES
IP PHONES VLAN SECURITY LEVEL 3
HMI
CONTROL ROOM WORKSTATIONS PROCESS CONTROL SYSTEM
ALARM SYSTEMS
OPERATIONAL CONTROL FOR SYSTEM #N SECURITY LEVEL 2
SYSTEM #N FIREWALL SECURITY LEVEL 2
BOUNDARY ZONE 2/3 FOR SYSTEM #N SECURITY LEVEL 2
SYSTEM #N FIREWALL SECURITY LEVEL 2
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER NAT/PAT
BOUNDARY ZONE 3/4 HIGHER SL ARE MASKED SECURITY LEVEL 3
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER NAT/PAT
10.3.1.0/24
I&C LAYER 4
ENGINEERING WORKSTATIONS
NETWORK PRINTERS
IP PHONES
IP PHONES VLAN SECURITY LEVEL 3
PLANT HISTORIAN
SUPERVISION REAL TIME SYSTEMS NOT REQUIRED FOR OPERATIONS SECURITY LEVEL 3
DMZ FOR INFORMATION EXCHANGE BETWEEN SL 2/3
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER
SITE BUSINESS INTERNAL DISTRIBUTION CORE SECURITY LEVEL 4
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER
BOUNDARY ZONE 4/5 SECURITY LEVEL 4
LAN ROUTER FIREWALL FAIL OVER ARCH. IDS FILTER
UPS
single corded loads
10.4.1.0/24
SITE BUSINESS WORKSTATIONS WORK PERMIT AND WORK ORDER SYSTEM
NETWORK PRINTERS
IP PHONES
IP PHONES VLAN SECURITY LEVEL 4
SITE BUSINESS PLANNING AND LOGISTICS ZONE SECURITY LEVEL 4

Security Level 2 **Security Level 3** **Security Level 4**



1. The SL3-4 kiosk engines are not up to date.

2. An infected USB stick is used for data exchange between SL3-4.

3. A network path (bad security gateway) allows uncontrolled traffic and a remote desktop connection between SL3 and SL4.

CD Pressure & Level Controllers

4. A dedicated condenser pump controller (PLC 1200 - tertiary) is wrong located in a SL3 zone.

5. Access to Internet from SL4 is allowed to users provided adequate protective measures. A remote maintenance access is allowed.

7. An malware allows *Incognitus* access through out remote desktop.

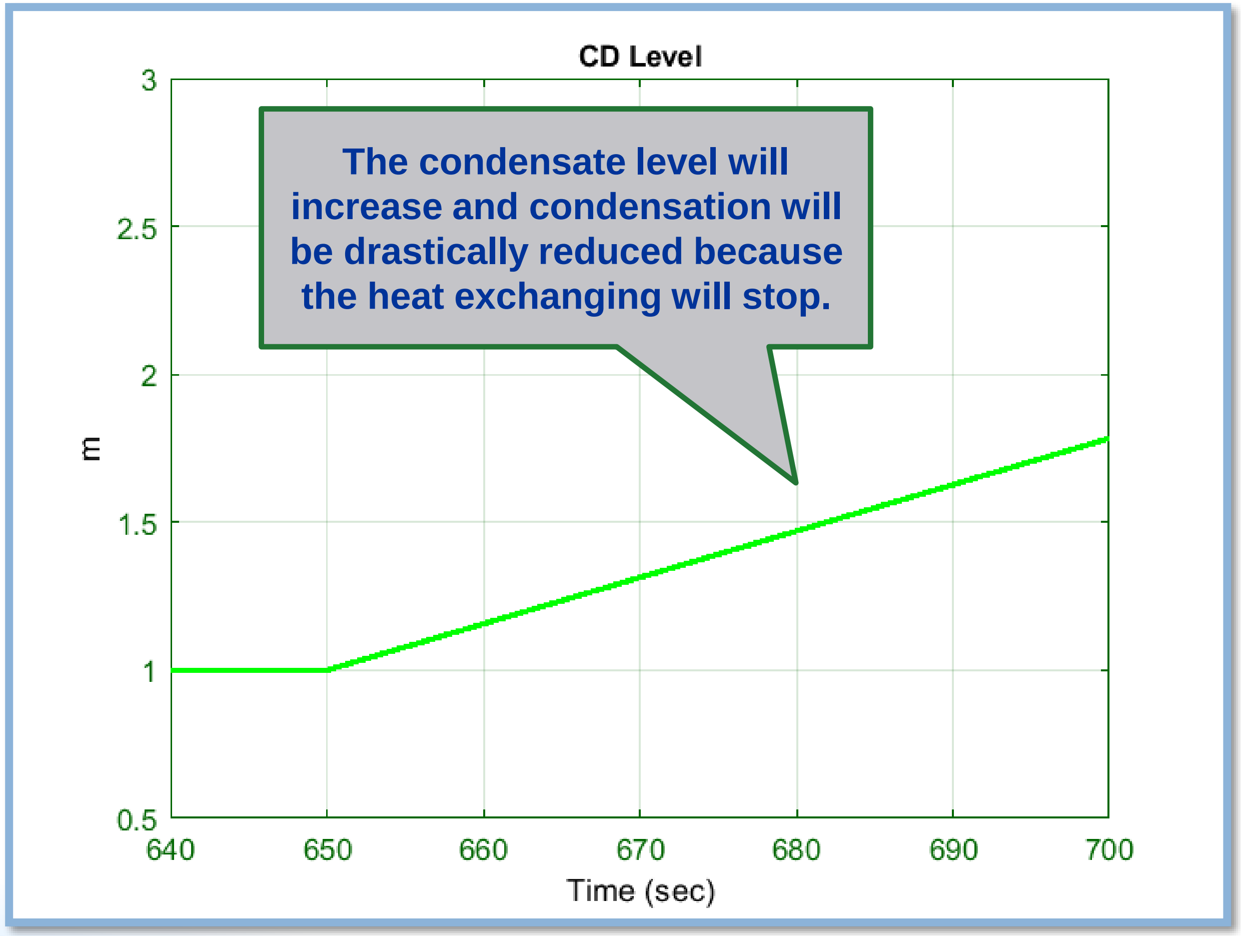
8. *Incognitus* uses captured information to perform a man-in-the-middle type attack. The OPC communication is compromised.

6. The condenser pump is turned off. The CR HMI does not present that information.

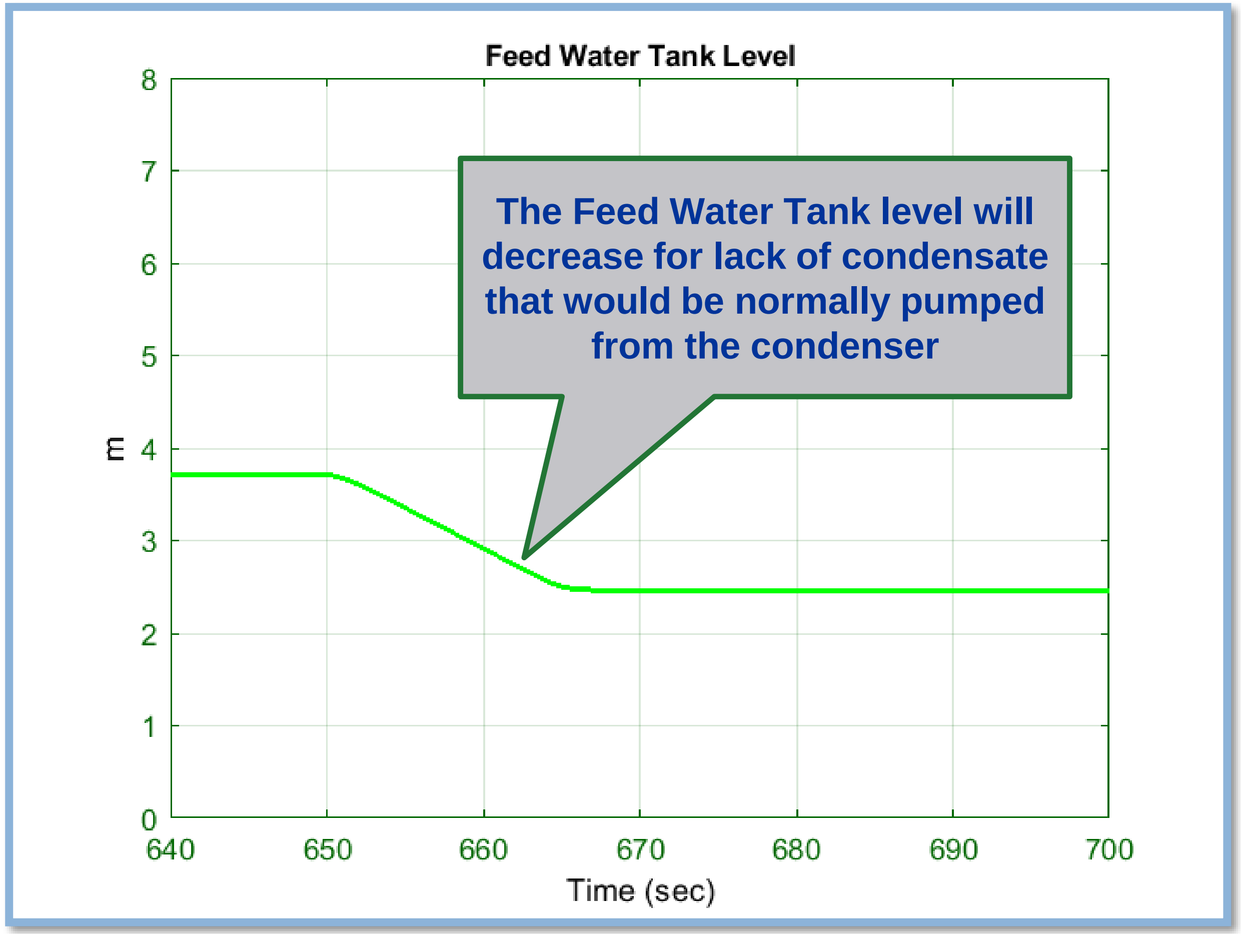
7. The Condenser Pump Controllers are compromised.

Firewall

Condenser & Feed Water Levels



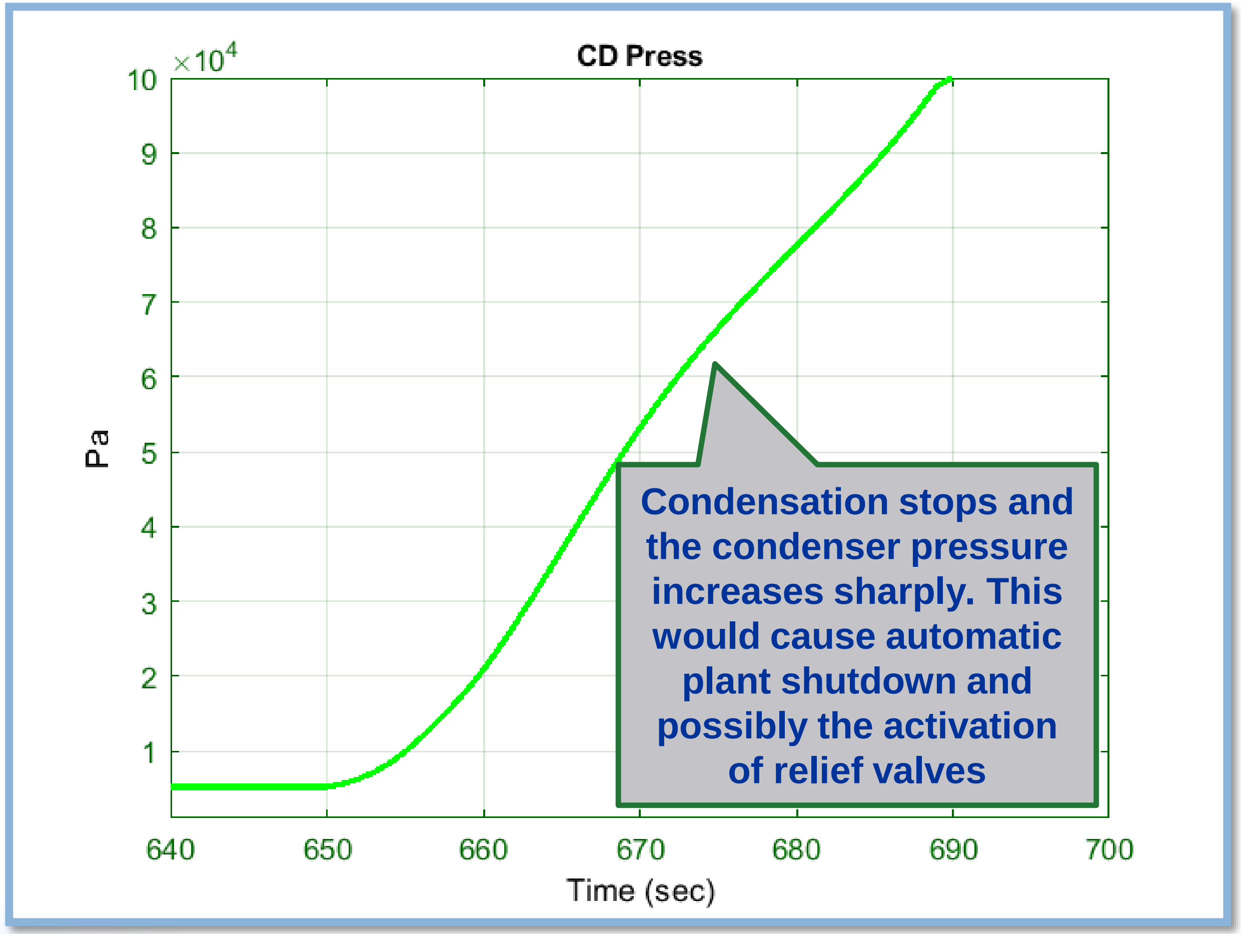
The condensate level will increase and condensation will be drastically reduced because the heat exchanging will stop.



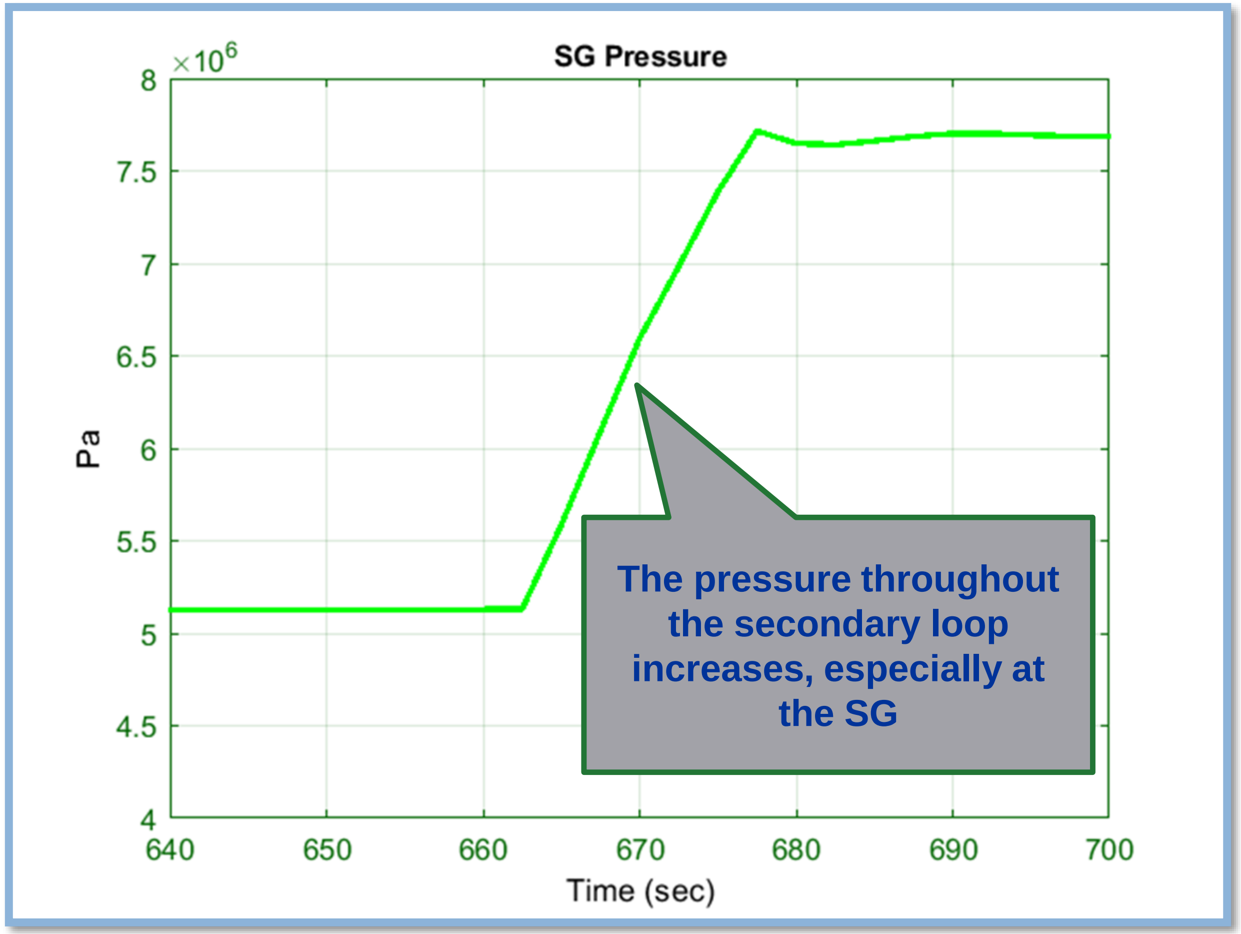
The Feed Water Tank level will decrease for lack of condensate that would be normally pumped from the condenser

No heat is extracted and condensation stops

Condenser & SG Pressure



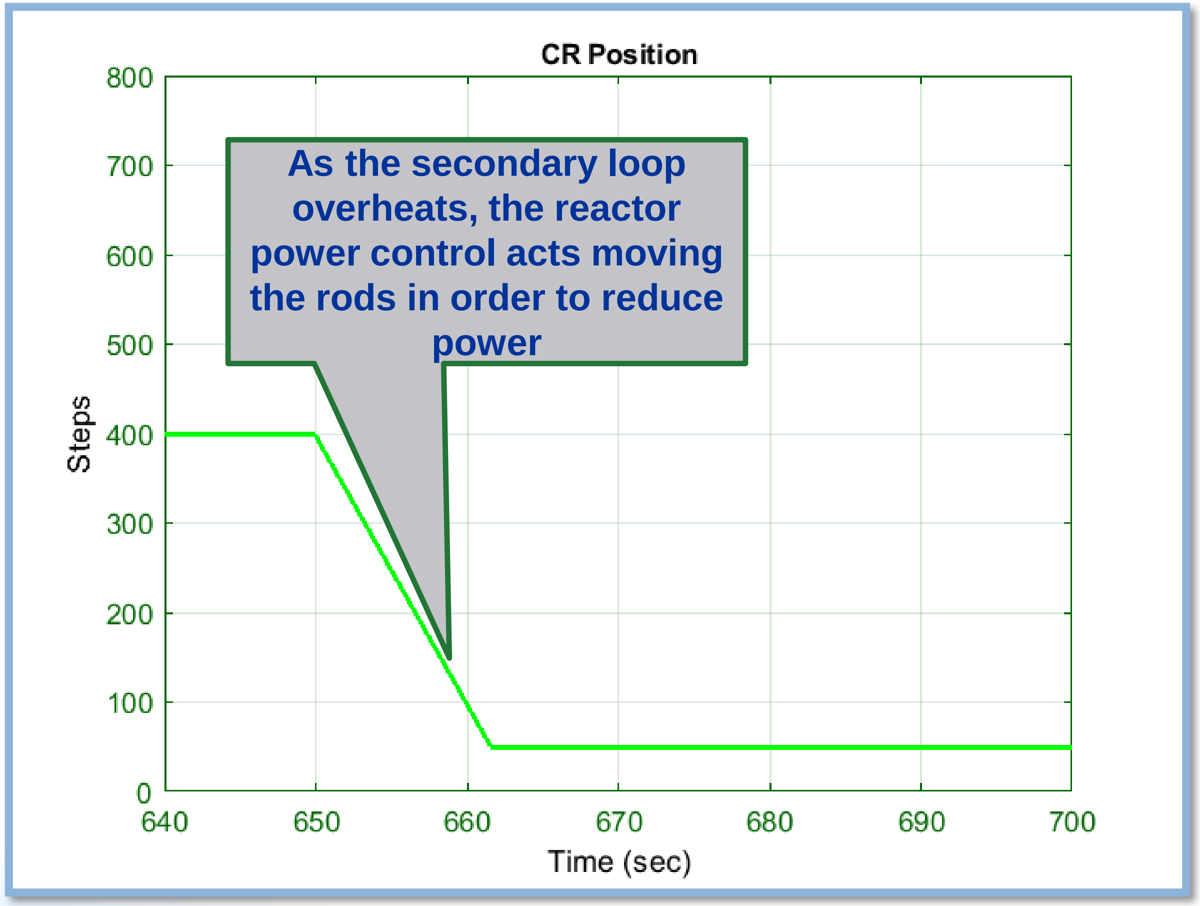
Condensation stops and the condenser pressure increases sharply. This would cause automatic plant shutdown and possibly the activation of relief valves



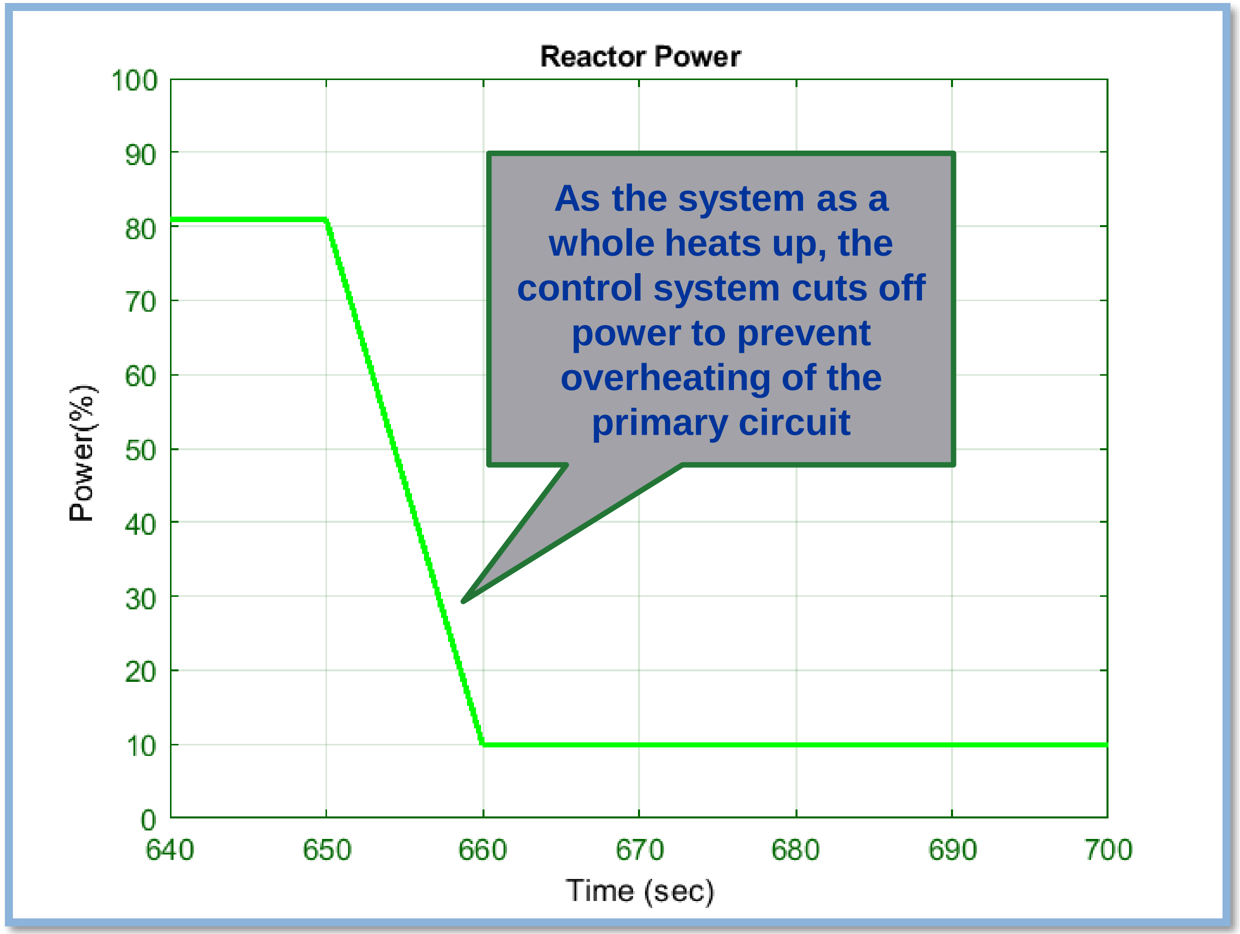
The pressure throughout the secondary loop increases, especially at the SG

Overpressure on TB and SG activates the Steam Dump Valve

Nuclear Reactor Power

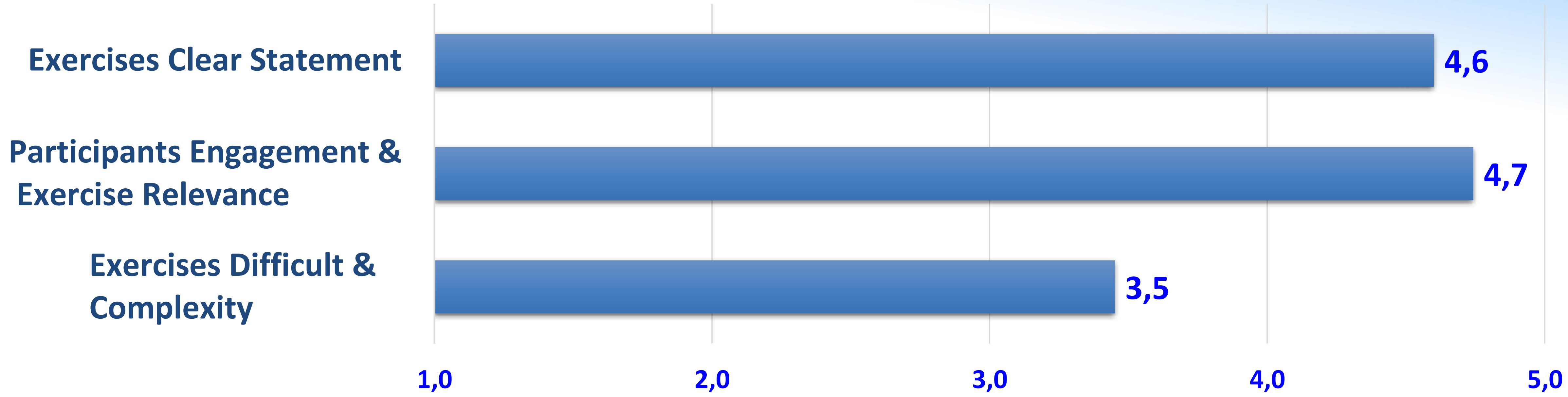


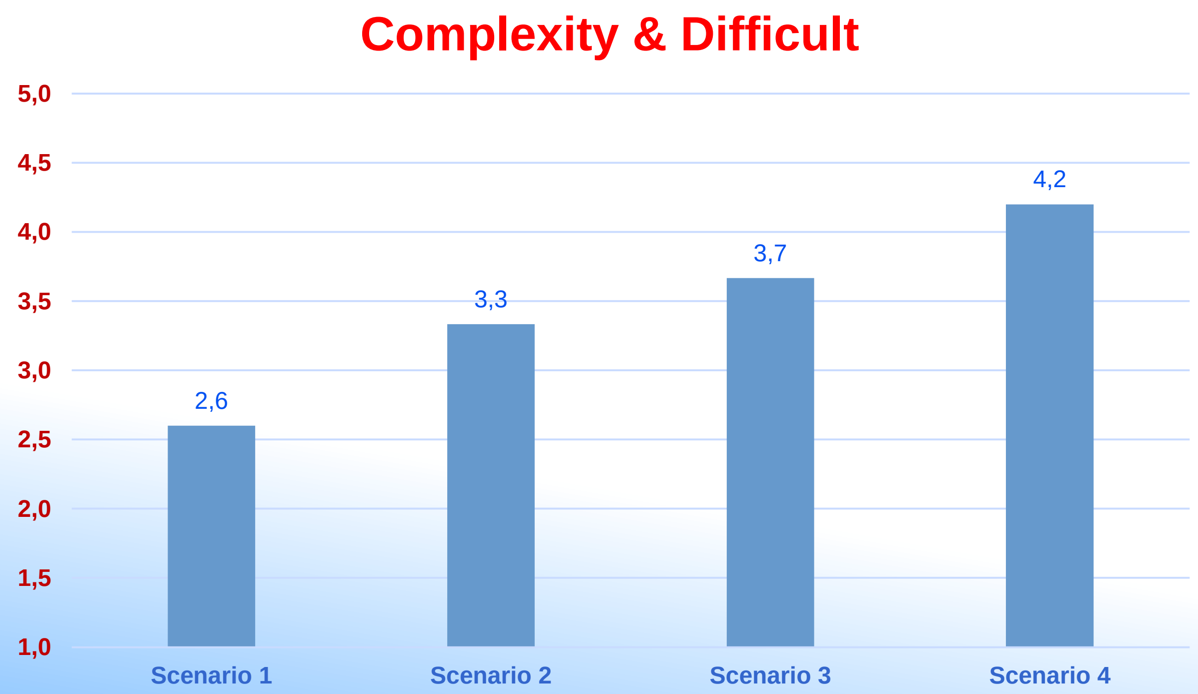
As the secondary loop overheats, the reactor power control acts moving the rods in order to reduce power

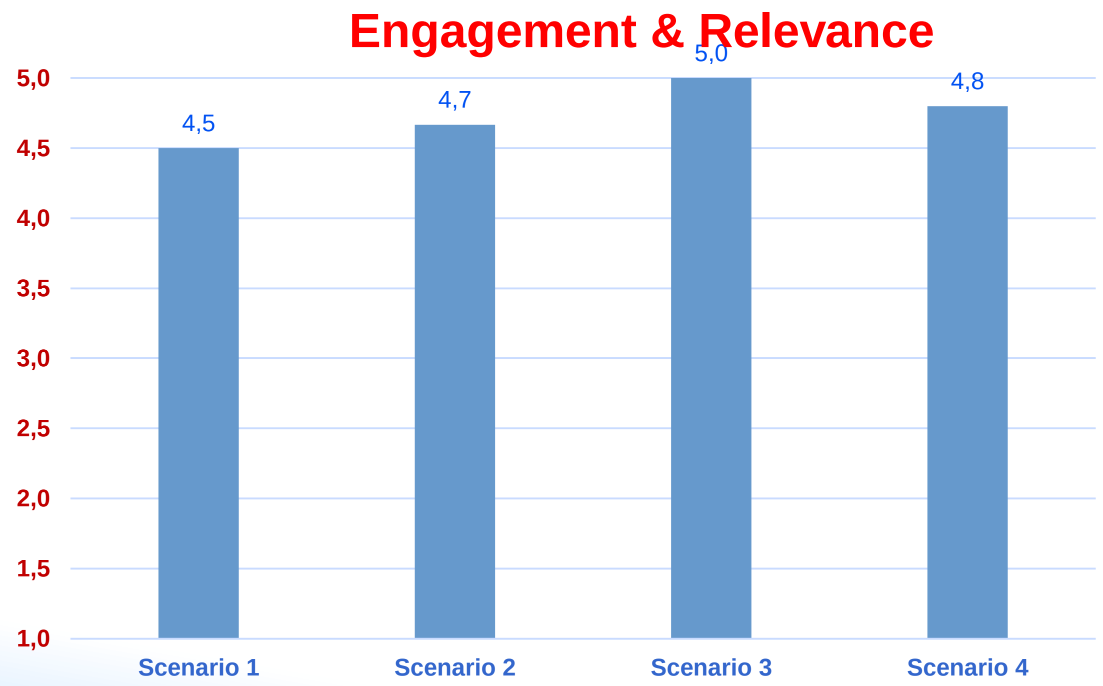


As the system as a whole heats up, the control system cuts off power to prevent overheating of the primary circuit

Hands On


Exercises Clear Statement
4,6
Participants Engagement & Exercise Relevance
4,7
Exercises Difficult & Complexity
3,5
1,0
2,0
3,0
4,0
5,0


Complexity & Difficult
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
2,6
3,3
3,7
4,2
Scenario 1
Scenario 2
Scenario 3
Scenario 4


Engagement & Relevance
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
4,5
4,7
5,0
4,8
Scenario 1
Scenario 2
Scenario 3
Scenario 4

#ICONS2020