# CYBER SECURITY ACCIDENTS AND I&C SYSTEMS IN NUCLEAR POWER PLANTS

**Assist. Prof. Magy M. Kandil**

Egyptian Nuclear and Radiation Regulatory Authority (ENRRA)
Cairo, Egypt

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities
13–17 November 2017, Vienna, Austria

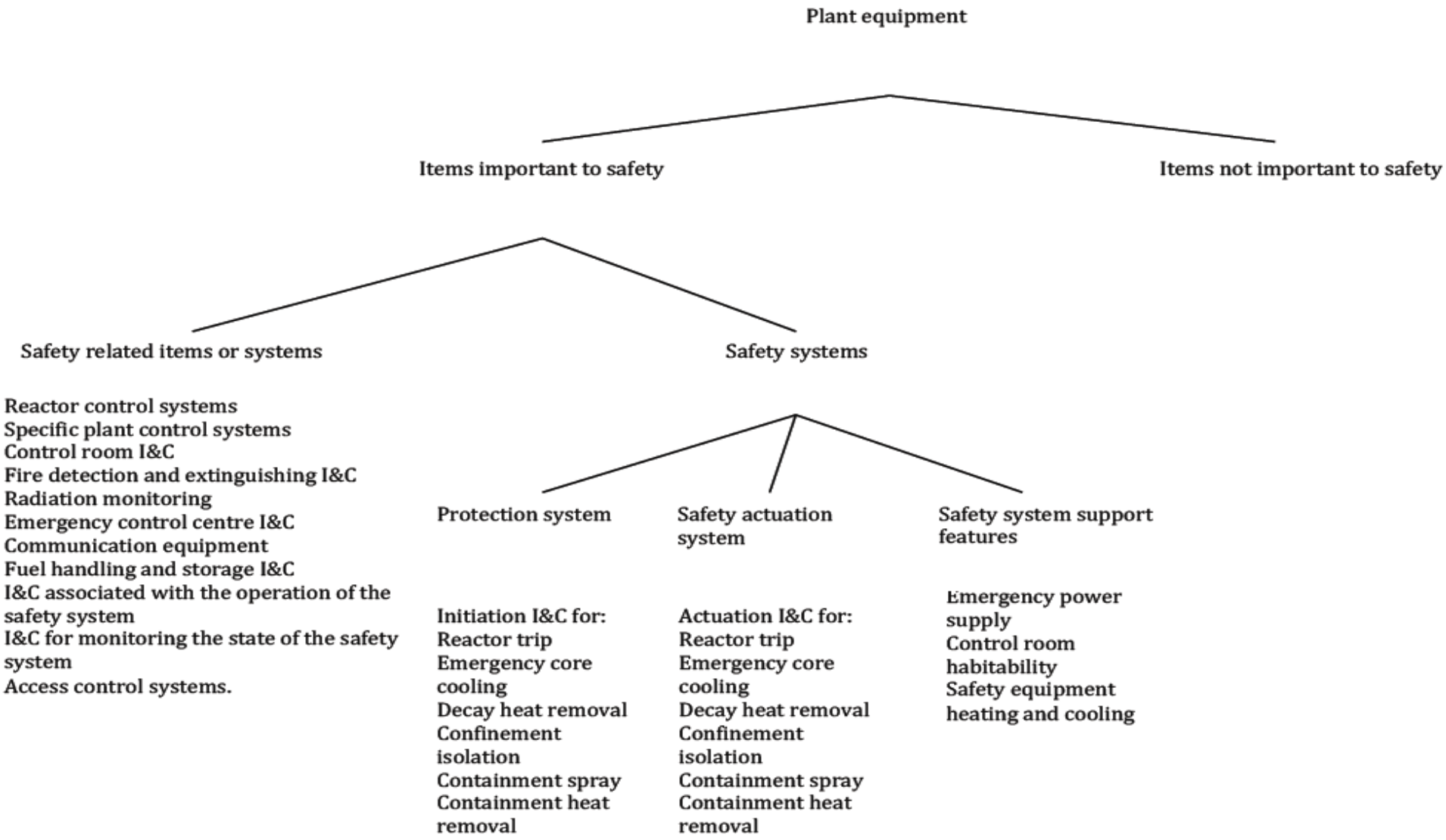
# AGENDA

- Introduction
- The Simplified Computer Security Defensive Architecture
- A Typical Configuration of I&C System In NPPs
- High Level Overview of I&C Main Functions
- The I&C System Architecture
  Main Functions.
- The Functional Overview of NPP I&C
- The Typical Systems and Networks in NPP
- The Interconnection of Control Networks in NPPs
- The Possible Structure of NPPs Network Computer Systems.
  The Possible Threats of The Control Networks in NPPs.
  The Vulnerabilities Of Control Networks in NPPs
- Cyber Physical Security Accidents in NPPs
- Conclusions

# 1. INTRODUCTION

- The Electrical and mechanical equipments for nuclear power plants are very important to nuclear safety and dependent upon computer based equipment, appropriate standards and practices for the development and testing of computer hardware and software shall be established and implemented throughout the service life of the system, and in particular throughout the software development cycle.
- It is important to classify the functions, systems and equipment of NPPs into safety classes. The purpose of the classification is to guarantee that each object in the NPP is getting the required attention based on its importance to safety as shown in fig. 1.

# FIG .1 THE ELECTRICAL AND MECHANICAL EQUIPMENTS SAFETY CLASSES IN NPPS



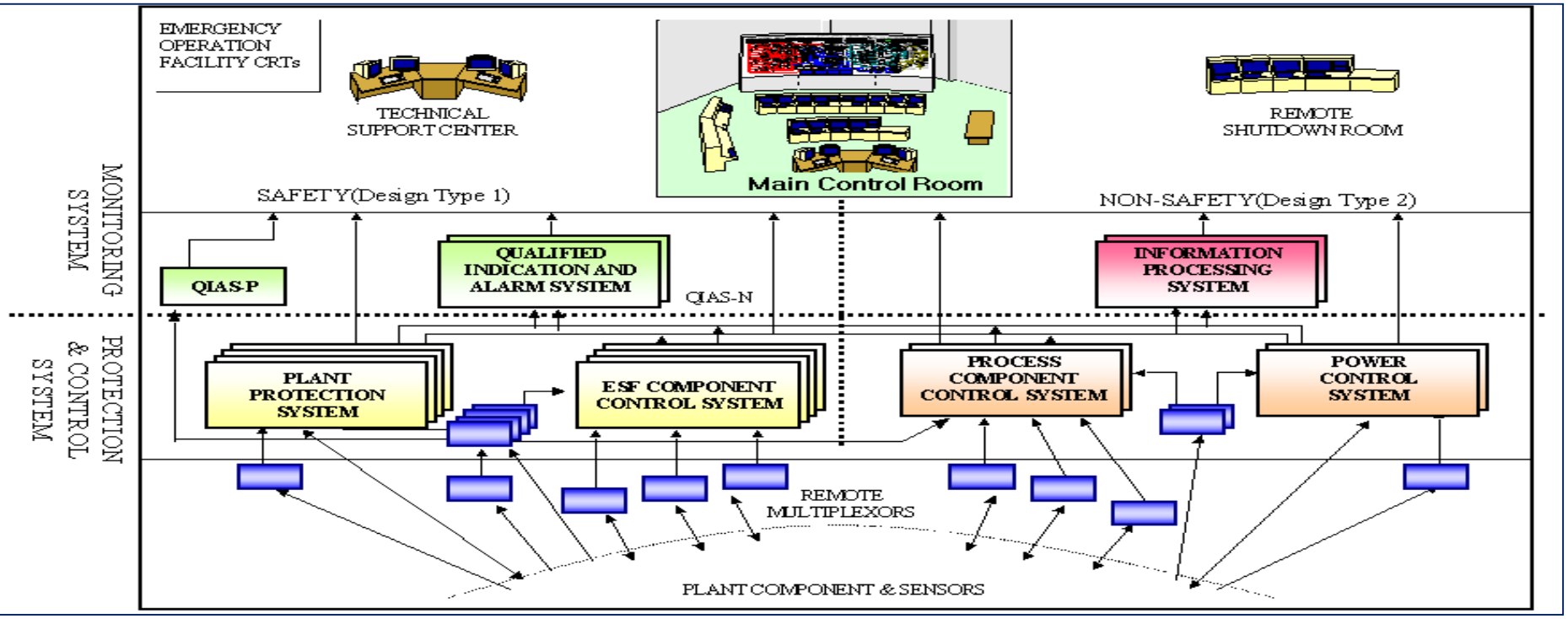
# TABLE 1. SAFETY CLASSIFICATIONS ARE APPLIED TO INSTRUMENTATION AND CONTROL SYSTEMS

| National or international standard | Classification of the importance to safety | | | | |
|---|---|---|---|---|---|
| IAEA NS-R-1 | Systems Important to Safety | | | | Systems Not Important to Safety |
| | Safety | | Safety Related | | |
| IEC 61226 Functions Systems | Systems Important to Safety | | | | Unclassified |
| | Cat. A Class 1 | Cat. B Class 2 | Category C Class 3 | | |
| Canada | Category 1 | Category 2 | Category 3 | | Category 4 |
| France N4 | 1E | 2E | SH | Important to Safety | Systems Not Important to Safety |
| European Utility Requirements | F1A (Auto.) | F1B (Auto. and Man.) | F2 | | Unclassified |
| Japan | PS1/MS1* | PS2/MS2 | PS3/MS3 | | Non-nuclear Safety |
| Rep. of Korea | IC-1 | | IC-2 | | IC-3 |
| Russian Federation | Class 2 | Class 3 | | | Class 4 (Systems Not Important to Safety) |
| Switzerland | Category A | Category B | Category C | | Not important to safety |
| UK Functions Systems | Cat. A Class 1 | Cat. B Class 2 | Category C Class 3 | | Unclassified |
| USA and IEEE | Systems Important to Safety | | | | Non-nuclear Safety |
| | Safety Related, Safety, or Class 1E | (No name assigned) | | | |

# THE SIMPLIFIED COMPUTER SECURITY DEFENSIVE ARCHITECTURE


The fig. illustrates a defense-in-depth example of computer security architecture, used to protect the critical digital assets (CDAs) from cyber-attack. Level 4 includes the data of the CDAs associated with safety, safety related, security related, and support systems and equipment. The level 4 data must be protected from all lower levels. Thus, the data at level 4 flows only in one direction, to level 3, and from level 3 to level 2. It is prohibited to start reversing communication from lower security, level 0, to the high security level 4 & 3 Currently, this

# A TYPICAL CONFIGURATION OF I&C SYSTEM IN NPPS




The safety systems are placed on the left half and the non-safety systems on the right half. The NPP I&C system has similar constituents and structure to those of control systems in other industries except the safety systems. The safety systems function to shutdown the reactor safely and maintain it in a shutdown condition. The safety systems require higher reliability, functionality, and availability than the non-safety.

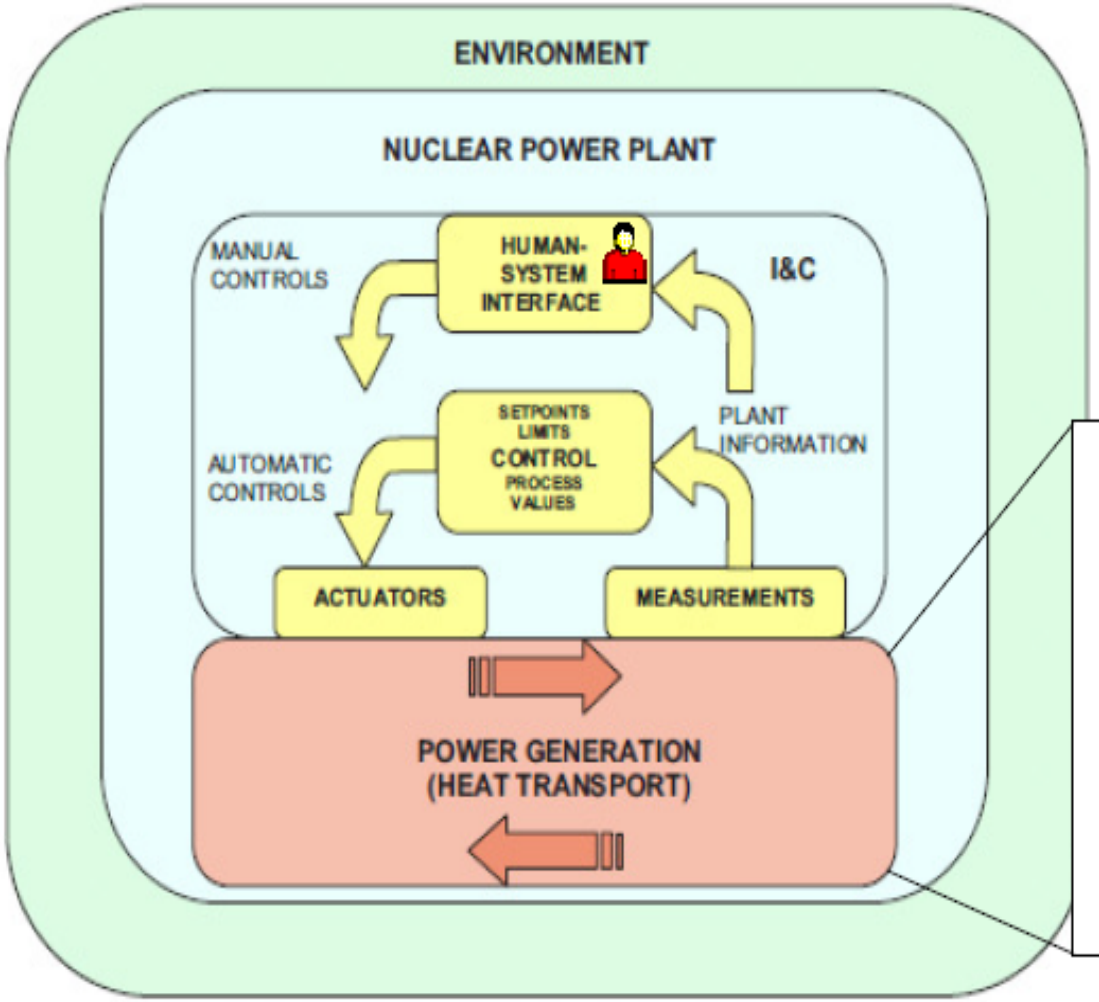
# THE I&C SYSTEM ARCHITECTURE
# MAIN FUNCTIONS

1. **Measurement and sensing, and detecting** the physical processes in the NPP and their signals are sent through communication systems to the operator, as well as to the decision-making applications (analogy or computer-based).

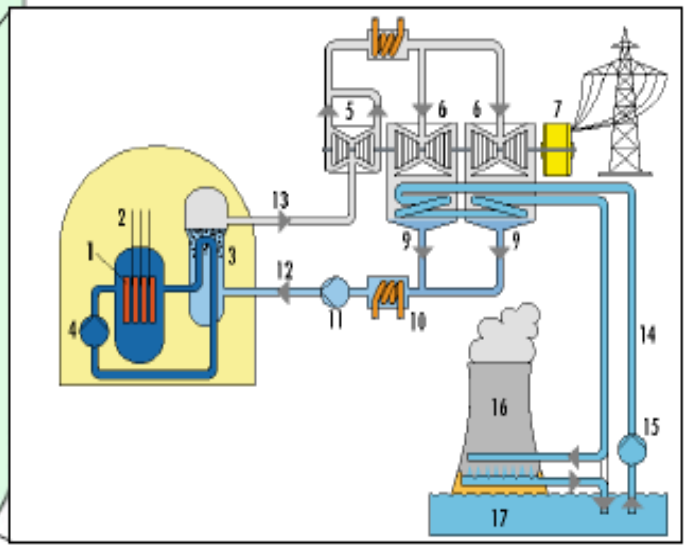
2. **Regulate plant processes** (i.e. keeping process parameters within acceptable limits) and to protect against abnormal conditions.

3. **Provide automatic control**, both of the main plant and of many ancillary systems.

# HIGH LEVEL OVERVIEW OF I&C MAIN FUNCTIONS (UNDERSTANDING NUCLEAR I&C) ASSETS)

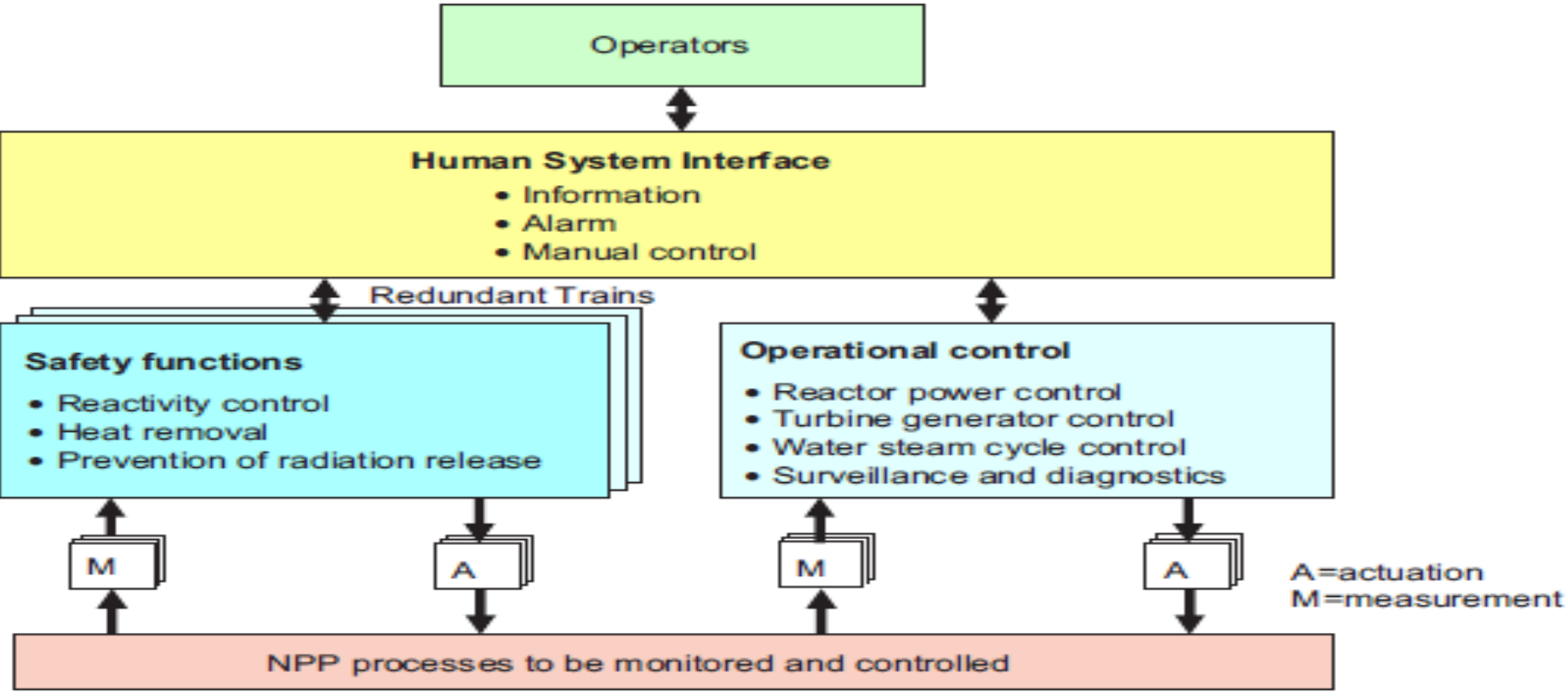



Energy production process



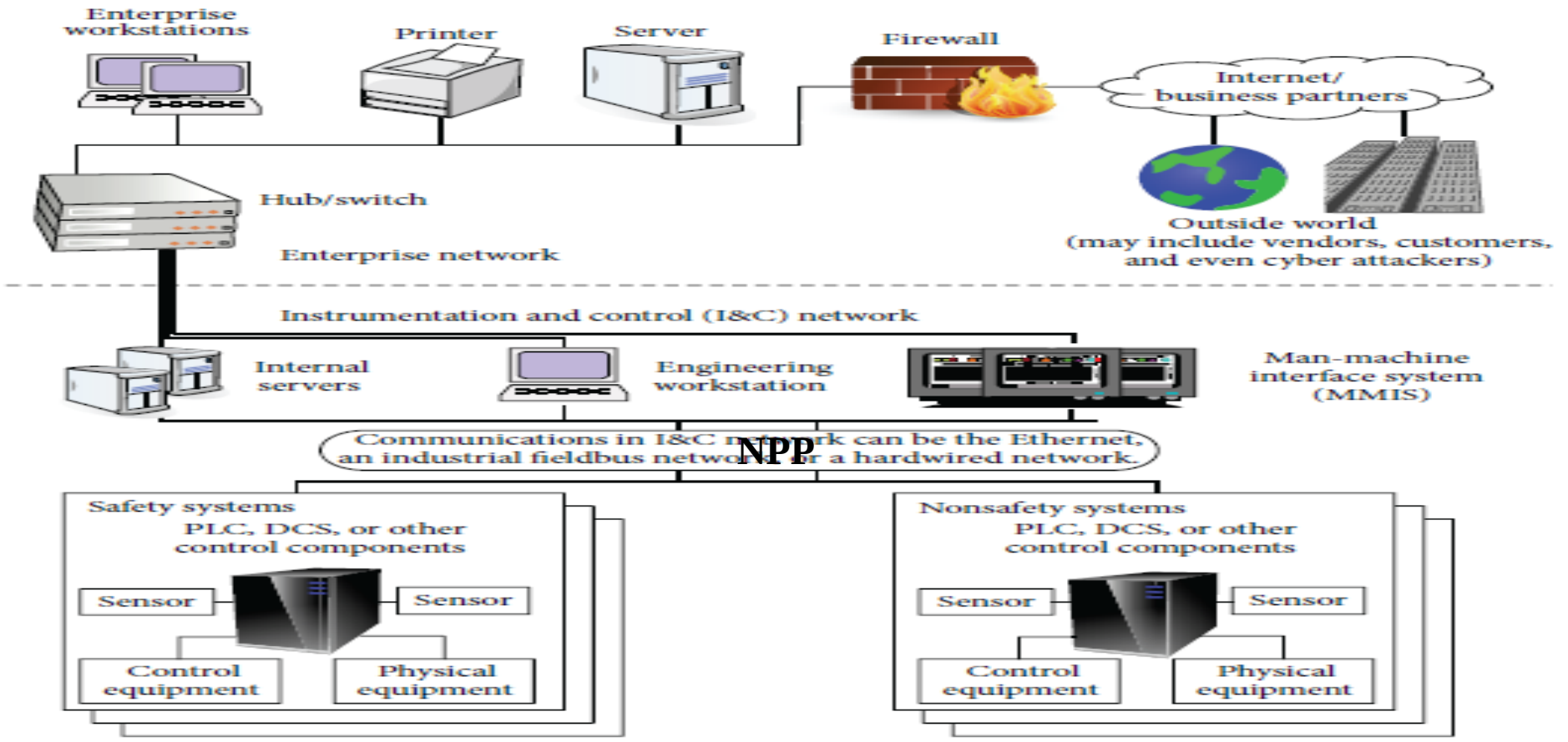

Source: IAEA Nuclear Energy Series NP-T-3.12

# THE FUNCTIONAL OVERVIEW OF NPP I&C




The functional of the I&C in a NPP is a main role to ensure a safe and reliable plant operation under all plant conditions, I&C systems have to monitor and control hundreds or thousands of plant parameters. Thus, nuclear power plant I&C systems are complex. Subdividing the plant I&C according to its functions facilitates understanding of the entire system.

# THE TYPICAL SYSTEMS AND NETWORKS IN NPP




A typical modern NPP I&C system consists of control components such as distributed control systems (DCSs) or programmable logic controllers (PLCs) that interact with physical equipment directly and industrial PCs or engineering workstations that are used to regulate control components and their related works.

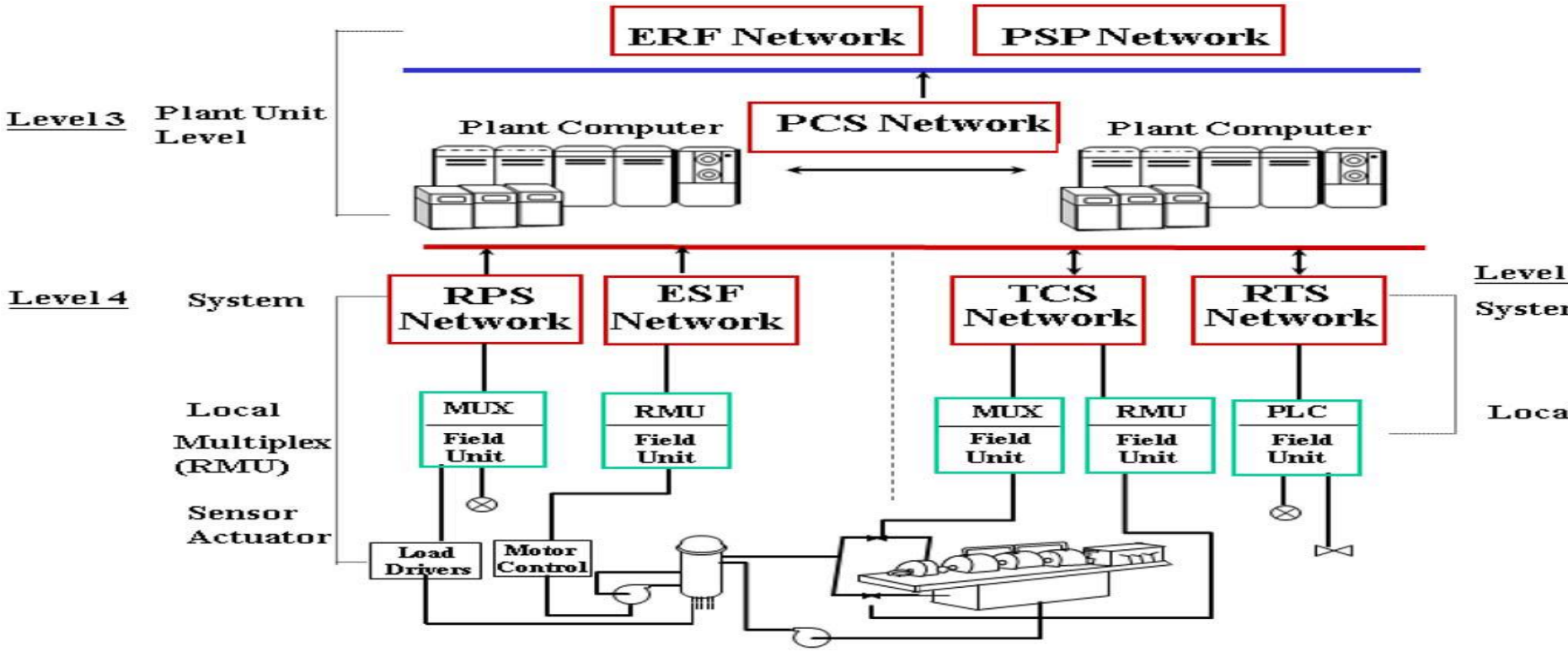
# THE POSSIBLE STRUCTURE OF NPP'S NETWORK COMPUTER SYSTEMS

1) **Internet :** The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite to serve billions of users worldwide.(Wikipedia). Representing homepage of NPP's must be connected to the internet so that people can access the homepage to get general information about the NPP. There are also some other information systems which are publicly open for the purpose of taking applications from job- seekers or contractors.

2) **Intranet** : An intranet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or network operating system within that organization(Wikipedia). Actually there are two types of intranet:

- The private network is connected to the Internet but it is protected by information security systems such as Firewall or Intrusion Protection System.
- The private network is physically isolated from outside network.

# THE INTERCONNECTION OF CONTROL NETWORKS IN NPPs




The control networks can be composed of seven components: the emergency response facility (ERF) system, the engineered safety feature (ESF) system, the plant control system (PCS), the physical security protection (PSP) system, the reactor protection system (RPS), the radwaste treatment system (RTS), and the turbine control system (TCS). Among the control networks, we concentrate on the ERF system and the PSP system, which are the only routes to provide information outside thus the cyber security as well as physical security are critical issues in analyzing control systems in NPPs.

# THE POSSIBLE THREATS OF THE CONTROL NETWORKS IN NPPS

- NPP I&C systems generally use closed data and communication networks or air-gaps such that access through the Internet to the systems becomes difficult.

- However, recent cases of Advanced Persistent Threat (APT) Attacks demonstrate that NPP I&C systems may also be infected by malware enabling cyber attacks through portable devices such as notebooks and USB drives.

- It is very important to identify all the connection points between humans with external electronic devices and the I&C systems, and to analyze potential security breaches that can be exploited by cyber threats. These connection points are usually related to the plant maintenance and test tasks.

# THE VULNERABILITIES OF CONTROL NETWORKS IN NPPS

The North American Electric Reliability Council (NERC) listed the top 10 vulnerabilities of control systems and recommended mitigation strategies :

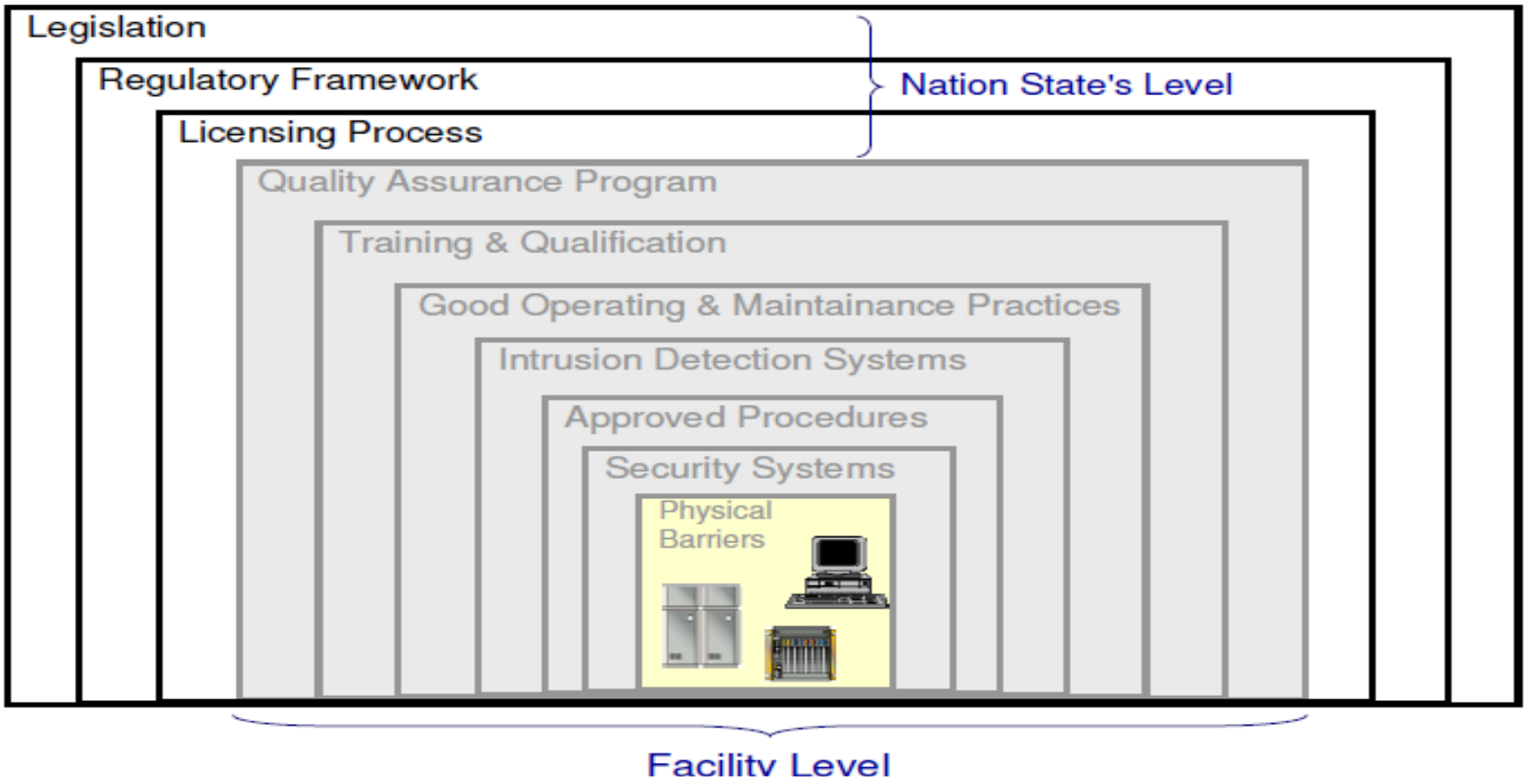
1. Inadequate policies, procedures, and culture that govern control system security,
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms,
3. Remote access to the control system without appropriate access control,
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained,
5. Use of inadequately secured wireless communication for control,

# THE VULNERABILITIES OF CONTROL NETWORKS IN NPPS cont'd

6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes,
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity,
8. Unauthorized or inappropriate applications or devices on control system networks,
9. Control systems command and control data not authenticated, and
10. Inadequately managed, designed, or implemented critical support infrastructure.

These vulnerabilities contain both managerial and technical vulnerabilities. Among these vulnerabilities, items 1), 2), 7), and 9) may exist in NPP I&C systems, but other items are less related.

# THE SECURITY LEVELS OF I&C SYSTEMS IN NPPS




The security of computer systems should be based on a graded approach: categorize computer systems into zones, where graded protective principles are applied The overall I&C architecture should define the defence-in-depth and diversity strategy to be implemented within the overall I&C. Build a security design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable

# CYBER PHYSICAL SECURITY ACCIDENTS IN NPPs

**In January 2003,** at Ohio's Davis–Besse NPP, the maintenance personnel bridged the private control networks to the dial-up T1 line. As the personnel at home dialed the plant control networks, the Slammer worm incubated in his personal computer spread to the control networks and disabled a safety parameter display system for nearly 5 h .

- **In August 2005**, at Seabrook NPP, a project engineer performed a test to verify that a remote LAN personal computer would not control a supplemental emergency power supply (SEPS). During the test, the two physical SEPS diesel generators started unexpectedly.
- **In March 2008,** at Hatch NPP, the reactor automatically scrammed on low reactor water level following a loss of coolant water since a software application test was being performed from a computer attached to the site LAN and was separated by a FW from the plant data acquisition system (DAS) server.

# CYBER PHYSICAL SECURITY ACCIDENTS IN NPPs cont'd

- **In Sep. 2011** A group of hackers attacked several North American natural gas producers, testing for possible ways to breach the system. In one attack, the hackers stole the subscriber contact list of a nuclear management newsletter and sent spyware-loaded e-mails to the e-mail addresses on the contact list before the newsletter was sent. This attempt ended with the successful breaking into the computer network of Diablo Canyon nuclear plant at the north of Santa Barbara.
- **In August 2012**, when a Chinese hacking team attempted to infiltrate a U.S. nuclear facility. The Department of Homeland Security (DHS) did not disclose the name of the nuclear power plant or other plants that experienced similar attacks, to protect the facilities from potential future attacks. Meanwhile, Chinese military hackers took control of a senior plant manager's computer. The plant's incident team investigators concluded that Chinese hackers wanted to identify security and operational vulnerabilities of U.S. nuclear reactors.

# CYBER PHYSICAL SECURITY ACCIDENTS IN NPPs cont'd

- **In October 2012**, when a technician inserted a compromised USB into a power plant's network during a scheduled outage for equipment upgrades, he inadvertently kept the plant offline for three weeks. The third-party technician did not know that the USB was infected. The Department of Homeland D security did not mention the name or location of the power plant but identified the malware in the third-party contractor's USB as a variant of the Mariposa virus. On cyber security lists, Mariposa is classified as a botnet, not a virus, which steals personal data, account information, usernames, passwords, and banking details from compromised computers. These infected computers can also be used for distributed denial of service (DDoS) attacks.

# CYBER PHYSICAL SECURITY ACCIDENTS IN NPPs cont'd

- **In January 2, 2014,** A computer, normally used to file company paperwork by on-duty facility employees in the Monju nuclear reactor facility in Tsuruga, Fukui Prefecture, began to suspiciously send and receive data from an unknown website at 3:00 PM. Upon closer inspection it was revealed that, the computer was infected during a regular update of a video playback program. Although the infected computer contained sensitive e-mails, employee data sheets, and training logs that could be used for another attack, the Japan Atomic Energy Agency claimed that no data that could compromise the safety of the plant was leaked.
- **In December 2015,** energy blackouts in Ukraine that affected 225,000 customers 9 and allowed attackers to control the grid's industrial control systems (ICS) and supervisory control and data acquisition (SCADA) components;
- **April 2016,** worm infection of the Gundremmingen nuclear power plant in Germany

# CONCLUSIONS

- **Digital technologies** such as computers, control systems, and data networks currently play essential roles in modern nuclear power plants (NPPs).
- **The new technologies** such as wireless sensor networks is also being considered. These digital technologies make the operation of NPPs more convenient and economical; however, they are inherently susceptible to cyber-attacks accidents or incidents demonstrate that the enterprise networks of NPPs connected to the Internet are exposed to the same cyber threats that target many unspecified systems in conventional IT environments.
- **There are many areas in NPPs** that are vulnerable to cyber-attacks. So that, the Nuclear power plants must be have strong defenses against an insider threat. Individuals who work with digital plant equipment are subject to increased security screening, cyber security training and behavioural observation.

# CONCLUSIONs cont'd

**Nuclear power plants are designed to:**

1. shut down safely if necessary, even if there is a breach of cyber secure
2. automatically disconnect from the power grid if there is a disturbance caused by a cyber attack. These A cyber attack must be not prevent critical systems in a nuclear energy facility from performing their safety functions

These features in each nuclear power plant's achieved by cyber security protects its digital computer and communication systems and networks against cyber attacks, including systems and networks associated with:

Safety-related functions and secondary functions considered "important-to-safety"; Security functions; Emergency preparedness functions, including offsite communications; and, Support systems and equipment important to safety and security.

# CONCLUSIONs cont'd

- **As the number of cyber and information attacks increases**, facilities must be increasingly vigilant of protecting their assets. This is especially true for nuclear facilities where compromised security can lead to degradation of safety systems, which in turn can lead to detrimental consequences to the facility, humans, and the environment. It is of utmost importance that information security professionals are trained properly and can stay ahead of the threat.
- **The cyber attack Accidents NPPs** proved the importance of having an incident investigation team for the protection of facilities against cyber attacks. Since having an incident investigation team was deemed not feasible and costly by NPP operates, such tasks are generally allocated to facility engineers. However, incident investigation requires unique techniques to detect, track and trace cyber attacks.

# THANK YOU FOR YOUR ATTENTION


## *QUESTIONS*