U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Cyber Security:
Safety and Security Interface

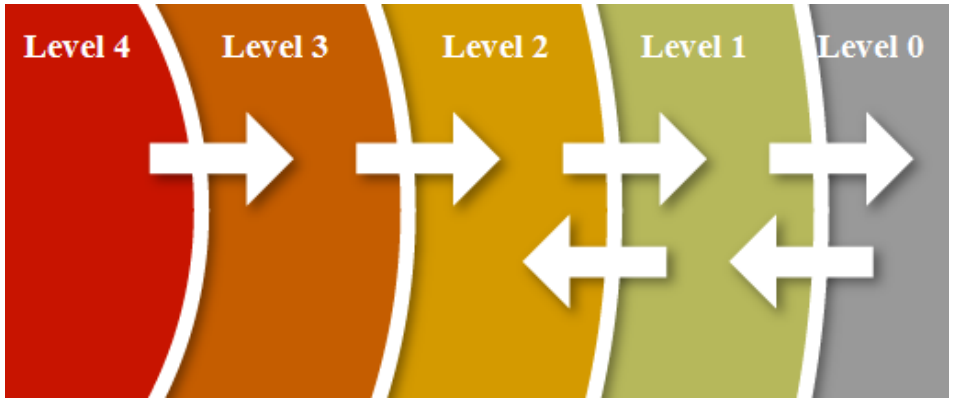
October 8, 2009

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Objectives

- RG 5.71: Defensive architecture
- Digital I&C ISG-04
- U.S. EPR I&C systems Architecture
- Interface issues between safety and security

Defensive Architecture



Simplified Cyber Security Defensive Architecture

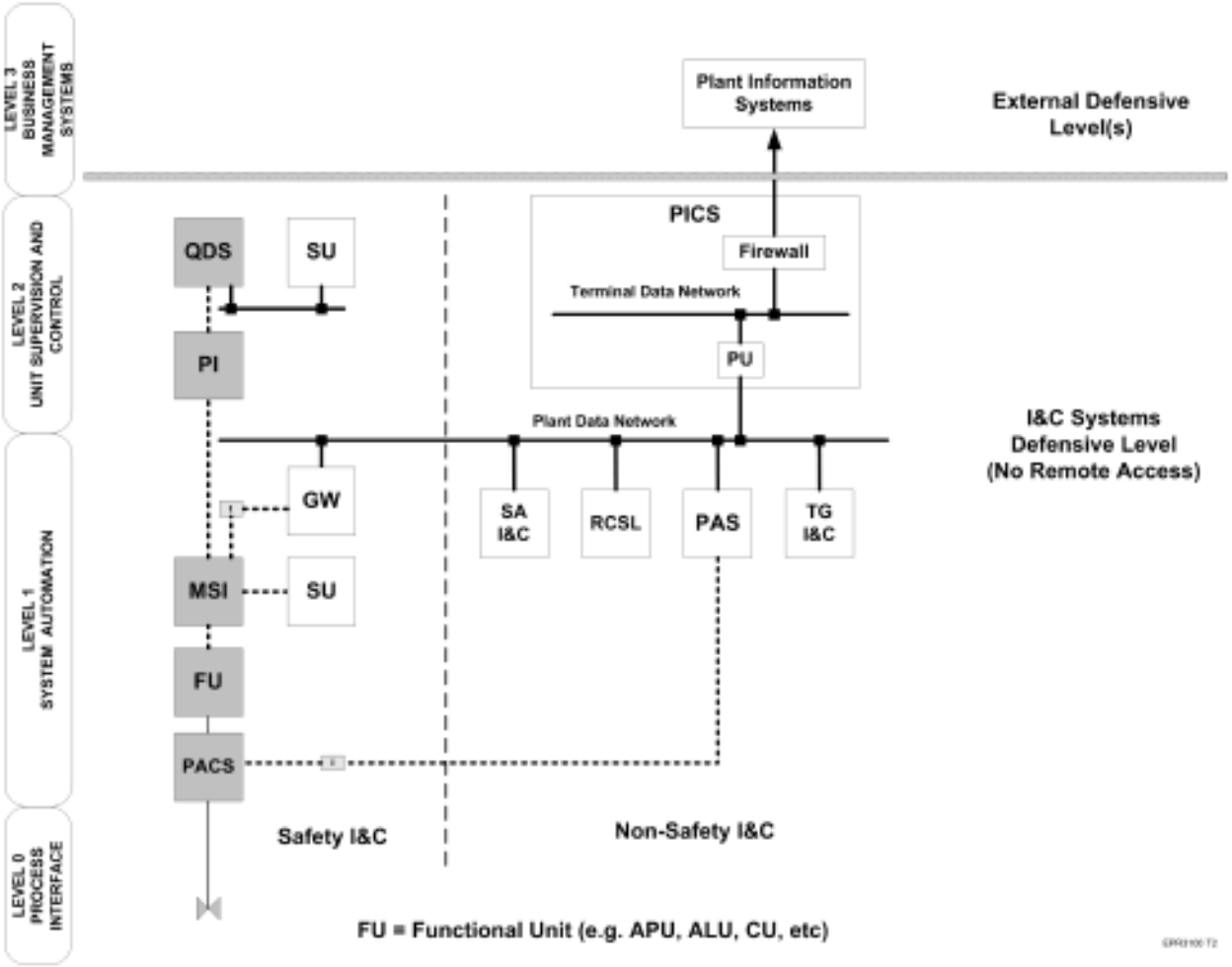
- Systems associated with safety, security, EP functions, and support systems are allocated to level 4 and are protected from all lower levels.
- Only one-way data flow is allowed from level 4 to level 3
- Data flows from one level to other levels only through a device that enforces security policy between each level
- Systems that perform safety, security, EP functions are to address security risks by applying security controls within Appendix B and C of RG 5.71.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ISG 4
HICR-Communications Issues

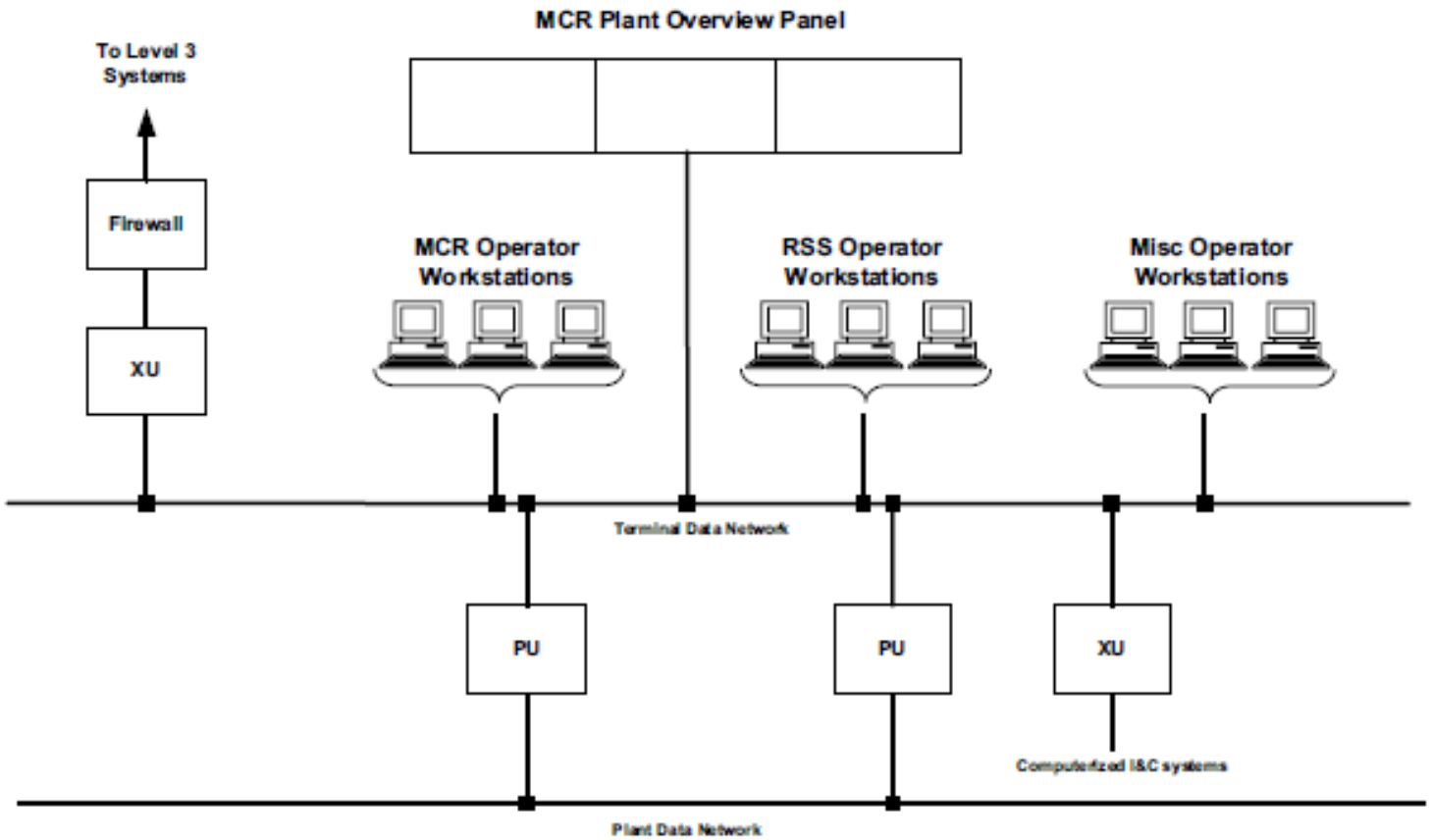
- Digital I&C ISG-04 HICRc-Communications Issues allows certain bi-directional communication between safety and non-safety systems.
  - ISG-04 only addresses communications independence between safety systems and non-safety equipment, and does not address cyber security.
  - Section 1 of ISG-04 provides twenty criteria that should be addressed to demonstrate sufficient independence for bi-directional communication between safety systems and non-safety equipment.

U.S. EPR I&C System Architecture



Levels of Defense for Cyber Security

U.S. EPR I&C System Architecture



Process Information and Control System Architecture

Safety-Security Interface

Although ISG-04 allows bi-directional communication between the safety system and other non-safety plant systems, the licensees referencing the U.S. EPR design also needs to address the following to meet the requirements of 10 CFR 73.54:

- Ensure that any non-safety equipment (including the supporting networks) communicating to safety systems (or EP, security, and support systems) is also afforded level 4 protection.
- Demonstrate that cyber risks are managed for these non-safety equipment by addressing the security controls in Appendix B and Appendix C of RG 5.71.
- Ensure any changes to these non-safety equipment undergoes a security assessment to ensure that the security of these equipment is not impacted by the proposed changes.