RIC 2011

Perspectives on Plant-Wide Data Systems:

Protection, Control, and Monitoring in Nuclear Power Plants

Paul J. Rebstock, Jr.
United States Nuclear Regulatory Commission
Office of Research / Division of Engineering
March 8, 2011

Introduction & Background

RIC 2010

Digital systems are fundamentally different from hardwired systems

- Much more interconnection & integration
- Vastly different failure modes & spurious operation potential
  - Even if ultimate effect is simply {pump does/doesn't start}… …probabilities are very different
- Vastly different control room design / HF

2

The DI&C Project

RIC 2010

- Created to address specific industry concerns/questions
- Directed specifically toward safety systems
- Created 7 guidance documents:
  - 5 concerning the use of digital systems in nuclear power plants
  - 1 concerning licensing requirements
  - 1 concerning the use of digital systems in fuel cycle facilities

3

USNRC *RIC 2010*

Scope

All systems that use plant data

- Protection Systems
- Safety Systems
- Nonsafety Systems
- Some types of systems will not be addressed explicitly:
  - Physical access control system
  - Systems unrelated to plant data, such as:
    - Personnel work scheduling and timekeeping
    - Inventory control

4

USNRC *RIC 2010*

The Big Picture

Many Systems

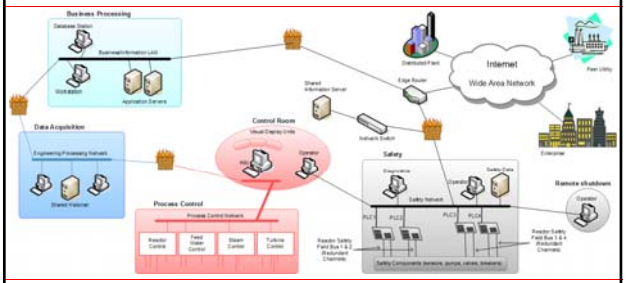
- Use of digital affects many areas
- All have economic implications
- Only a few are important to safety

What is needed to ensure safety while allowing for maximum flexibility in other areas?

5

USNRC *RIC 2010*

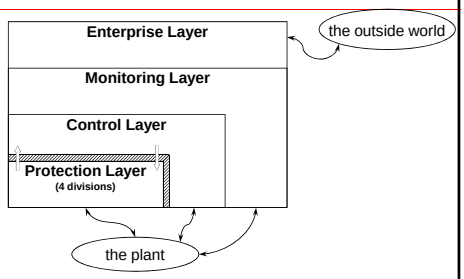
A System of Systems



6

Layers of Systems

RIC 2010



7

Two Main Areas of Concern

RIC 2010

- Interconnections among digital systems
  - Including pathways for errors and malfeasance
- Interactions between digital systems and the plant
  - Including new kinds of failures & spurious actuations not addressed in traditional safety analyses

8

Importance of Simplicity

RIC 2010

"There is no alternative to simplicity. Advances in technology or development methods will not make simplicity redundant; on the contrary, they will give it greater leverage. To achieve high levels of dependability in the foreseeable future, striving for simplicity is likely to be by far the most cost-effective of all interventions. Simplicity is not easy or cheap, but its rewards far outweigh its costs."

-- Software for Dependable Systems: Sufficient Evidence?
National Research Council of the National Academies
The National Academies Press, 2007
Page 81

9

Managed Complexity

RIC 2010

- Most essential functions are simple but have difficult licensing constraints.
- Some optional functions are complex but have no licensing constraints.

The Wall
The Blackboard
The CyberSecurity Bonus

10

Need for Flexibility

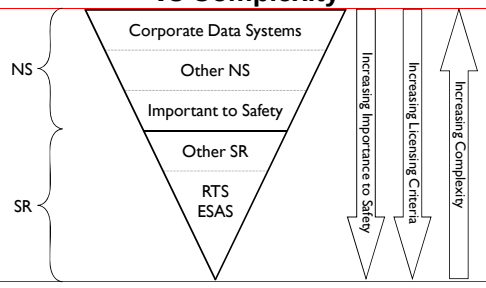
RIC 2010

	Protection Systems (SR)	*Mid-layer Systems (SR / NS)*	*Enterprise Systems (NS)*
Logic	Almost never changes	→	Highly flexible
Program	Almost never changes	→	Highly flexible
Settings	Change rarely	→	Highly flexible
Need for Outside Information	None	→	Extensive
Therefore:			
Need to modify	Minimal	→	Maximal
Reprogramming Facilities	Replace EPROM	Console	Network connection

11

Safety & Licensing vs Complexity

RIC 2010



12

CyberSecurity Considerations

RIC 2010

- 10CFR73.54 establishes cybersecurity requirements
- SECY-10-0153, Nov19, 2010 (ML10349034)
  - Clarifies NRC/FERC cybersecurity jurisdiction boundary
    - BOP items with "nexus to radiological health and safety" should be included within the scope of 73.54
    - Some items don't directly or indirectly affect reactivity or grid reliability
      - » therefore not directly subject to NRC nor FERC requirements
  - Items outside 73.54 could provide pathway to in-scope items
    - "extent of condition" review to evaluate potential precursors to issues impacting 73.54 systems

13

Communications & Independence

RIC 2010

- Independence among redundant functions – per CFR
- Independence among nonredundant functions
  - "Well-formed dependence" may be adequate
    (from *Software for Dependable Systems*, page 79)
- Need / reason for NS→SR communications
  - Must be *NO* safety need
  - Control of SR equipment from NS workstation
    - when there is no need for SR function
    - Special timing considerations when the intended *function* is SR

14

Simplicity Redux

RIC 2010

"Unfettered growth in {complexity}
… is incompatible with dependability."

-- Software for Dependable Systems: Sufficient Evidence?
National Research Council of the National Academies
The National Academies Press, 2007
Page 105

15