U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Evaluating Hazard Analysis Of A Distributed Digital System For Nuclear Reactor Safety

Sushil Birla
Division of Engineering
Office of Nuclear Regulatory Research

October 28, 2013

Outline

- **Hazard Analysis: What we mean**
  - Hazard as defined in standards
  - HA explained via IEEE Std 603 § 4-h
  - Many ways in which things can go wrong
  - HA place in safety analysis
- **Motivation & Scope**
  - Trends scenario 1/2
  - Trends scenario 2/2
  - Current State & Trends
  - Motivation for RIL-1101
  - Organizational & analytical framework
  - Role of RIL-1101 in review NRC process
  - RIL-1101 scope
  - Contributory hazard space in focus
  - RIL-1101: Relationship with Plant HA
- Research Method
- Envisioned Roadmap
- **Dependencies**
  - Types of dependencies: Examples
  - Dependency example: System architecture dimension
  - Product-process dependency over lifecycle
  - Dependency on a process activity
- **Evaluation of Hazard Analysis**
  - Factors affecting quality of HA
  - Reasoning Model
  - Techniques surveyed

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

Hazard: Definition(s)

- (IEC Vocab) Potential for harm
  - Condition. Circumstance. Scenario.
  - Scope boundary: System to be analyzed.
- (ISO/IEC/IEEE 24765 3.1283-1) An intrinsic property or condition that has the potential to cause harm or damage.
  - {Harm OR damage} = Loss

HA explained in terms of IEEE Std 603 criterion 4h

A specific basis shall be established
for the design of each safety system
of the nuclear power generating station;
the design basis shall document as a minimum …

the conditions having the potential for functional degradation of safety system performance

Hazards

and for which provisions shall be incorporated to retain the capability of performing the safety functions.

Hazard Controls

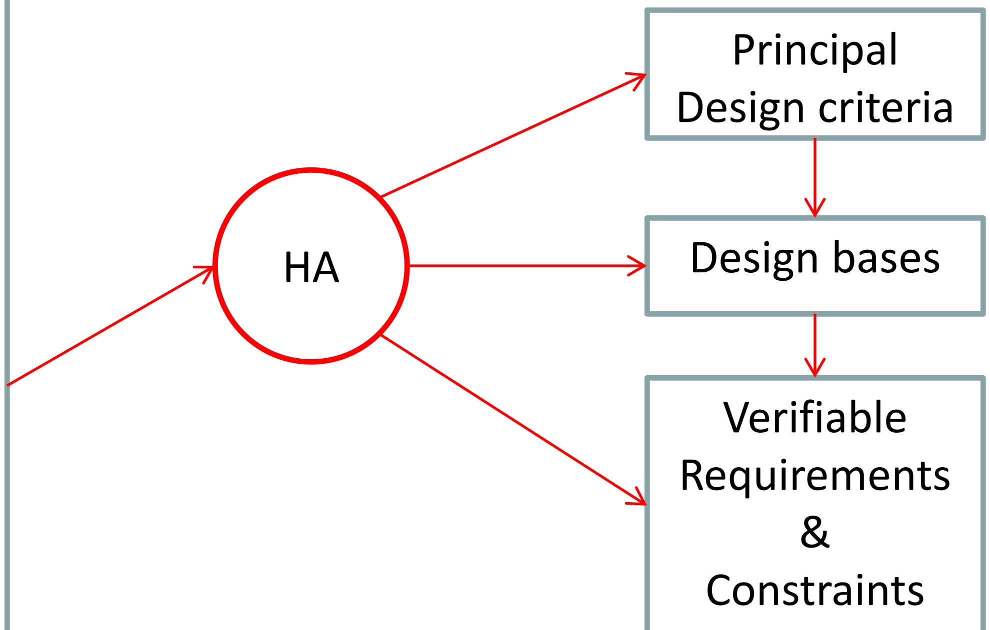
Many ways for things to go wrong

- Not provided, e.g.:
  - Data sent on bus is not delivered
- Provided when not needed
- Incorrect state transition
- Incorrect value provided, e.g.:
  - Invalid data
  - Stale input value treated inconsistently.
  - Undefined type of data
  - Incorrect message format
  - Incorrect initialization
- Provided at wrong time / out of order
- Provided for too long a duration (e.g., for continuous-control functions)
- Provided for too short ~, e.g.:
  - Signal is de-activated too early
- Intermittent instead of steady, e.g.:
  - Chatter or flutter
  - Pulse; spike
  - Impairment is erratic
- Interferes with another action, e.g.:
  - Deprives access to needed resource, e.g.
    - "Babbling idiot"
    - Locking up & not releasing resource
  - Corrupts needed information
- Byzantine behavior

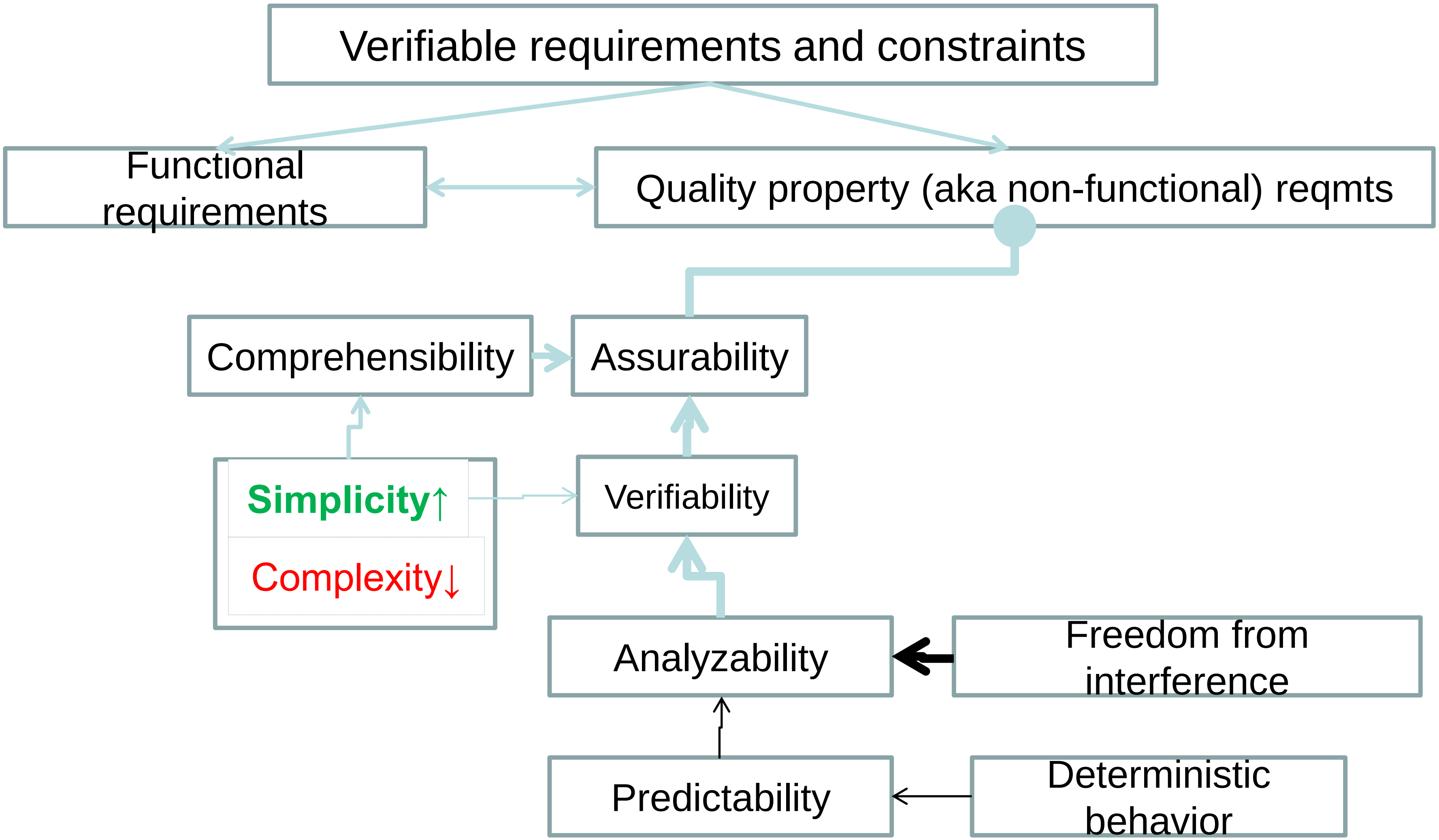
HA is Part of Safety Analysis

10 CFR 52.47(a), "…presents the design bases

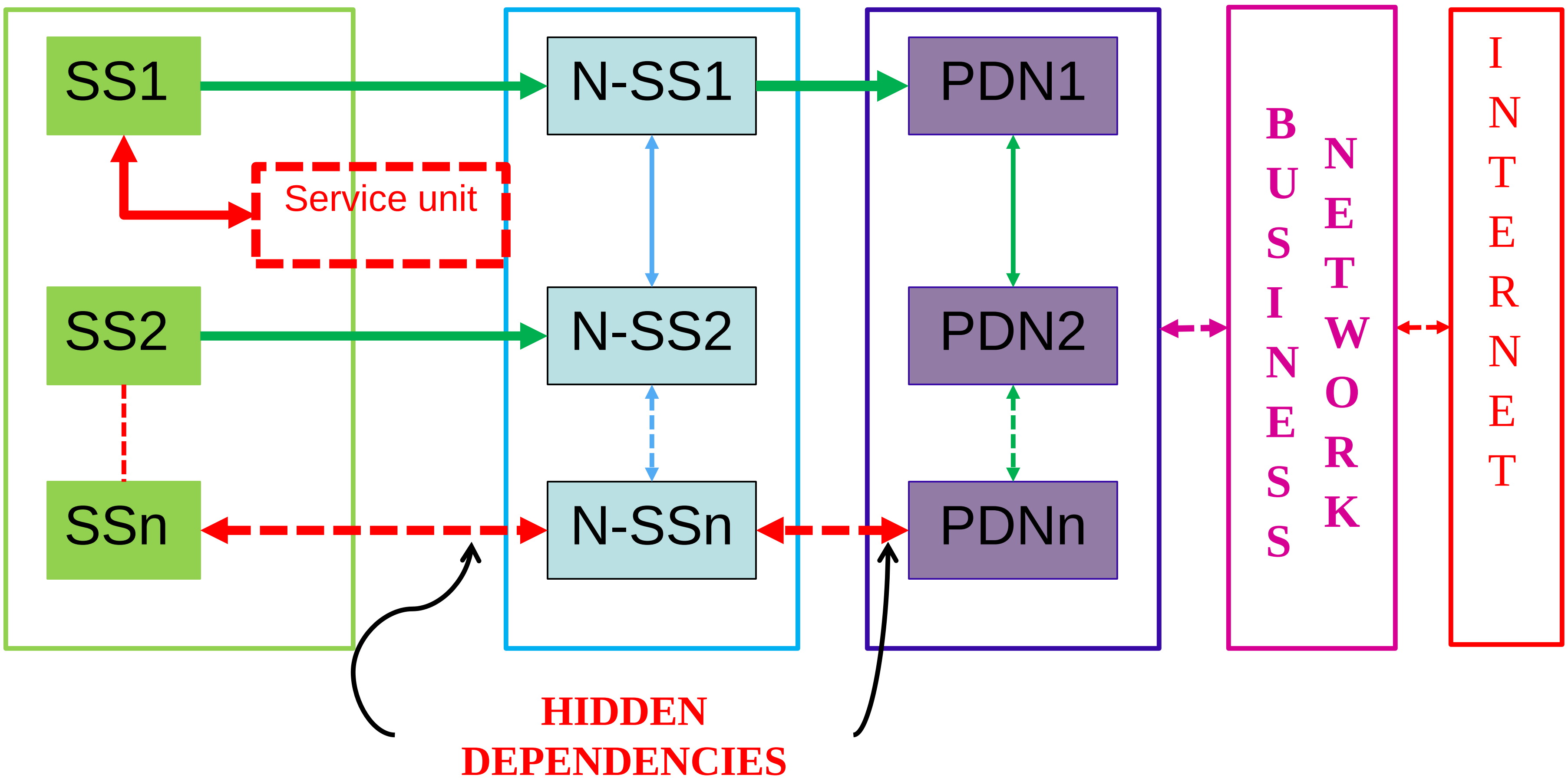
10 CFR 52.47(a)(2), "…analysis…performance requirements, the bases … the description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations …"



Derived requirements & constraints

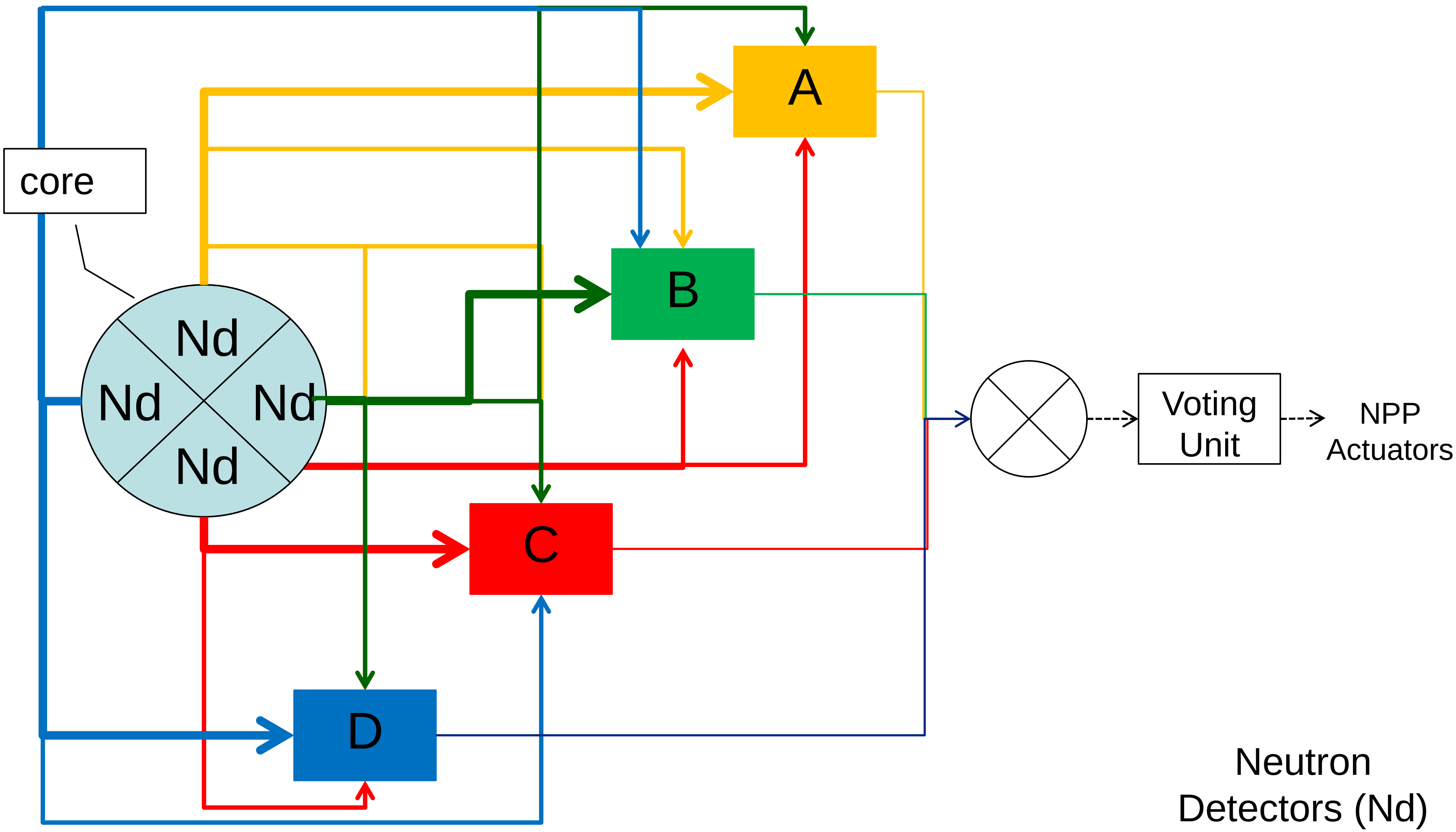


Trend Scenario 1/2: connections across different-grade elements



LEGEND Safety | Non-Safety | Plant Data | Business Data | Internet

Trend Scenario 2/2: connections across redundant divisions



Neutron Detectors (Nd)

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

Current State & Trends

Trends

Interconnections ↑
Feedback paths↑
→ Complexity ↑
→ Comprehensibility ↓
Verifiability ↓
Analyzability ↓
Deterministic behavior ↓

Side effects

Unwanted interactions↑
→ Hidden dependencies ↑
Independence ↓
Common cause ↑
Redundancy ↓
Diversity ↓
Defense in depth ↓
Safety margins ↓

Consequence

Traditional HA techniques (FTA; DFMEA) ineffective
[RIL-1001; RIL-1002; NUREG/IA-0254; EPRI]
↓
NRC's technical basis eroded

Motivation for RIL-1101

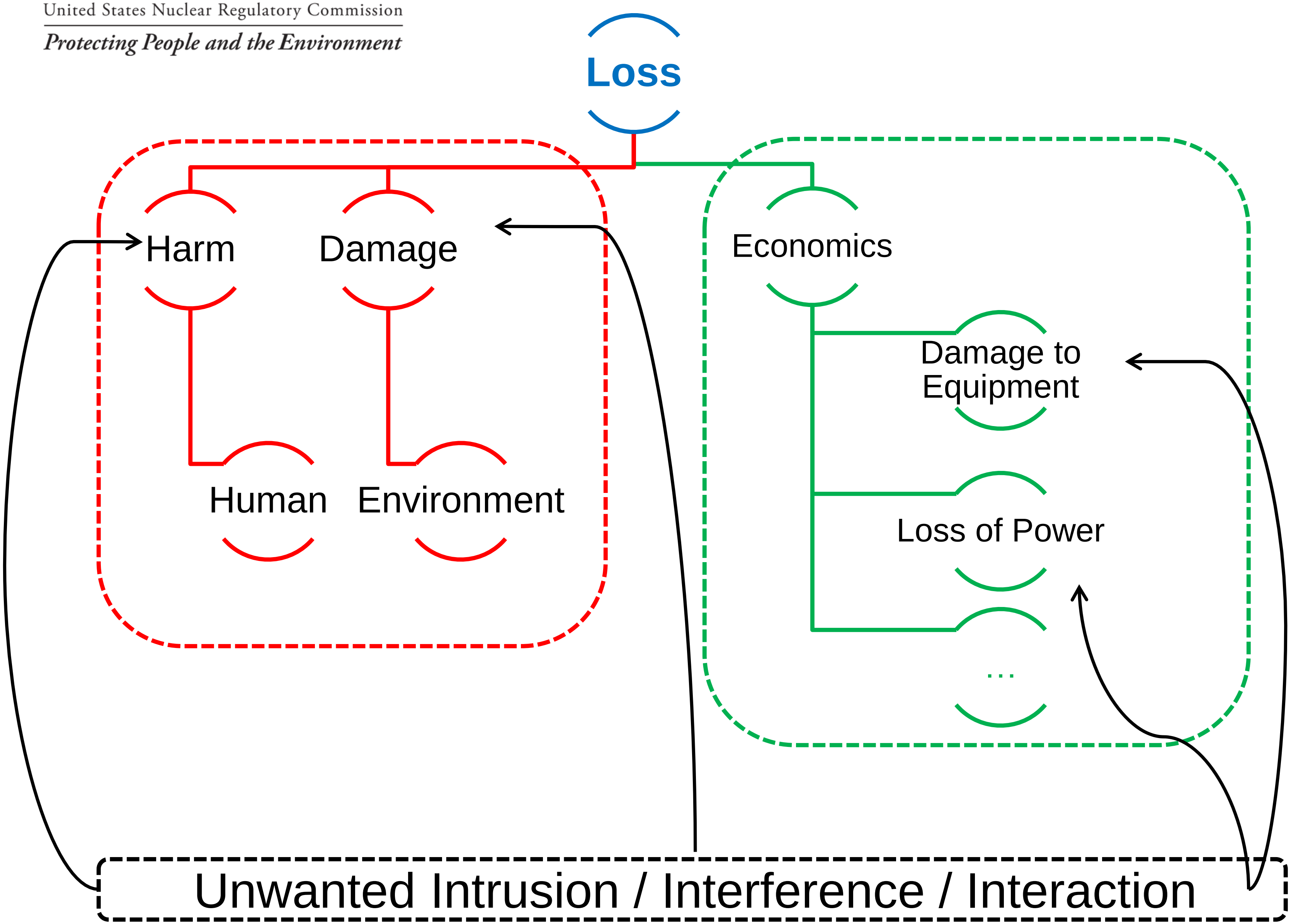
User need

Technical basis to review HA of a digital safety system
- Support mPower DSRS Chapter 7 Appendix A
- Support reviewer in judgment

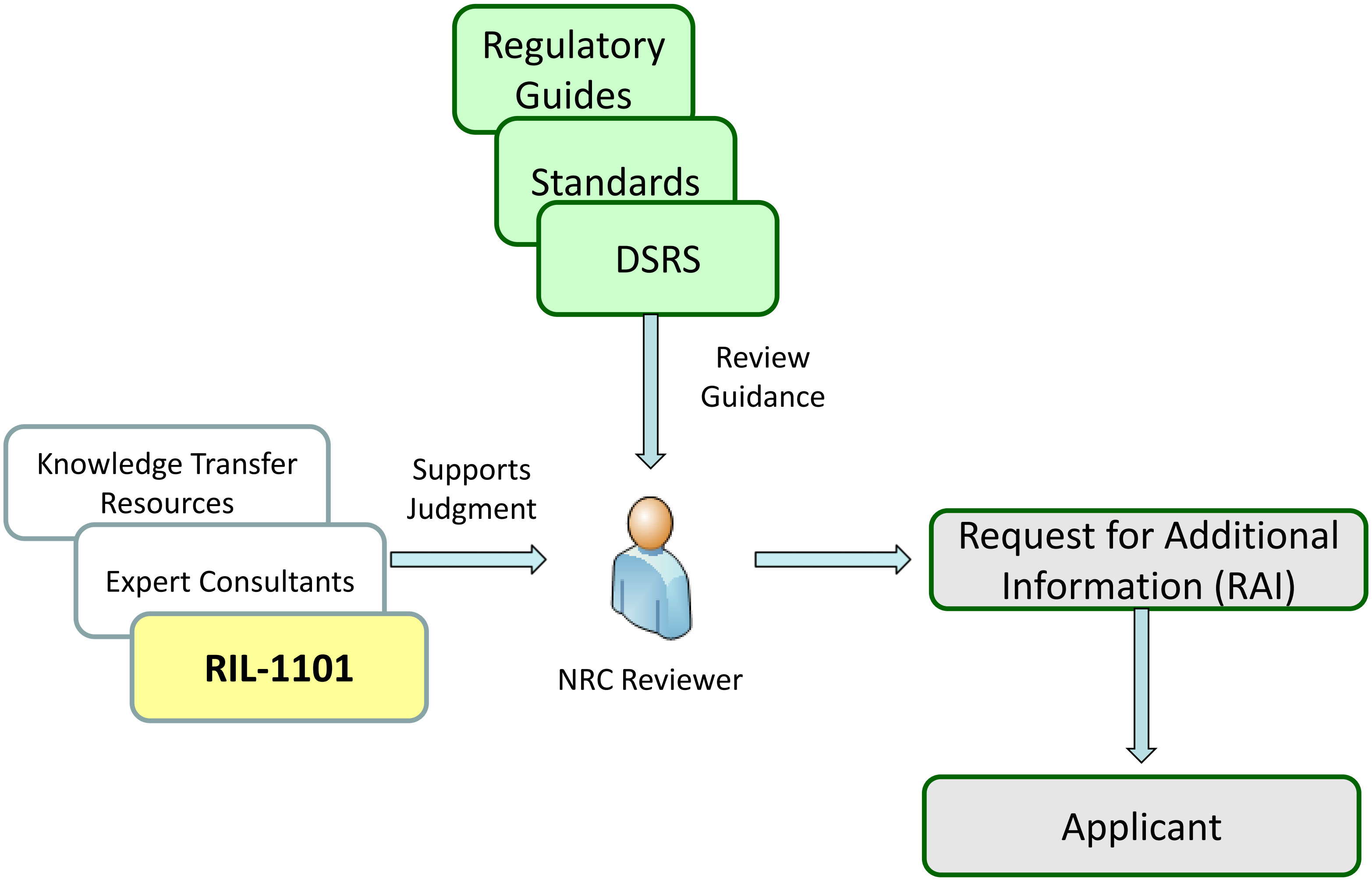
Value to others

- Organization & Analytical framework
- Technical reference

Organizational & Analytical Framework



Role of RIL-1101 in NRC Review Process



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

RIL-1101 Scope

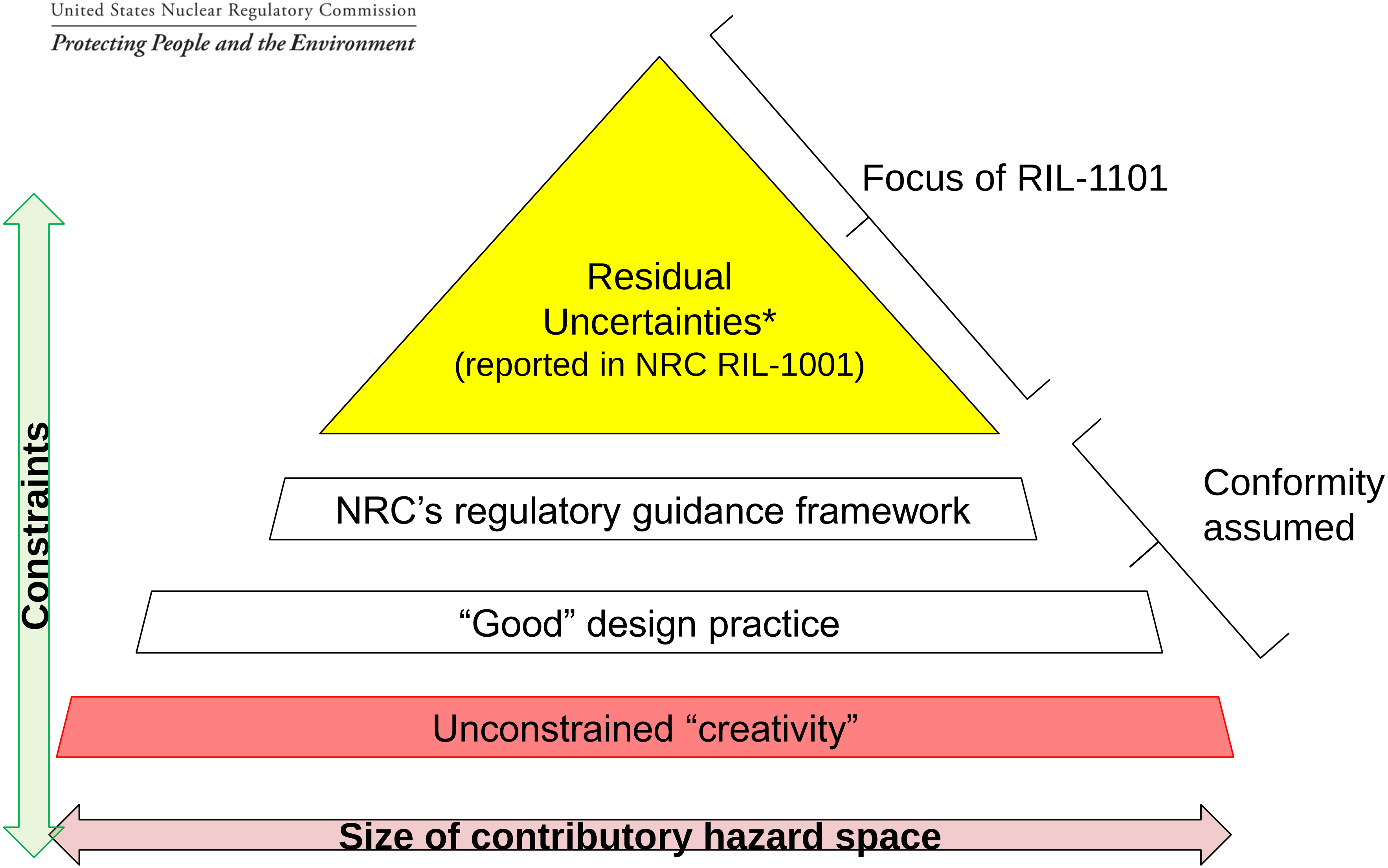
Includes

- Contributory hazards rooted in systemic causes through system development activities
- Focused on evaluation of HA (rather than performance of HA)
- Digital Safety System AND
  - Any system or element interfacing with or affecting digital safety system
  - Any correct timely performance of a safety function is dependent

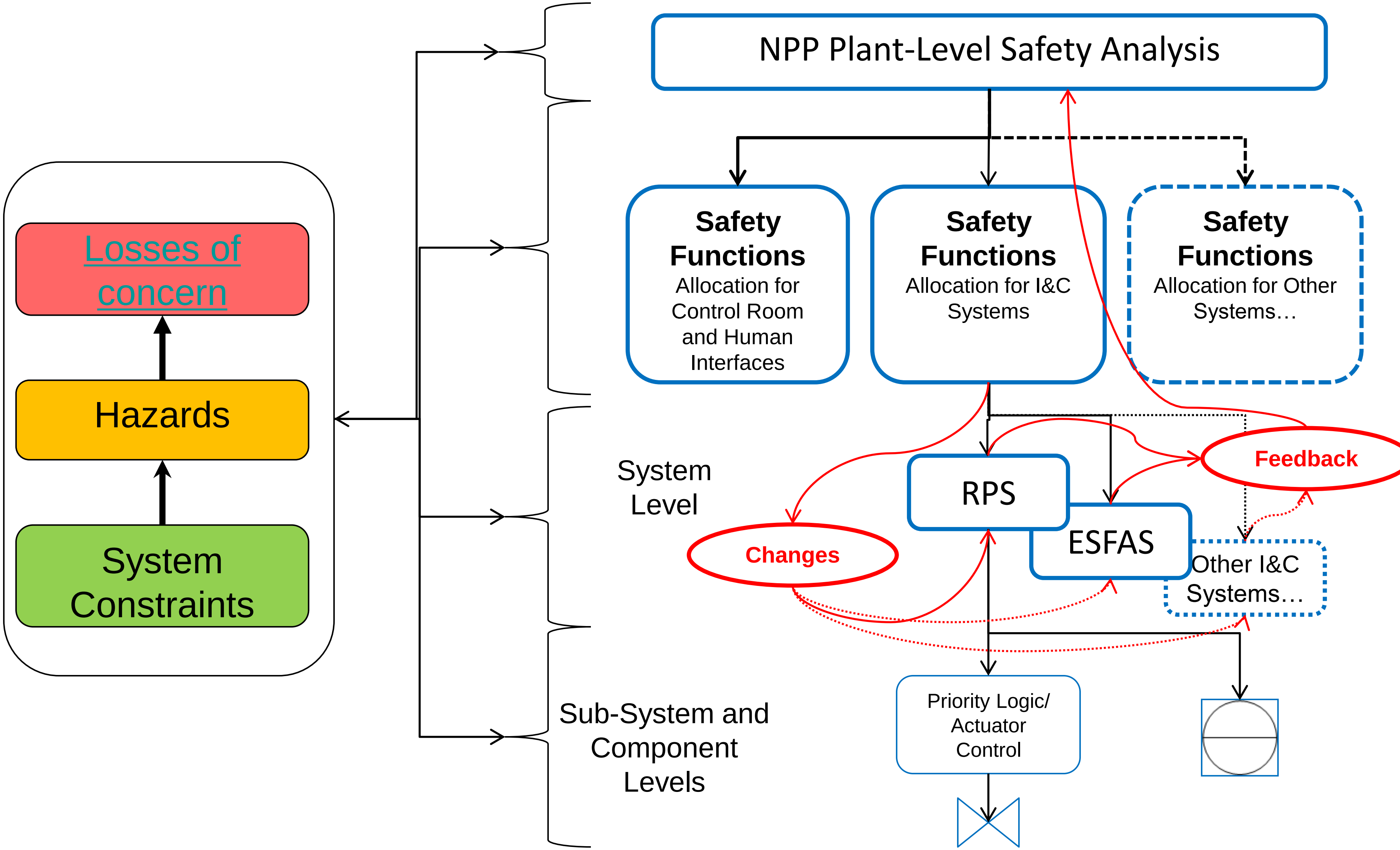
Excludes

- Risk Quantification

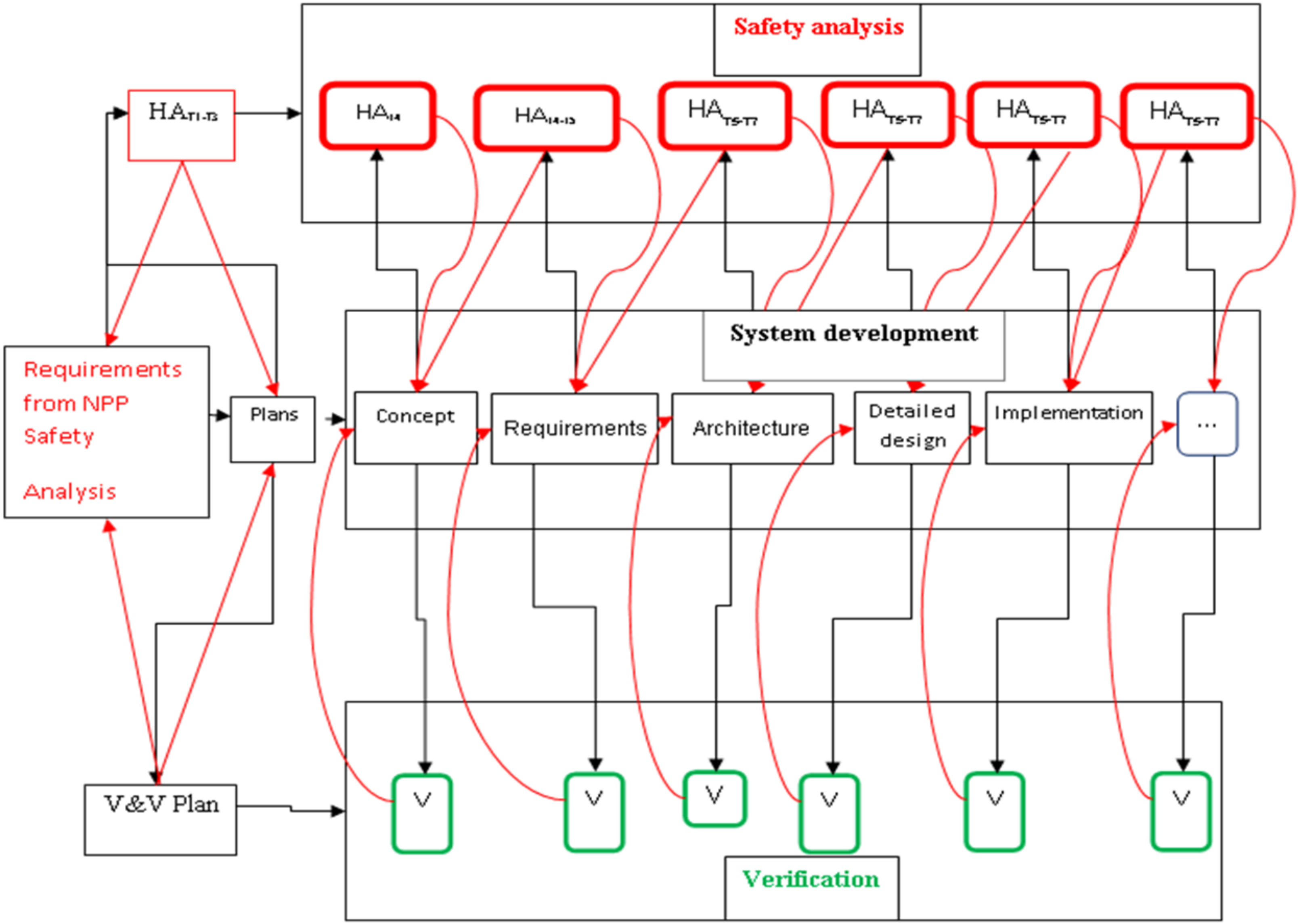
Contributory Hazard Space in Focus



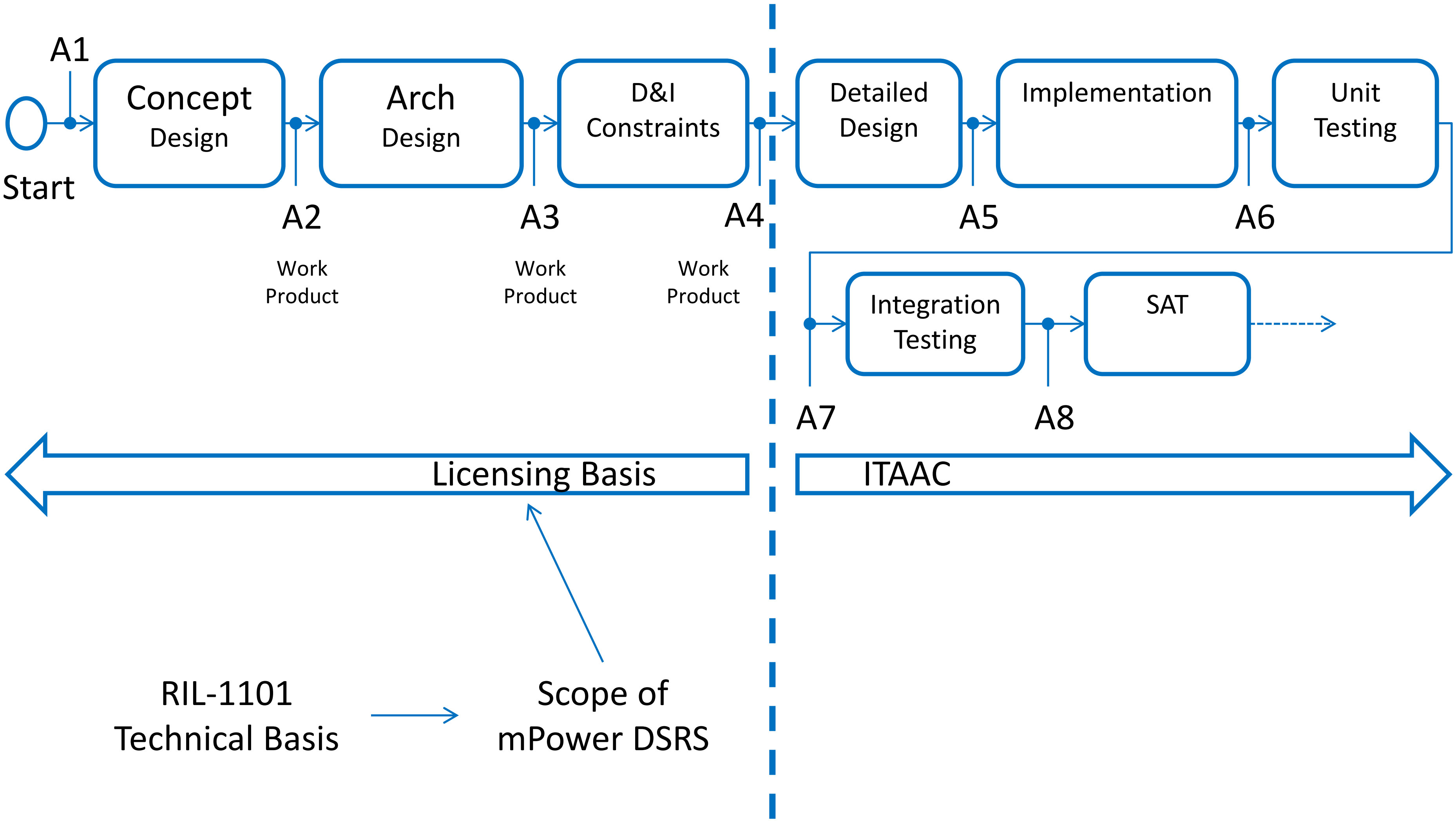
RIL-1101: Relationship with Plant HA



Product-Process Dependency Over Lifecycle



Focus: Licensing Basis for new reactors



HA Activities and Tasks – Reference Model (1/2)

<table>
<tr><th>HA Task</th><th>Input</th><th>Output</th></tr>
<tr><td>T1: Generate Baseline HA Plan</td><td rowspan="3">1. Concept
2. Requirements
3. Premises & Assumptions
4. Plat to validate assumptions
5. Consequences of behavior shortfall
6. Overall V&V Plan
7. Mainstream Development Plan
8. Corresponding information about or from entities in the dependency path</td><td>Baseline HA Plan

Dependencies of Plan</td></tr>
<tr><td>T2: Identify dependencies of HA plan</td><td>Evaluation report.
1. Deficiencies.
2. Changes needed.
3. Request for additional information (RAI).</td></tr>
<tr><td>T3 Evaluate other plans, following the dependencies identified above.
T3.1. Coordinate information exchanges with HA activities</td><td>Rejection or Acceptance

Revision to HA Plan, as needed</td></tr>
<tr><td>T4. Understand HA-relevant characteristics of the object to be analyzed</td><td>Items above +
9. Other requirements allocated to the object.
10 .Non-safety related constraints on the object.
11. Relationship with NPP-wide I&C architecture.
12. Distribution of responsibilities across organizational units/interfaces.
13. Provisions for information exchange across organizational units/interfaces.
14. Lifecycle models; processes; resources; information exchange interfaces.
15. Identification of reused objects and conditions of use.
16. Explicit record of dependencies.</td><td>1. Revision to HA plan.
2. Addition to hazard log
3. Change needed;
4. RAI</td></tr>
</table>

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

HA Activities and Tasks – Reference Model (2/2)

<table>
<tr><th>HA Task</th><th>Input</th><th>Output</th></tr>
<tr><td rowspan="5">T5. Analyze object for (contributory) hazards.</td><td rowspan="5">Items above +
Information specific to object of analysis</td><td>1. Addition to Hazard log</td></tr>
<tr><td>2. Changes Needed</td></tr>
<tr><td>3. Rejection / Acceptance</td></tr>
<tr><td>4. Revision to HA Plan</td></tr>
<tr><td>5. RAI</td></tr>
<tr><td>T6. Integrate analyses from lower levels in the integration hierarchy and contribution paths up to the top-level analysis.</td><td>Items above + information needed about inter-object dependencies for overall system HA</td><td>As in T5.</td></tr>
<tr><td>T7. Analyze change proposal (e.g., hazard control proposal).</td><td>Change proposal, including information on which it depends (e.g, items listed above).</td><td>As in T5.</td></tr>
</table>

HA tasks in object development lifecycle

ID	Description
T1	Generate Baseline HA Plan
T2	Identify dependencies of HA plan
T3	Evaluate other plans on which HA plan depends. Co-ordinate information exchanges.
T4	**Understand HA-relevant characteristics of the object to be analyzed**
T5	Analyze object for hazards ← contributors / causes
T6	Integrate analyses from lower levels in the integration hierarchy and contribution paths up to the top-level analysis
T7	Analyze change proposal (e.g., for hazard control).

HA planning tasks (T1 – T3)

Inputs

1. Concept
2. Requirements
3. Premises & Assumptions
4. Plan to validate assumptions
5. Consequences of behavior shortfall
6. Overall V&V Plan
7. Mainstream Development Plan
8. Corresponding information (items 1-7) about or from other objects in the dependency path

Outputs

Baseline HA Plan

Dependencies of Plan

Evaluation report.
1. Deficiencies.
2. Changes needed.
3. Request for additional information (RAI).

Rejection or Acceptance

Revision to HA Plan, as needed

HA task T4: Understand HA-relevant characteristics of the object to be analyzed

Inputs

1. Input items identified for tasks T1-T3
2. Other requirements allocated to the object
3. Non-safety related constraints on the object.
4. Relationship with NPP-wide I&C architecture.
5. Distribution of responsibilities across organizational units.
6. Provisions for information exchange across them.
7. Lifecycle models; processes; resources; information exchange interfaces.
8. Identification of reused objects; Their conditions of use.
9. Explicit record of dependencies.
10. Prior HA results, if any

Outputs

Revision to HA Plan

Addition to hazard log

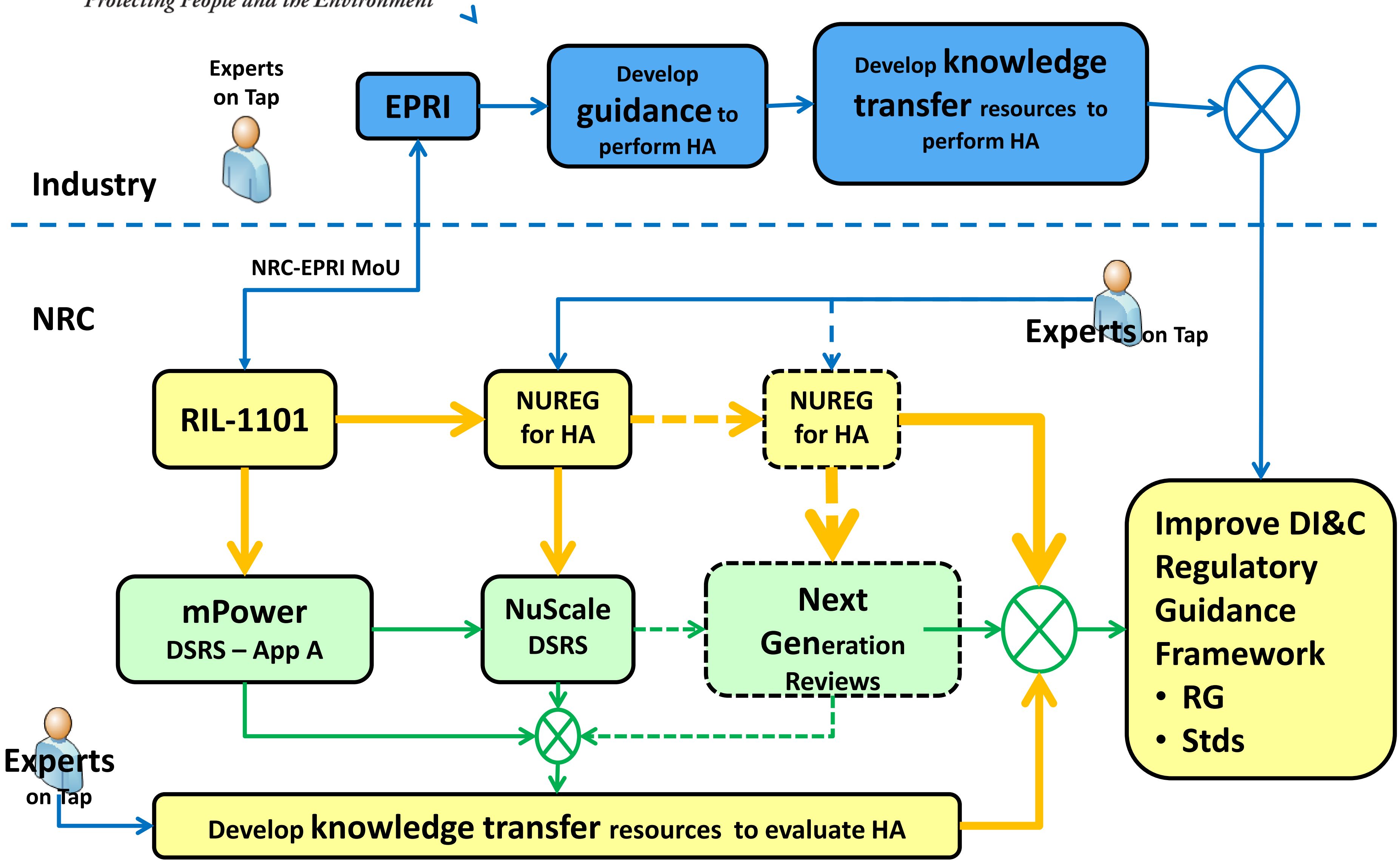
Change needed;

RAI

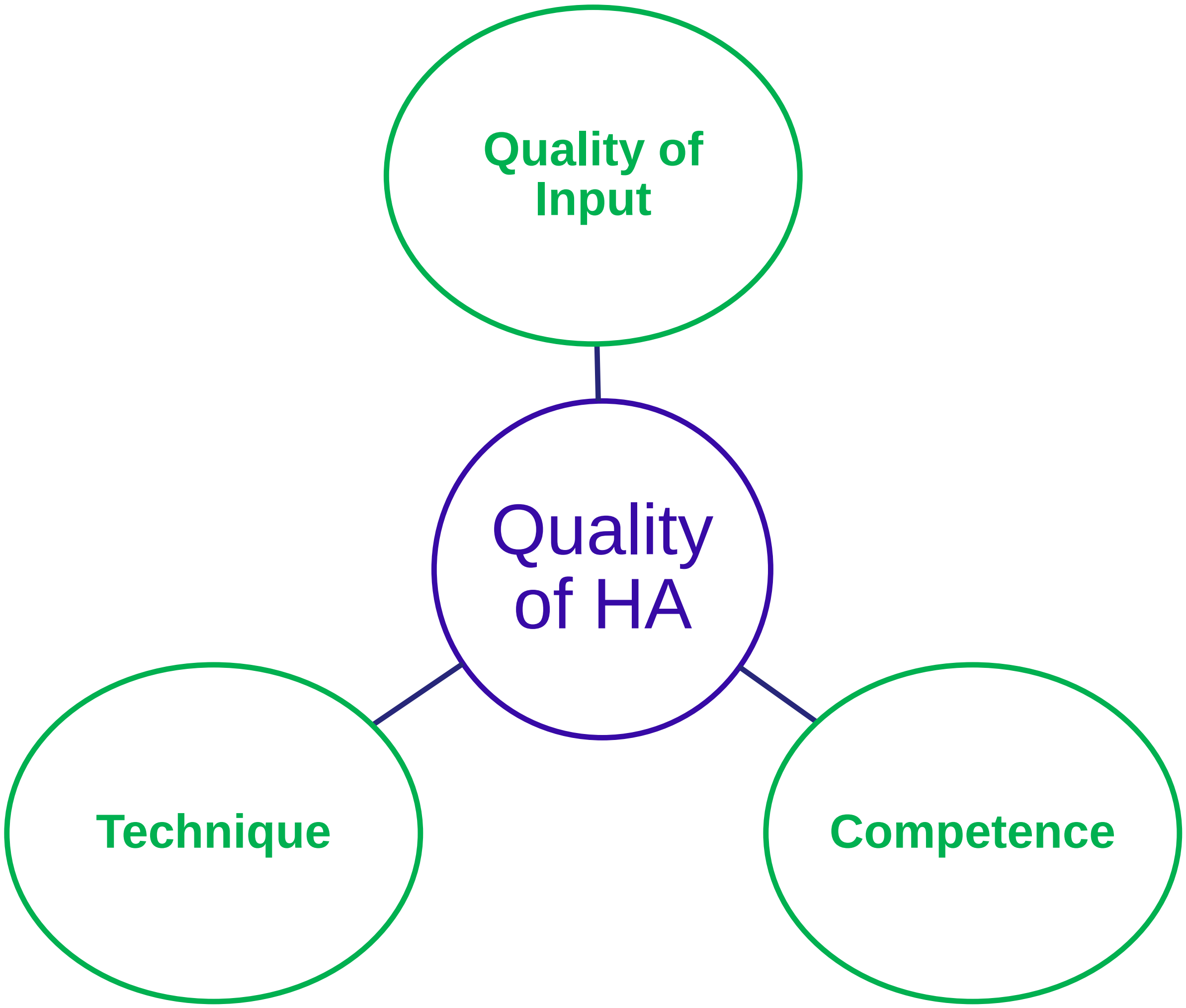
Our research: Organize existing knowledge

- Knowledge available in technical literature
  - Over 150 public / non-public articles / reports {journals, conferences, technical meetings, and technical orgs}.
- Knowledge acquired from respective experts
  - Comments unresolved in RIL-1101 → Candidates for future work

Envisioned HA R&D Roadmap



Factors Affecting Quality of HA



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Some Surveyed HA Techniques (1/2)

HA Technique	Salient Feature
Hazard and operability studies (HAZOP)	• Concept of using teamwork, aided by HAZOP process expert. • Systematizing enquiry through key words. • Systematizing understanding effects through understanding the associated deviations.
Fault Tree Analysis (FTA)	Representation and understanding of fault propagation paths, when the paths are branches of a tree.
Design Failure Mode and Effects Analysis D-FMEA	Representation of faulted behavior of a hardware component for understanding its effect, without requiring knowledge of its internals.
Functional Failure Mode and Effects Analysis	• Understanding effect of unwanted behavior of a function of the system, without requiring knowledge of its internals. • Useful in concept phase.
Cause Consequence Analysis	Concept of using causality model to understand fault propagation paths.
Hazard Analysis & Critical Control Points	Concept of focusing on critical process variables that affect the outcome.
Software hazard analysis and resolution	Adaptation of HAZOP to software, through customization of the key words.

Some Surveyed HA Techniques (2/2)

HA Technique	Salient Feature
Fault propagation and transformation network/calculus FPTC	Representation and analysis of fault propagation, when the faults are transformed during propagation, and when there are feedback paths, supporting mechanized traversal and reasoning.
Dynamic Flowgraph Method DFM	Behavior modeling of the system in the finite state machine paradigm facilitates or enables: • Mathematical underpinning. • Analysis of its interactions with environment. • Analysis of dynamic behavior across its elements. • Mechanized traversal. • Mechanized reasoning, esp. if directed cyclic graph.
System-Theoretic Process Approach STPA	• Applicable at concept phase (without a finished design). • Applicable to understanding of organization-culture systems.

Quality-levels of Input in Phase Work Products (1/3)

ID	Work Product of Lifecycle Phase	Common Practice	State of the Practice	State of the Art
1	Requirements from next higher level of integration, e.g. from NPP-level safety analysis	Textual narrative. No configuration-controlled vocabulary. "Flat list" organization (i.e., no explicit relationship across requirements is identified).	Restricted natural language with defined vocabulary and structure across elements of a statement.	Use case scenarios
			SpecTRM-RL	Framework for specification & analysis
			Requirements engineering support in Naval Research Labs (NRL). Tables (Darlington) 4-variable Models to support mechanized reasoning.	
2	Plans {Safety plan; V&V plan; HA plan}	Low level of detail; relatively late in the lifecycle.	V&V plan Safety plan	Integrated safety and security plan.

Quality-levels of Input in Phase Work Products (2/3)

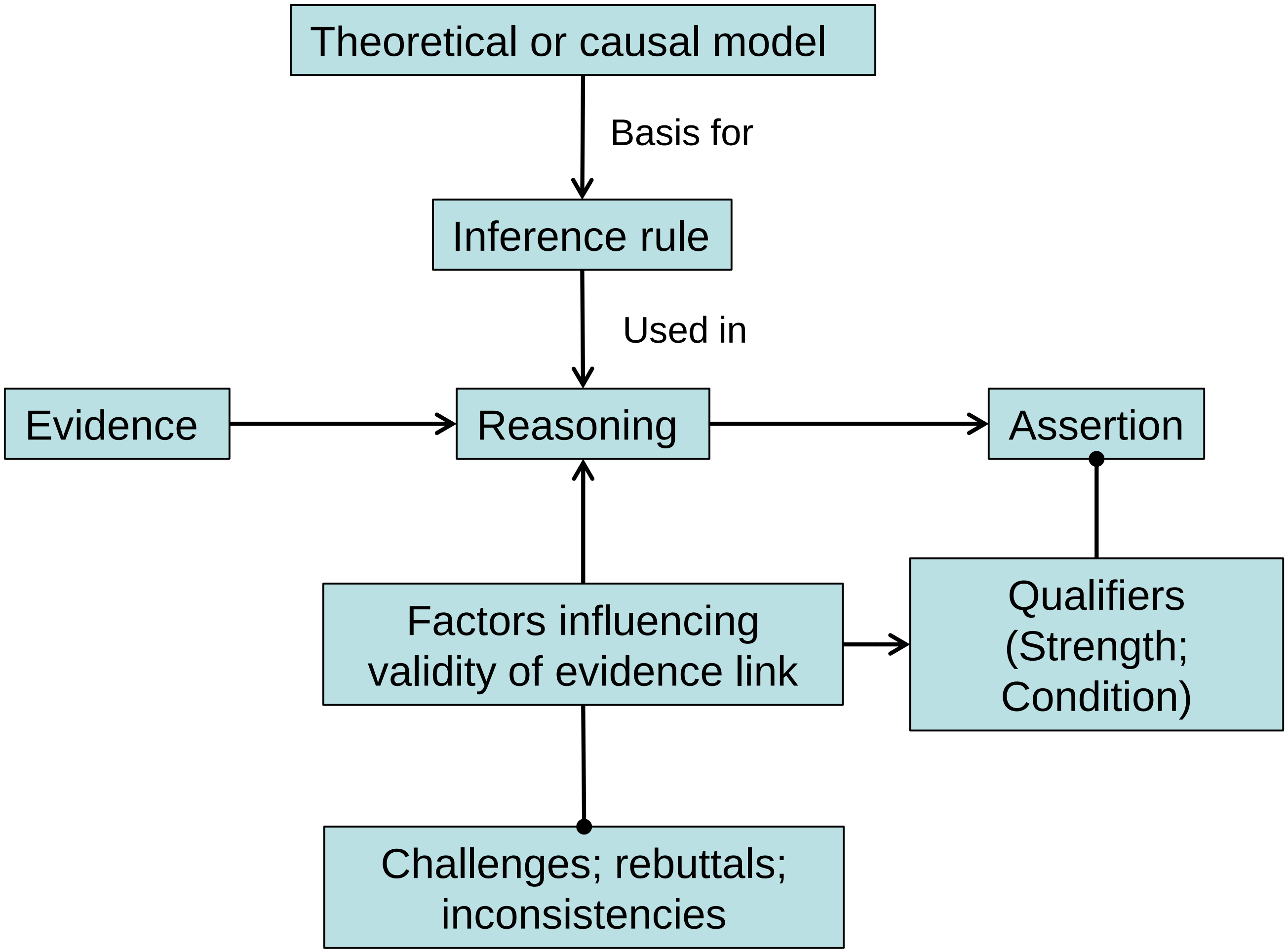
ID	Work Product of Lifecycle Phase	Common Practice	State of the Practice	State of the Art
3	Concept	Combination of (a) block diagram without semantics on the symbols and (b) textual narrative	Models to support mechanized reasoning. SysML. AADL - Extensions	META
4	REQuirements of digital system	See row 1	See row 1	See row 1
5	ARCHitecture of digital system	See row 3	See row 3	META
6	Requirements for software	See row 1		See row 1
7	Architecture for software	See row 3	See row 3. MASCOT AADL	META

United States Nuclear Regulatory Commission
Protecting People and the Environment

Quality-levels of Input in Phase Work Products (3/3)

Row ID	Work Product of Lifecycle Phase	Common Practice	State of the Practice	State of the Art
8	Detailed design of software	For application logic: Function block diagram. For platform software: Combination of (a) block diagram without semantics on the symbols and (b) textual narrative.	SPARK	META Refinement from architectural specifications
9	Implementation of software (code)	For platform software, including communication protocols: C programming language + processor-specific assembler language	Concept of using safe subset of an implementation language: MISRA C Language for programming FPGAs	Auto-generation from detailed design.

Reasoning Model



Some ongoing work; issues

- Catalog(s) of contributors?
- HA example for FPGA environment.
- Competence.
- “Quality of Safety” Requirements.
- Refinement. “Integrate-then-build.”
- Composition. Compositionality.
- Completeness issue … (open-ended) …

Collaborative R&D Potential

- NRC's "long term" research projects (LTRP)
  - Extent of automation support for efficiency?
    - Automation support in HA activities?
    - Automation support in specification of logic
    - Automated code generation
    - Automated proof generation
- USA-Canada collaboration
- OECD/NEA: Broader international collaboration
- Learning from operating experience

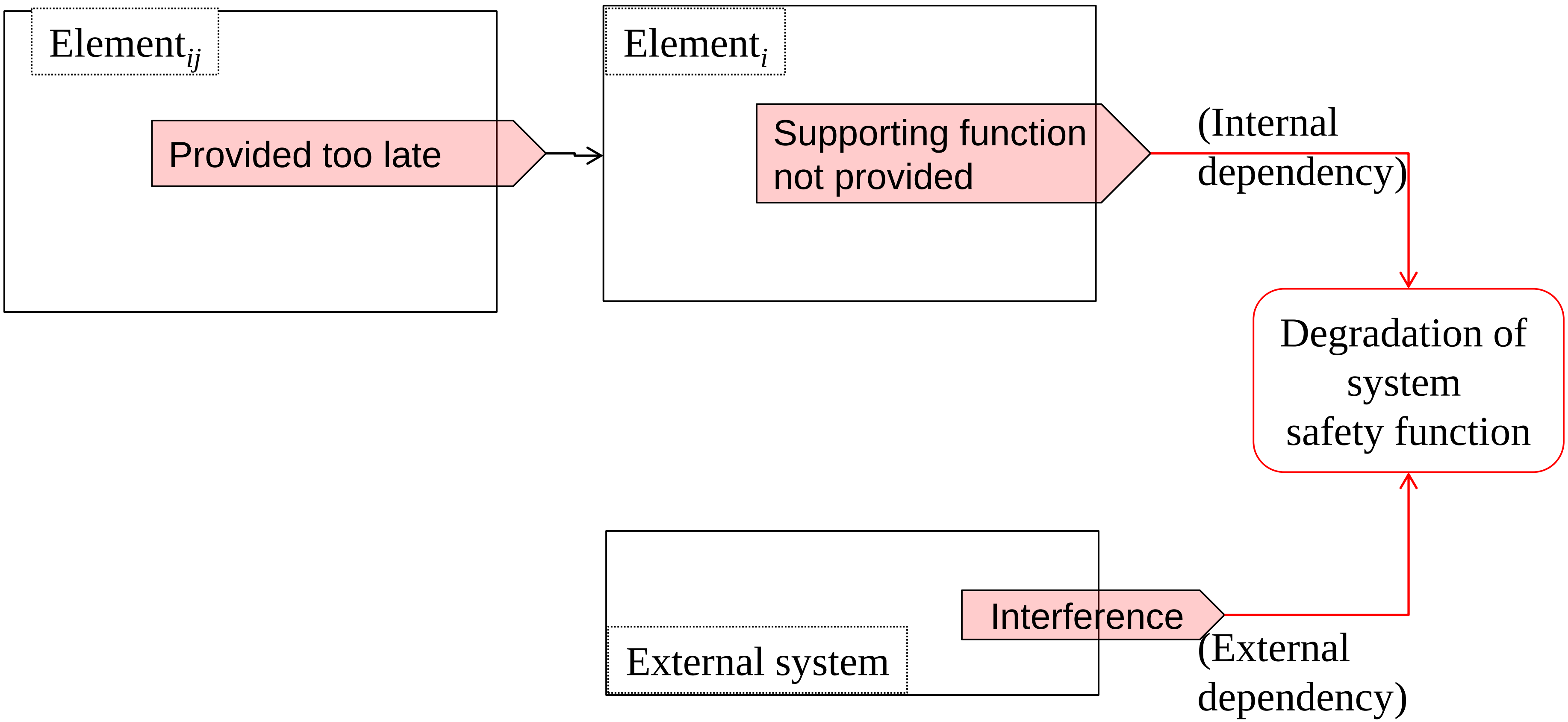
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Back-up slides

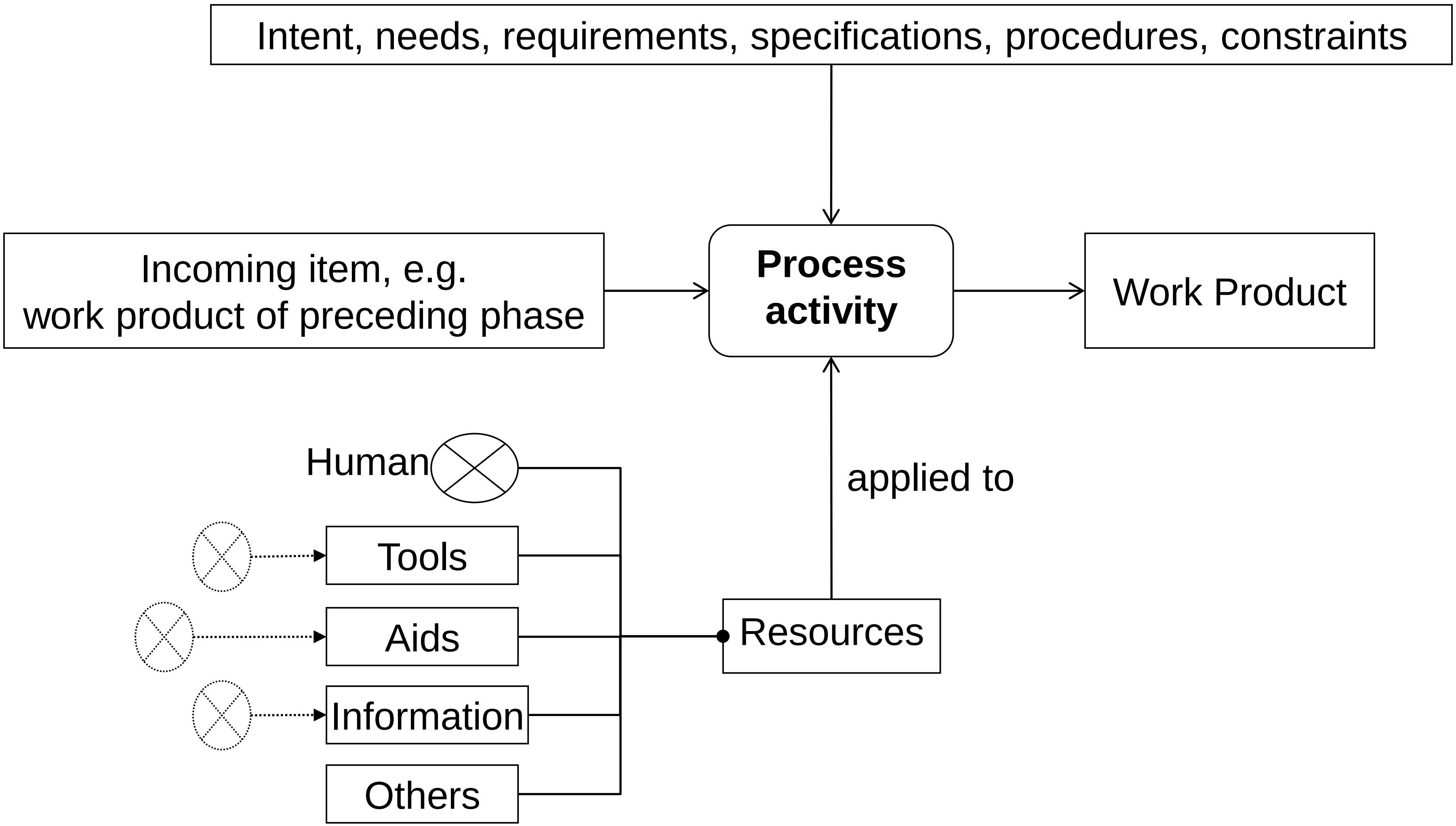
Types of Dependencies: Examples

- Function
- Control flow
- Data; information
- Resource sharing or constraint
- Conflicting goals or losses of concern
- States or conditions in the environment
  - Controlled processes
  - Supporting physical processes
- Concept
- Some unintended, unrecognized form of coupling.

Functional dependency Example: System Architecture Dimension



Dependency on a Process Activity



Acronyms

- **ACRS** Advisory Committee for Reactors and Safeguards
- **CFR** Code of Federal Regulations
- **DI&C** Digital Instrumentation and Control
- **DSRS** Design Specific Review Standard
- **ESFAS** Engineered Safety Features Actuation System
- **EPRI** Electrical Power Research Institute
- **HA** Hazard Analysis
- **I&C** Instrumentation and Control
- **I/O** Input/Output
- **INPO** Institute of Nuclear Power Operations
- **ITAAC** Inspections, Tests, Analyses, and Acceptance Criteria
- **NPP** Nuclear Power Plant
- **NRC** Nuclear Regulatory Commission
- **NRO** NRC Office of New Reactors
- **PWR** Pressurized Water Reactor
- **R&D** Research and Development
- **RAI** Request for Additional Information
- **RES** NRC Office of Nuclear Regulatory Research
- **RG:** Regulatory Guides
- **RIL** Research Information Letter
- **RPS** Reactor Protection System
- **SAR** Safety Analysis Report
- **SMR** Small Modular Reactor
- **SRP** Standard Review Plan
- **V&V** Verification and Validation