Digital systems research

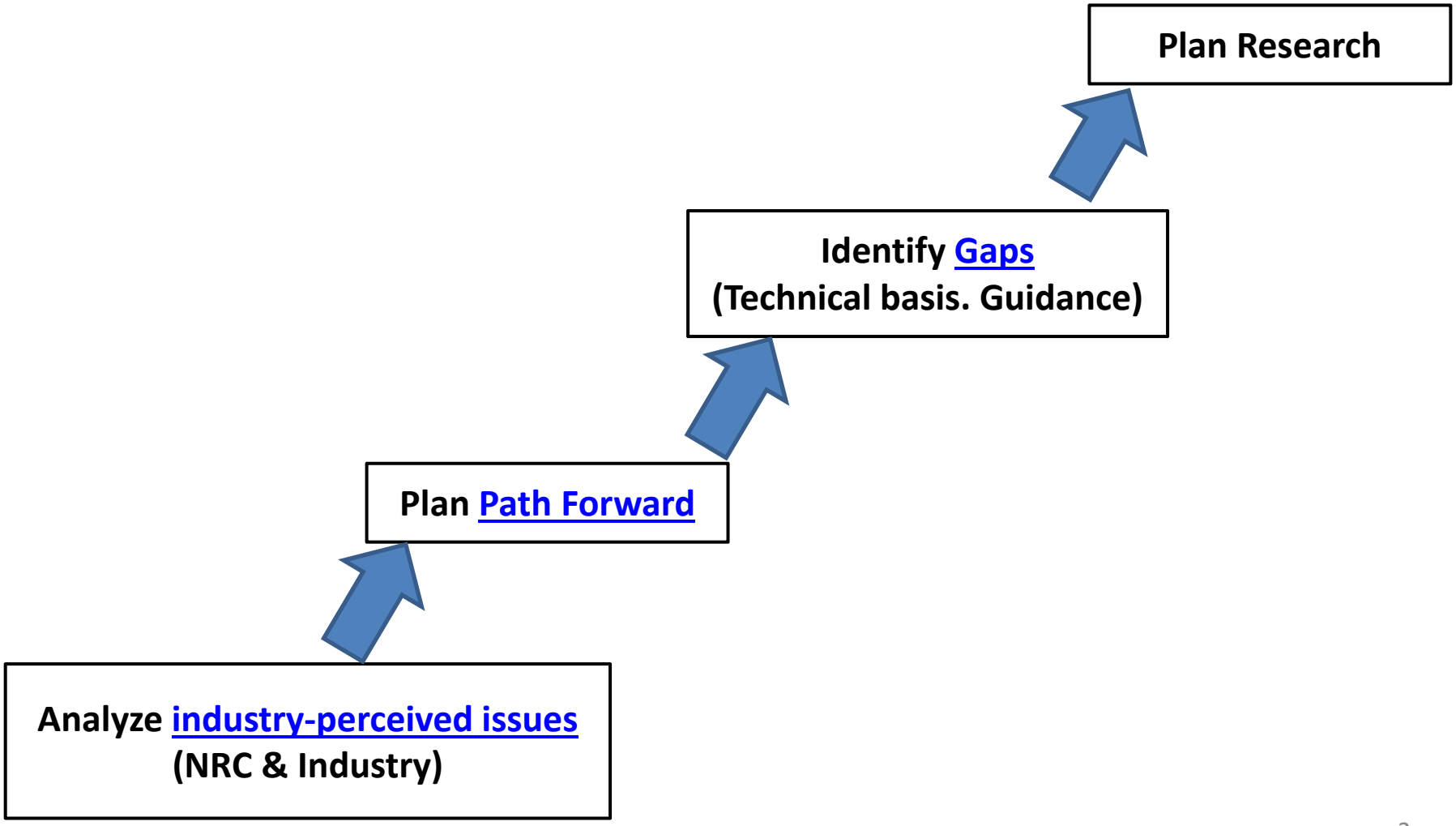
From Issues to Research needs

Sushil Birla
Senior Technical Advisor, NRC/RES/DE

Enlarged Halden Program Group, May, 2016

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

Industry-perceived issues → NRC Path Forward: Gaps → Research



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

Industry-perceived issues

ID	Industry-perceived issue
CCF	Common Cause Failure
FAT	Factory Acceptance Testing
CGD	Commercial Grade Dedication
HFE	Human Factors Engineering
HCU	High Cost and Unpredictability

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

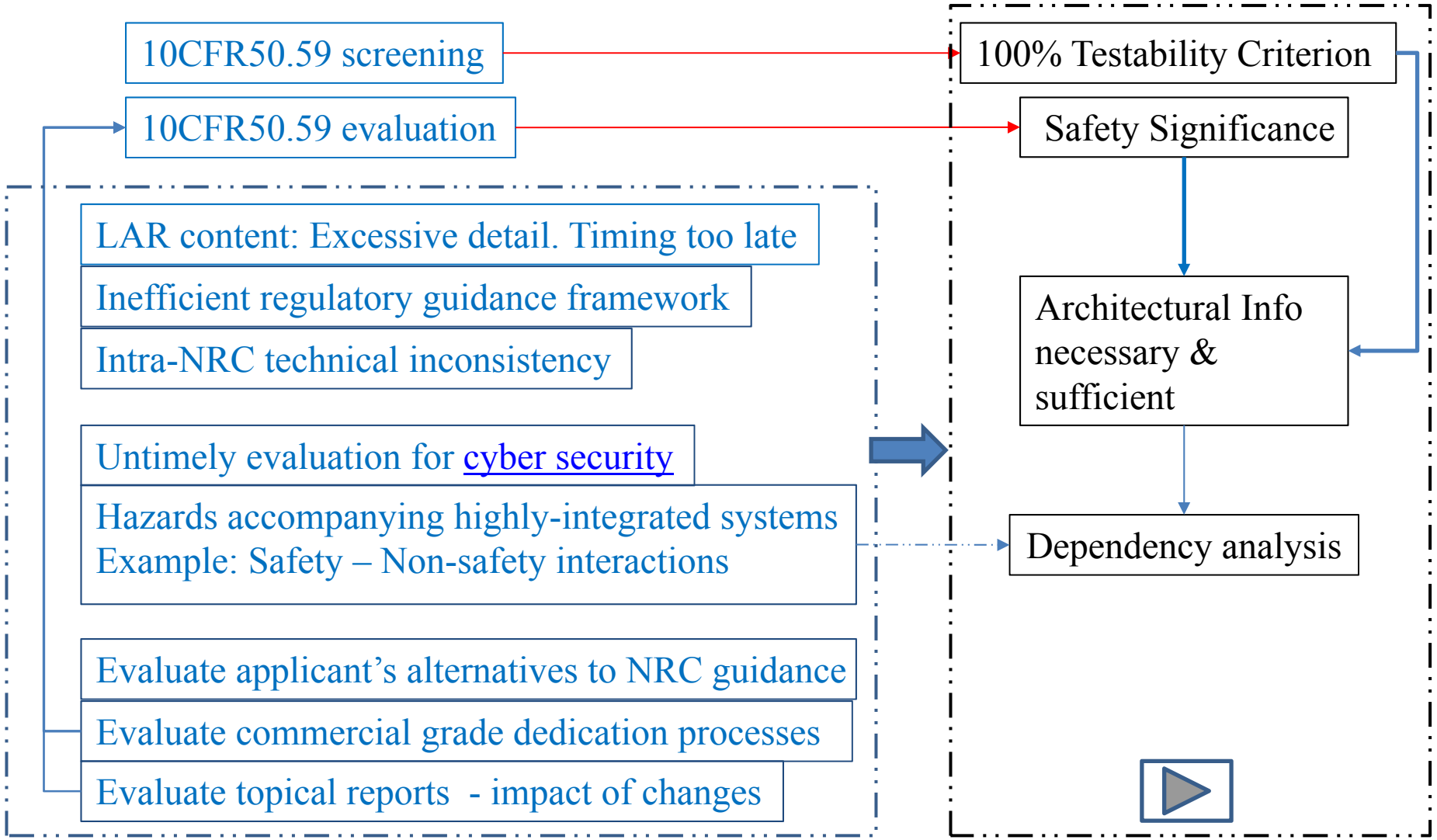
Prioritized Problem Statements from DI&C Path Forward Action Plan

ID	Title
I-1	Staff Assistance in Updating Industry Guidance for DI&C 10 CFR 50.59 Modifications
I-2	Content and Schedule of DI&C Application Submittals
I-3	Evaluation of NRC Policy on Software CCF
I-4	Guidance for Evaluation of Proposed Alternatives to Regulatory Guides and Endorsed Standards
II-1	Guidance for Evaluation of Highly-Integrated Digital Technology
II-2	Regulatory Infrastructure Improvements
II-3	Improvement in DI&C Technical Consistency Among NRC Headquarters and Regional Offices
II-4	Early-Development Stage Evaluation of Security Aspects of Proposed DI&C Designs
II-5	DI&C Topical Report Evaluation and Update Process

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

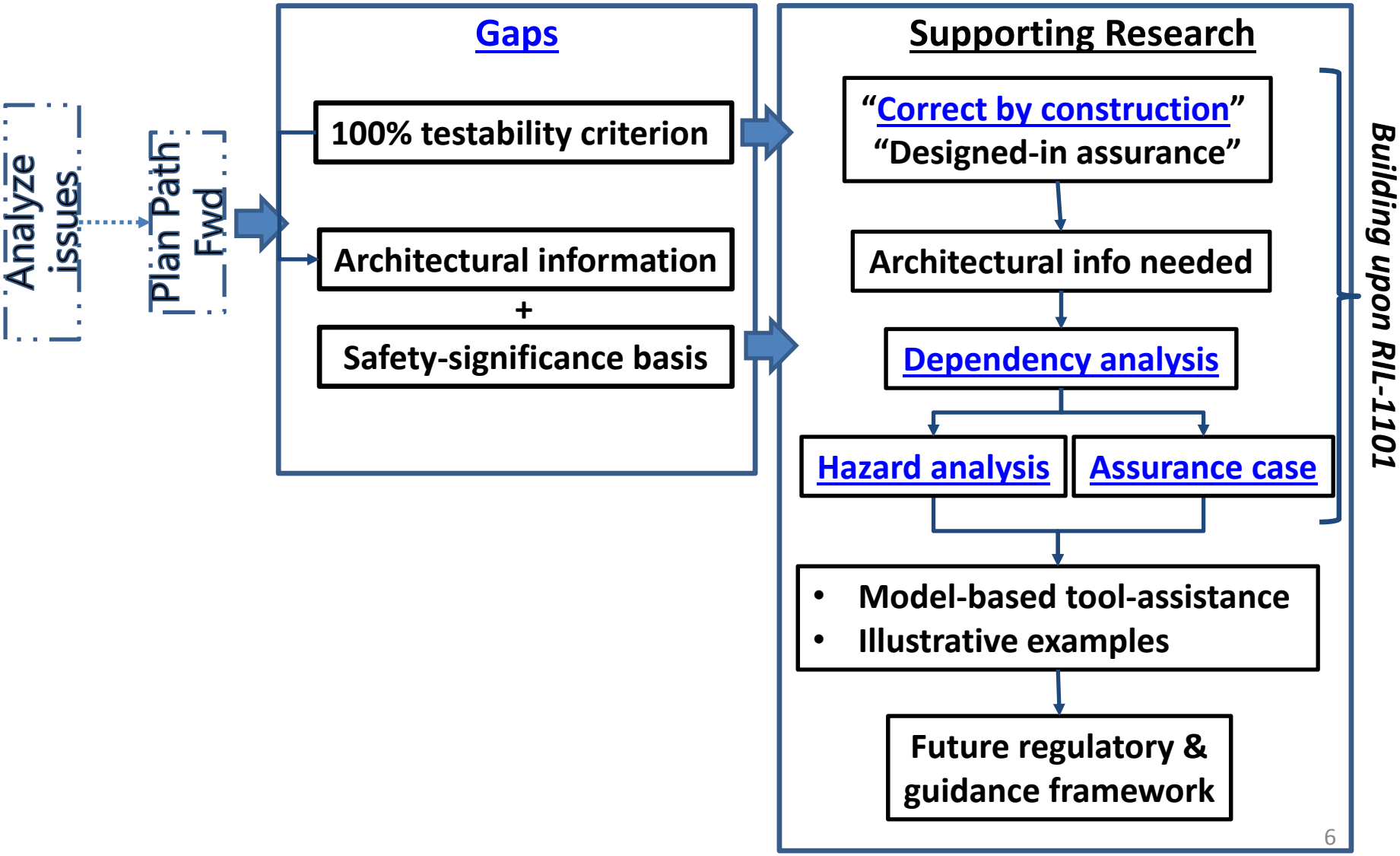
Technical basis gaps

mapping from NRC path forward problem statements



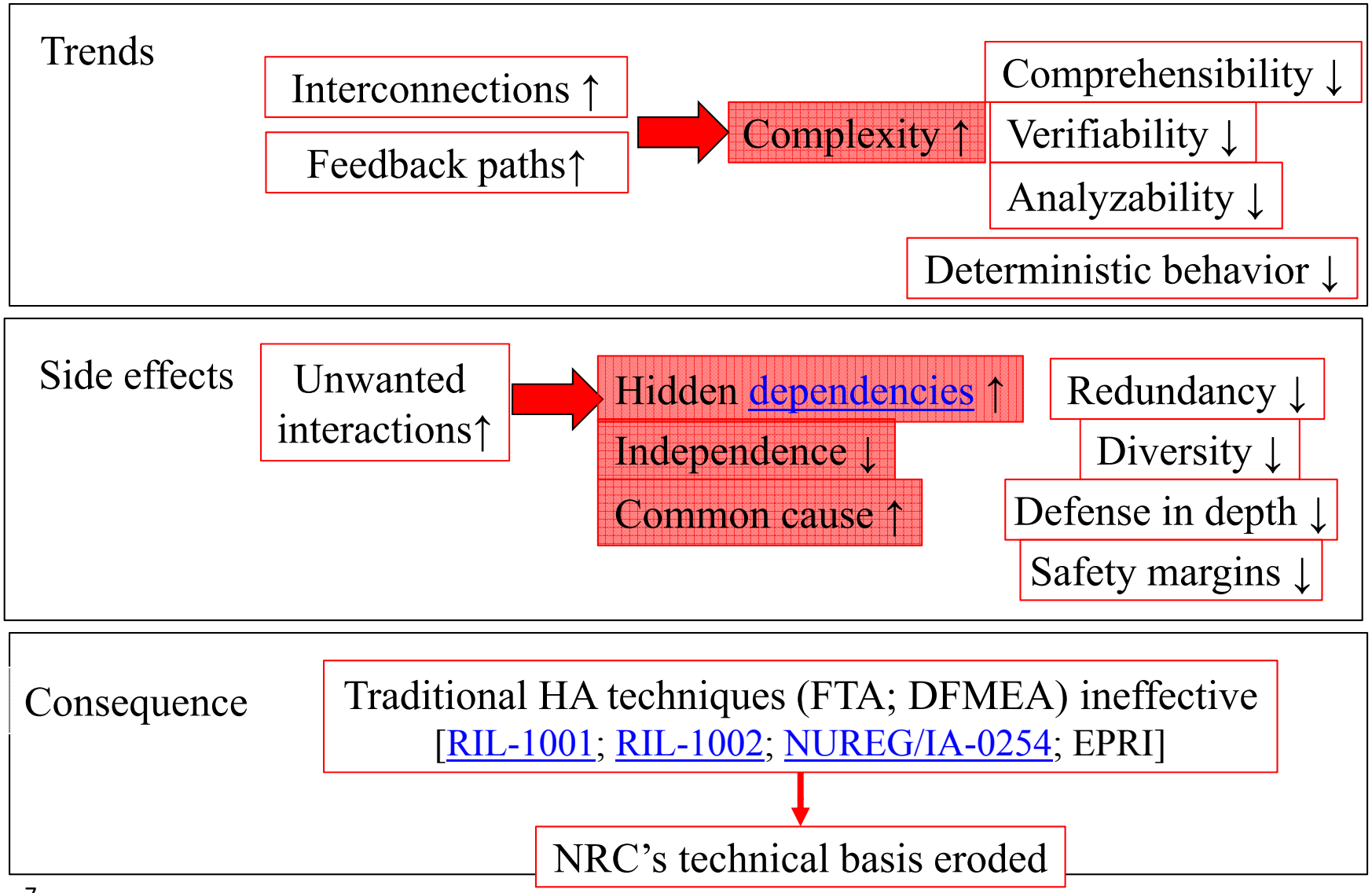
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Gaps → Research directions



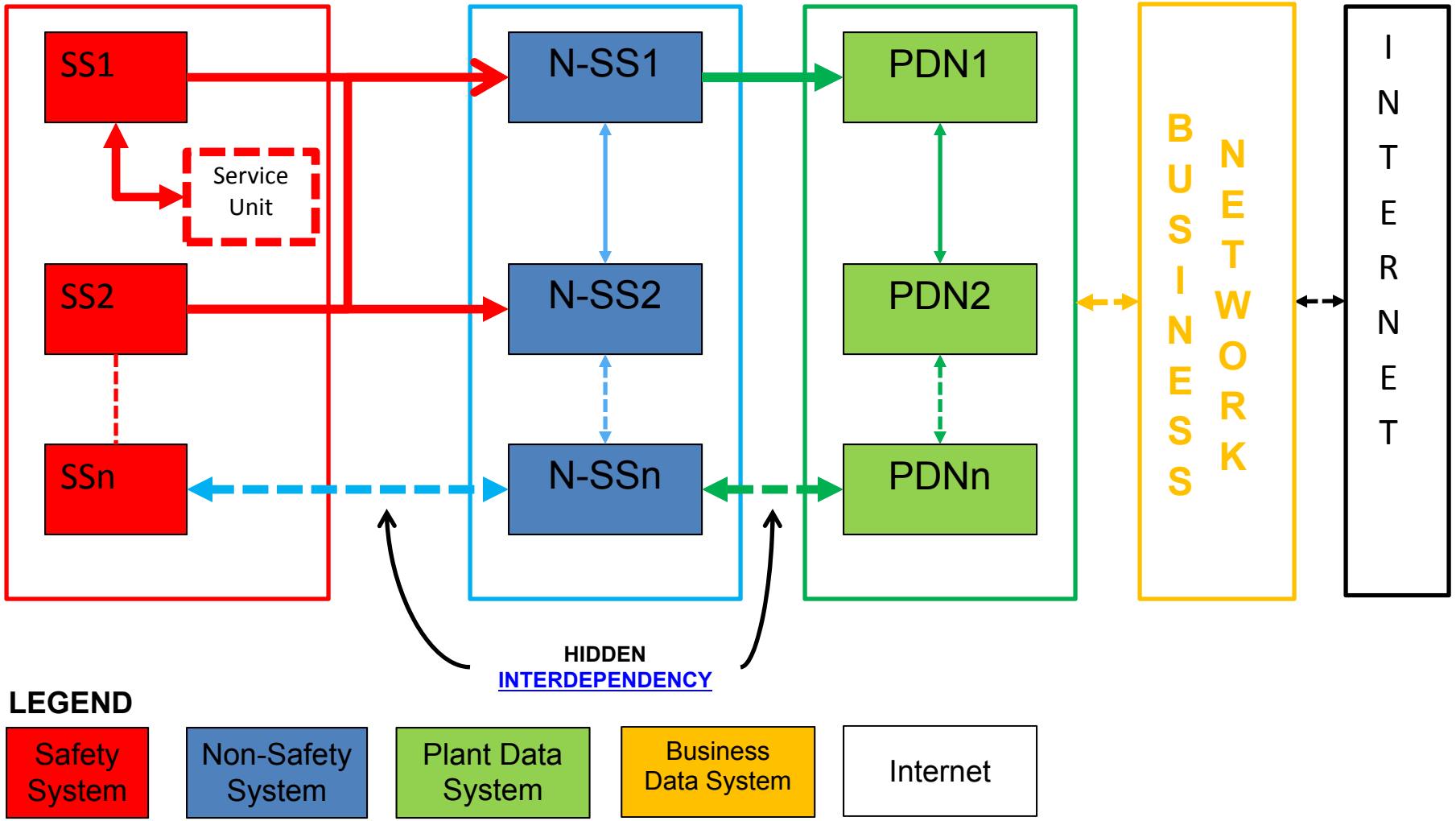
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Current State & Trends



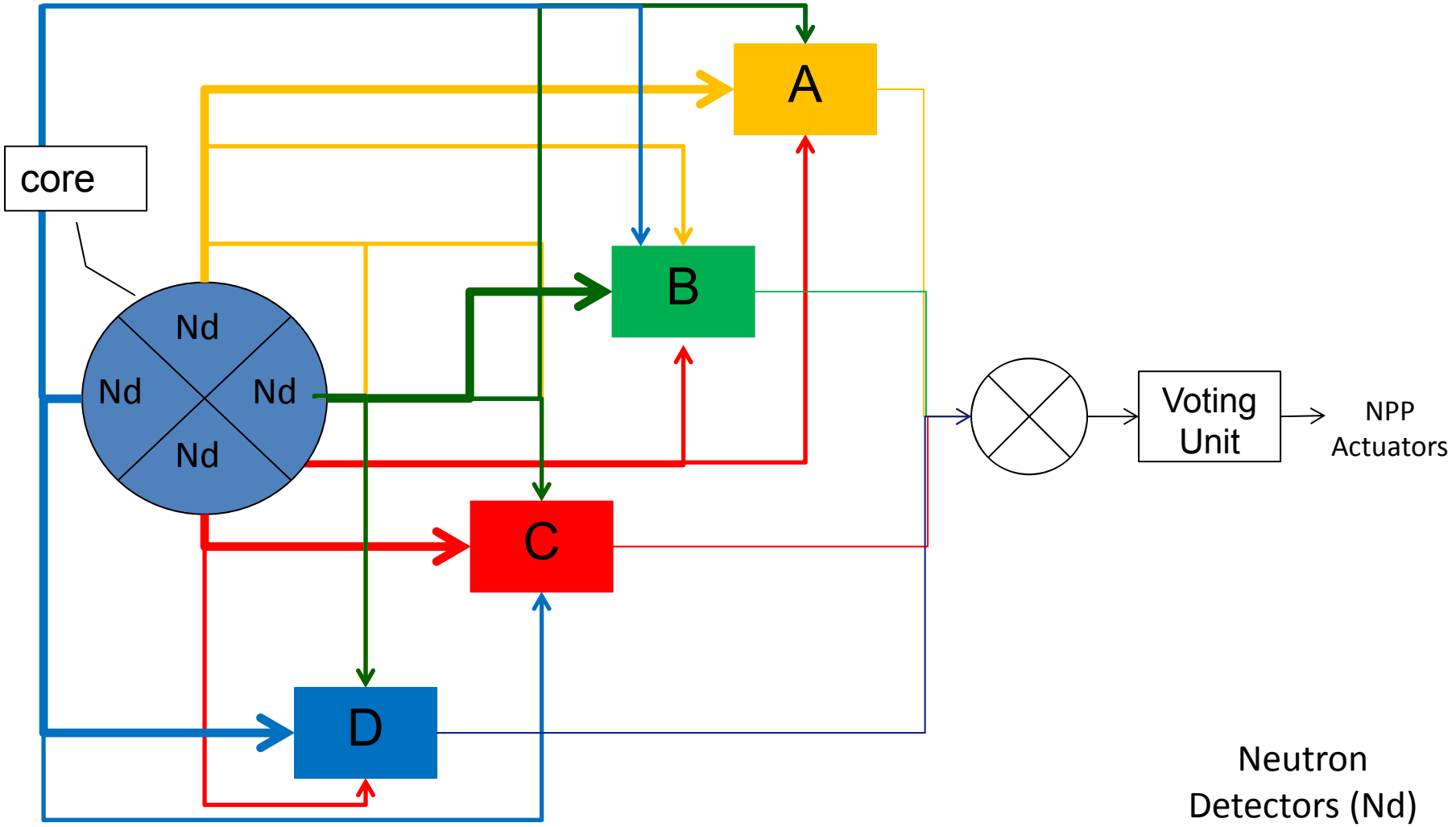
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Contributory Hazard Scenario (1/2): Safety – "Non-Safety" Interconnections



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

Contributory Hazard Scenario (2/2): Cross-Divisional Interconnections



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

Collaboration examples & opportunities

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

Collaboration channels: Examples

Industry

- EPRI
- IEEE
- INPO

International

- OECD/Halden
- MDEP
- TF SCS
- SCC
- IRSN
- KAERI
- STUK

Interagency

- NSF
- NASA
- FAA
- DoD/ OASD
- SERC
- AFRL
- SEI
- AMRDEC
- FDA
- DHS
- NSA
- NIST
- NRL

Academia

- MIT
- UVA
- KSU
- CMU
- Vanderbilt
- York

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

Cross-domain collaboration opportunities: Technical

1. Work product evaluation – necessary and sufficient criteria
2. Technological infrastructure, e.g.:
   a. Harmonized vocabulary. Ontologies of key concepts.
   b. Modeling different types of dependencies
   c. Strict stepwise refinement
   d. Tools. Their qualification
   e. Reusable assets
   f. Third party certification infrastructure

See in U.S. NRC RIL-1101:
- Appendices C for item 1
- Appendix A for item 2a
- Appendix D for item 2c
- Appendix K for item 2b

Aspirational Roadmap: Assurance Capability:
http://pbadupws.nrc.gov/docs/ML1511/ML15113A337.pdf

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

Example of common need 1/2 - modeling dependencies

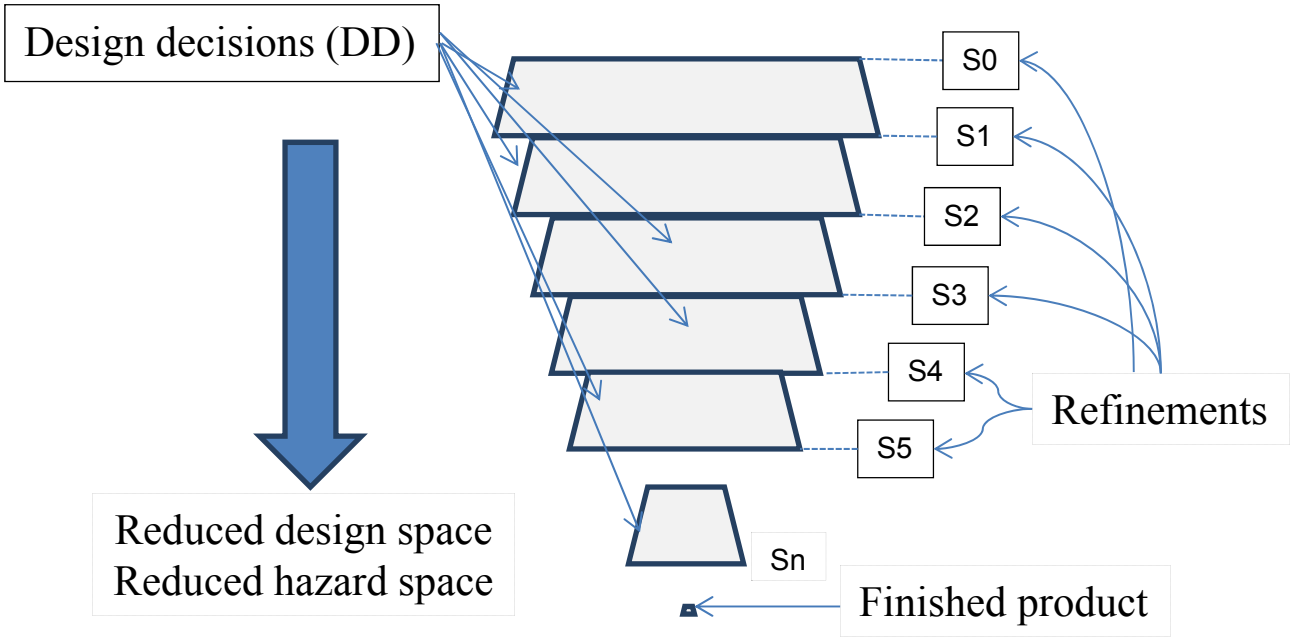
Modeling different kinds of dependencies, e.g.:

- 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.

(See U.S. NRC RIL-1101 Appendices I, J, K)

Example of common need 2/2 – stepwise refinement

Concept of stepwise refinement - steps S0, S1, S2, S3, S4, S5 … Sn



See U.S. NRC RIL-1101 Appendix D

Enables "correct by construction"

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

Collaboration opportunities: Other than technology

1. Capability development: individual
2. Capability development: communal
3. Culture
4. Business case: societal; lifecycle economics

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

Recap

Need driven research planning

- Starting from industry-perceived issues
- Addressing foundational gaps ← technical collaboration opportunities
- Iterative, evolutionary paradigm shift

From Past Practice	To Future Vision	Example research activity
Compliance-based	Goal-driven (example)	Improved hazard analysis methods & tools
Prescriptive	Performance based	Future regulatory & guidance framework
Rework. Patchwork. Workaround. Mitigation.	Prevention (example)	Designed in assurance Correct by construction
Short term fragments	Integrative foundation	Integrated safety-security evaluation
Reactive	Proactive	Embedded digital devices

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

Supporting information

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

Research support to licensing offices

- Perform confirmatory research; develop technical bases
  - Work products: RILs, NUREGs, technical papers
  - External Resources: Labs; Collaborations: In USA; International
- Develop regulatory guidance
- Other supporting activities:
  - Rulemaking
  - Standards development
  - Identify & resolve technical issues
  - Seminars and workshops: Knowledge to evaluate digital systems

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

How recently developed technical basis fits in Regulatory Activities

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

Work products - examples

2011: NUREG/IA-0254, "Suitability of Fault Modes and Effects Analysis for Regulatory Assurance of Complex Logic in Digital Instrumentation and Control Systems" [*IRSN-USNRC collaboration*]

2011: RIL-1001, "Software-Related Uncertainties in the Assurance of Digital Safety Systems" [*Internal + expert clinic*]

2014: RIL-1002, "Identification of Failure Modes in Digital Safety Systems" [*Internal + expert clinic*]

2016: RIL-1003, "Feasibility of Applying Failure Mode Analysis to Quantification of Risk Associated with Digital Safety Systems" [*Internal + expert clinic*]

2015: RIL-1101, "Technical Basis for review of Hazard Analysis" [*Internal + experts*]

2015: Technical Reports, "Evaluation of Guidance for Tools Used to Develop Safety-Related Digital Instrumentation and Control Software for Nuclear Power Plants" [*Contractor: ISL*]

In process: Rulemaking language & draft guide DG-1251 (RG 1.153, Proposed Rev 2) "Criteria for the Power, Instrumentation, and Control Portions of Safety Systems for Nuclear Power Plants"[*Internal*]

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

Current Work - examples

- Support for Digital I&C Path Forward Action Plan [*Internal*]

  → Research Plan FY 2015-2019 [*Internal* ← *CMU/SEI*]

- Safety demonstration (or assurance case) framework
  - Case-based research: EPR case → APR 1400 case [*OECD/Halden*]
- Evaluation of an embedded digital device
  - Case-based research {smart actuators; smart sensors; connected cases} [SERC/CMU]
- Hazard analysis knowledge transfer
  - Case-based activity → APR 1400 [*CMU/SEI*]
- Review Management System: Tool to review current SRP [*NRC/OIS*]

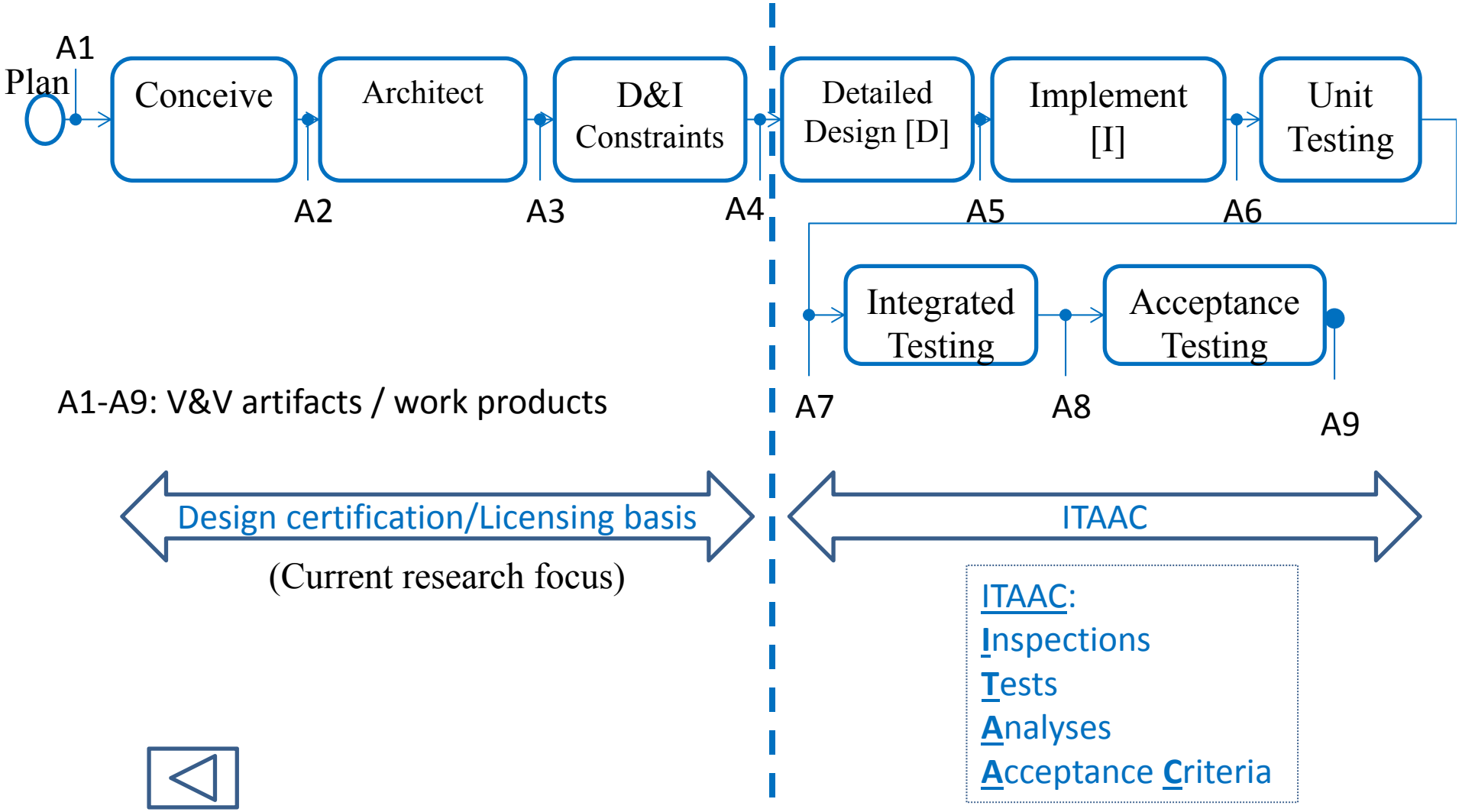
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Hazard analysis (HA) → Requirements → Architecture

Broken chain

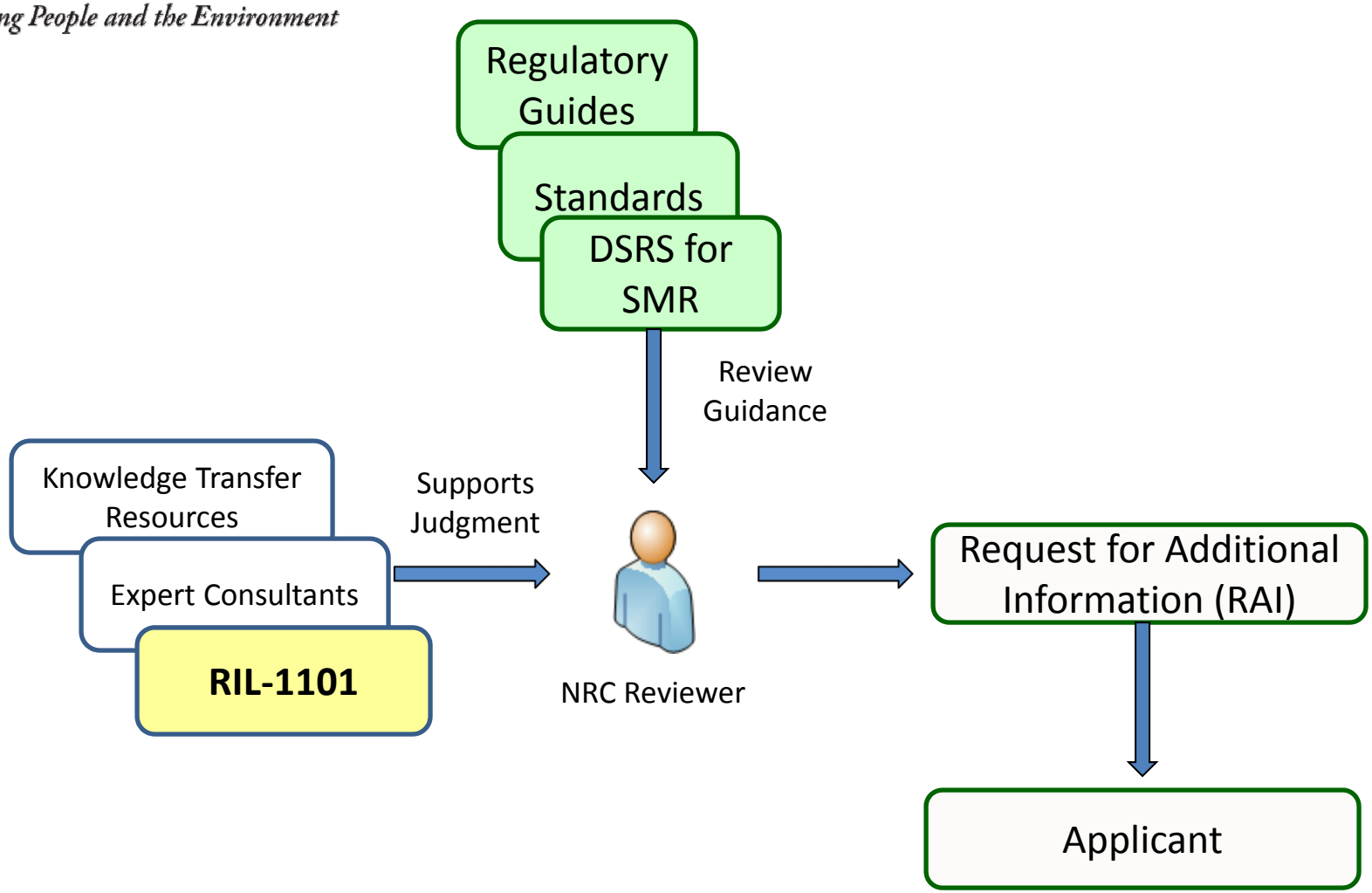
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Scope of Licensing Basis for new reactors



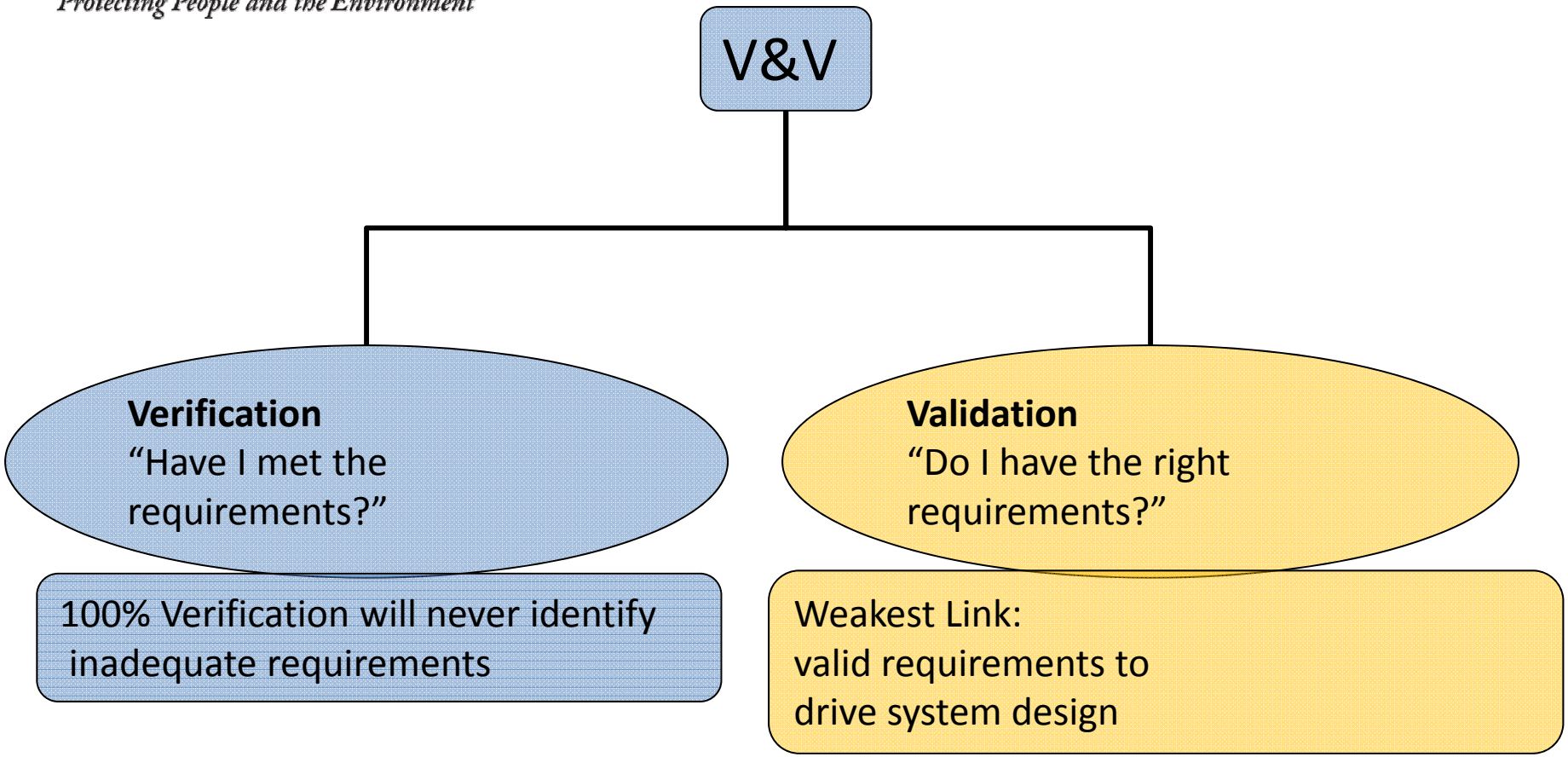
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Role of RIL-1101 in NRC Review Process



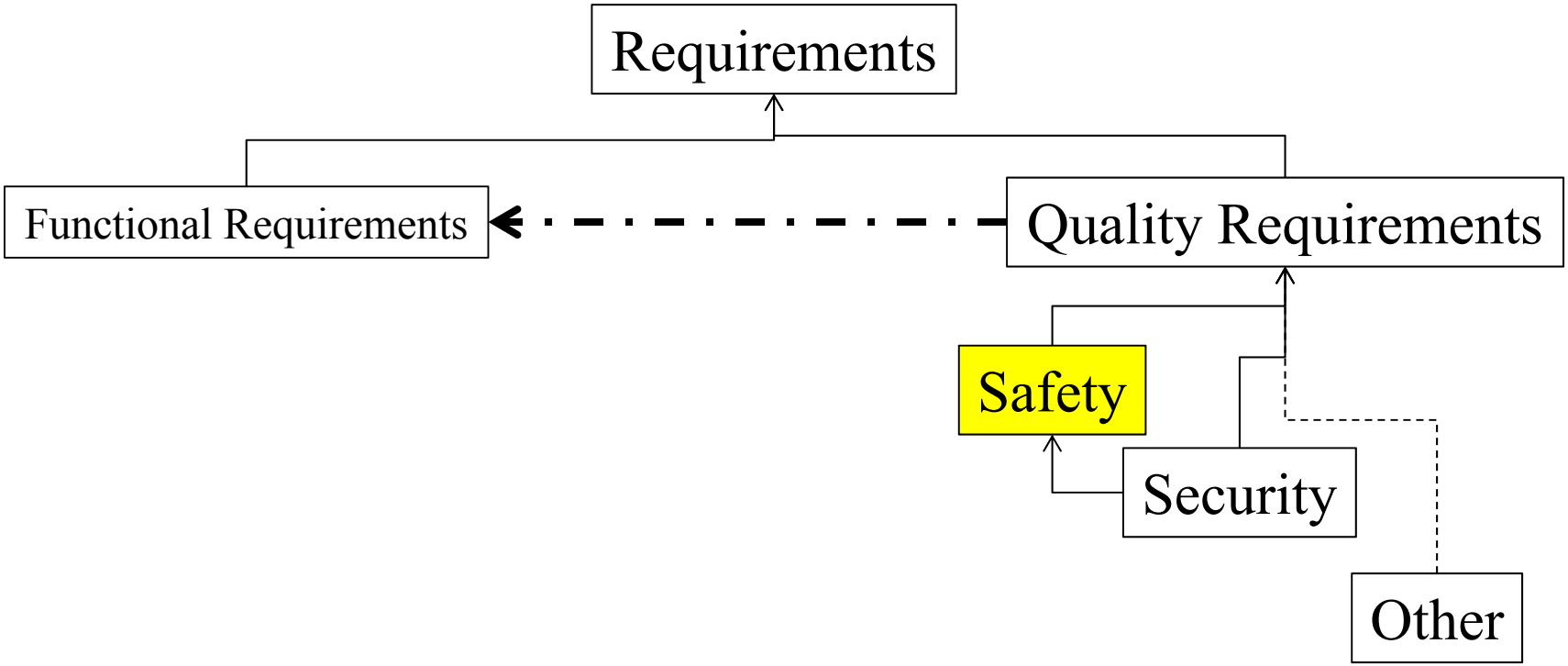
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Valid requirements are needed



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

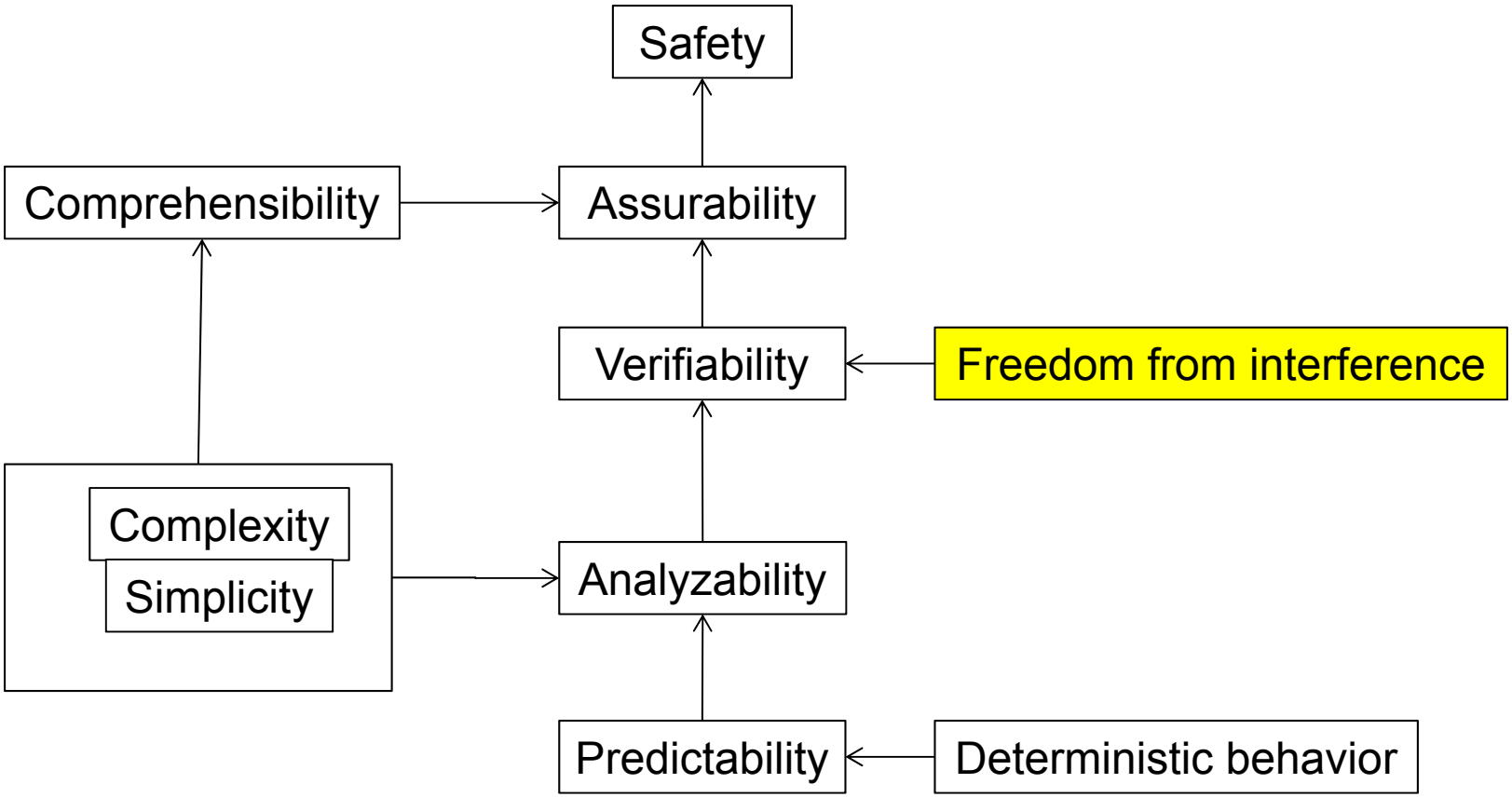
The gap in valid requirements: not the specification of functions



Quality requirements drive architecture!

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

Safety: some sub-characteristics



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

Hazard Analysis explained in terms of IEEE Std 603 criterion 4h

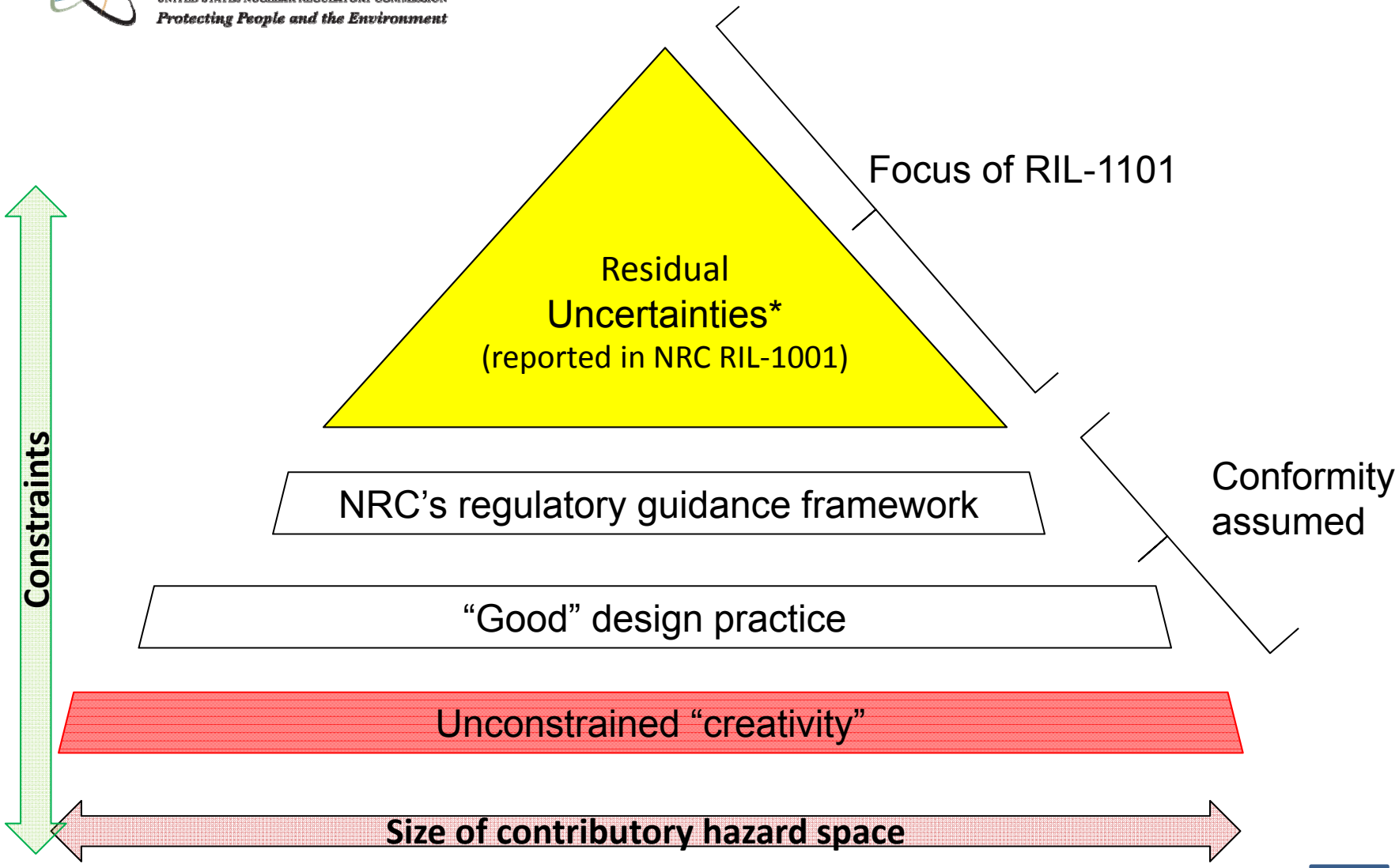
A specific basis shall be established
for the design of each safety system
of the nuclear power generating station;
the design basis shall document as a minimum …

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

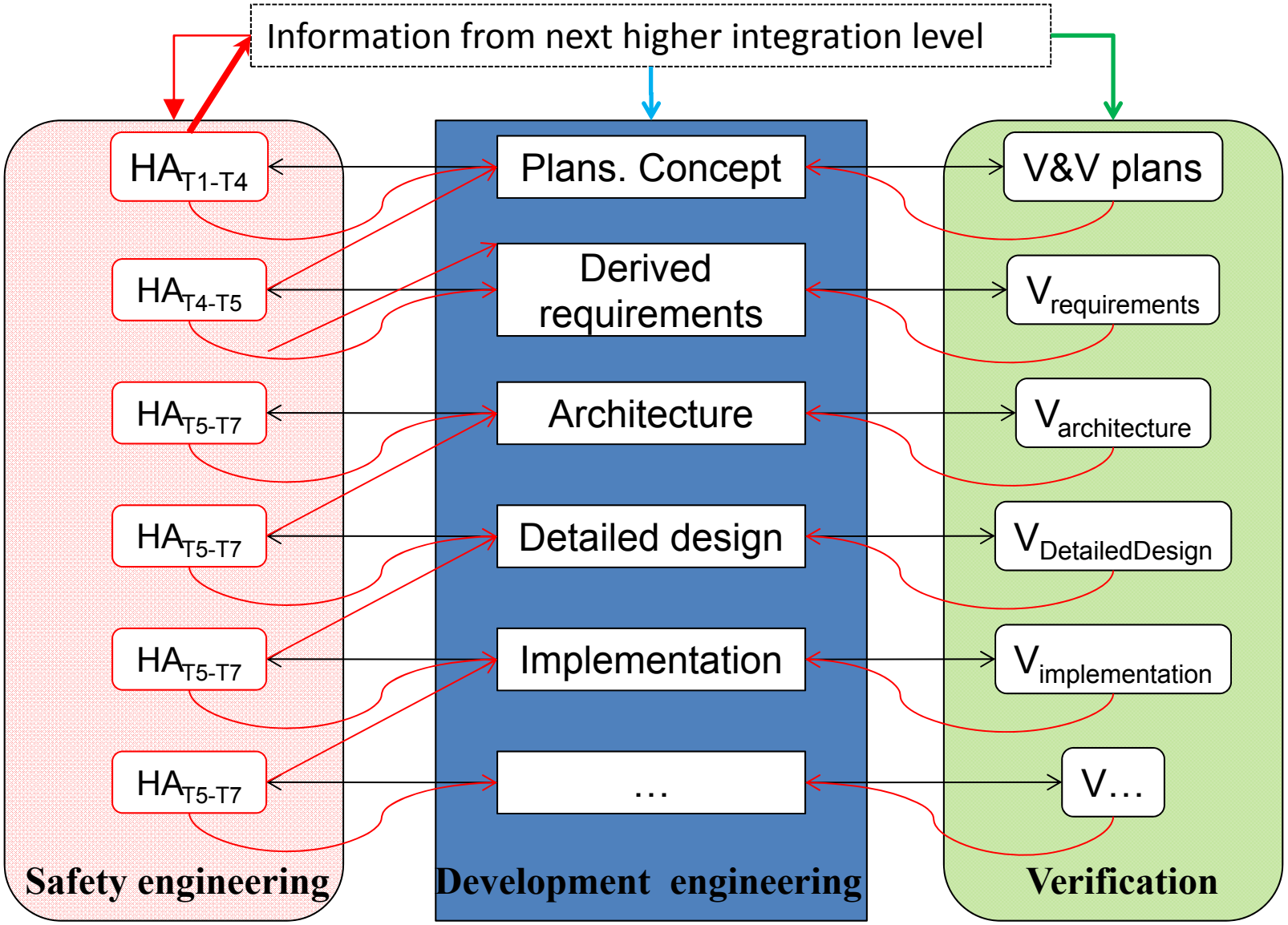
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Contributory Hazard Space in Focus



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

Hazard Analysis: Source of validated safety requirements



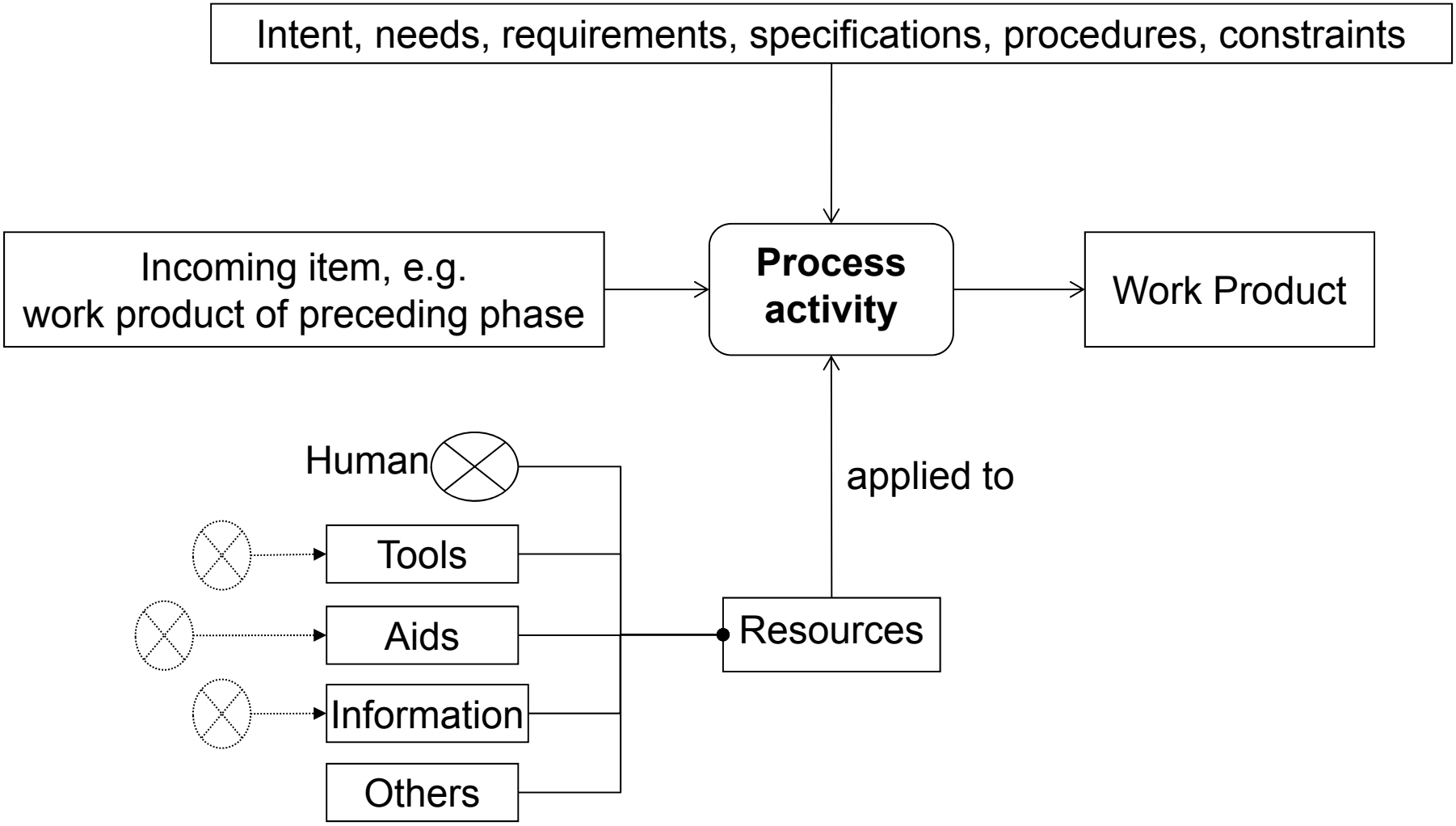
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

How a safety function can be degraded
[*RIL-1002*]

1. Not provided; examples:
   - Data sent on a communication bus is not delivered.
2. Provided when not needed
3. Incorrect value provided; causes:
   - Invalid data
   - Stale input value is treated inconsistently.
   - Undefined type of data
   - Incorrect message format
   - Incorrect initialization; etc.
4. Provided at wrong time or out of seq.
5. Provided: duration too long (e.g., for continuous-control functions).
6. Provided: duration too short; e.g.:
   - Signal is de-activated too early (e.g., for continuous-control functions).
7. Incorrect state transition
8. Intermittent, when required to be steady; examples:
   - Chatter or flutter
   - Pulse; spike
   - Impairment is erratic
9. Byzantine behavior
10. Interference in other ways:
    - Deprives access to a needed resource; for example:
      - "Babbling idiot"
      - Locking up and not releasing resource
    - Corrupts needed information

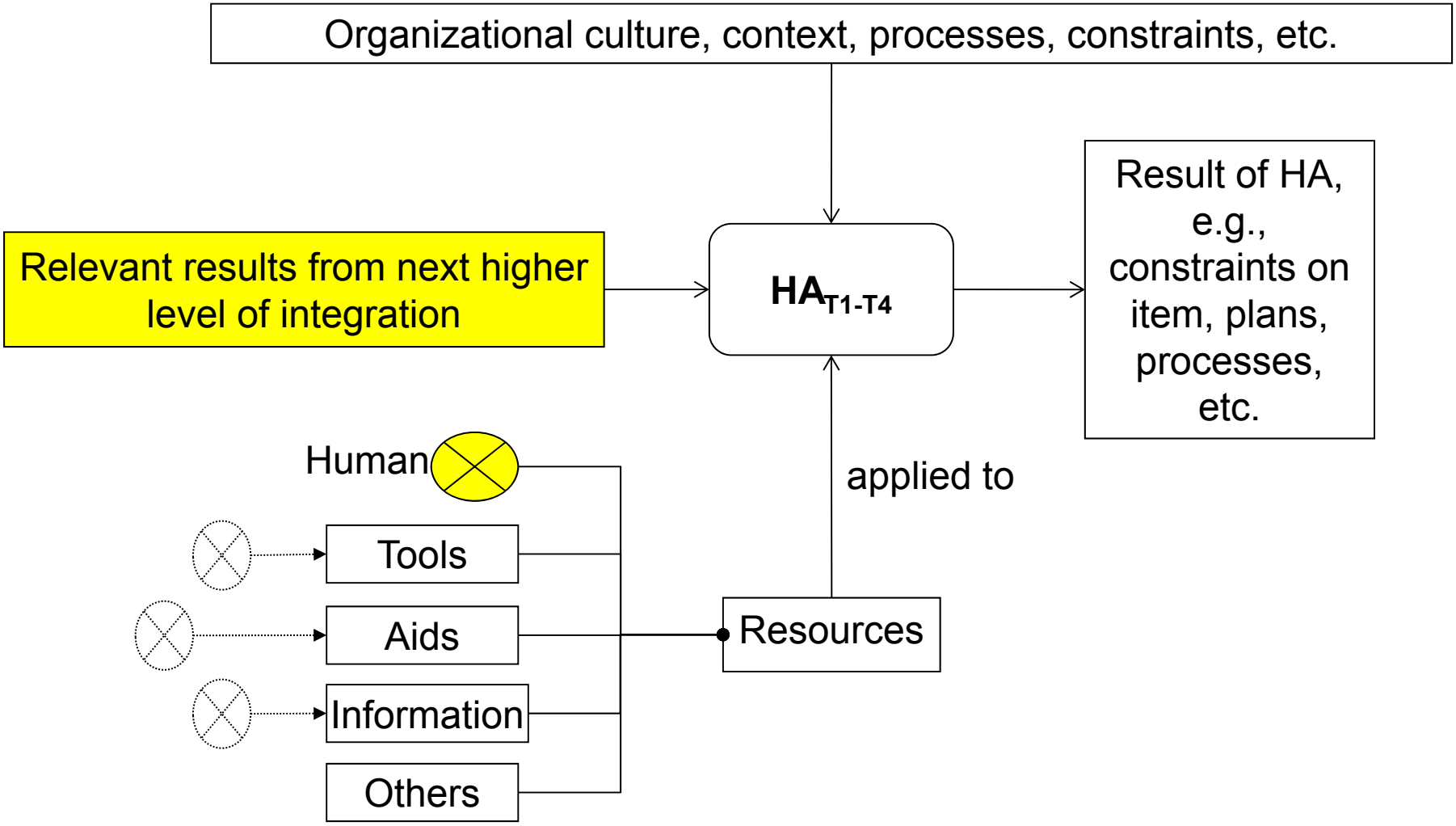
Identify & specify constraints to prevent degradation

Process Activity (e.g., Hazard Analysis): General influencing factors



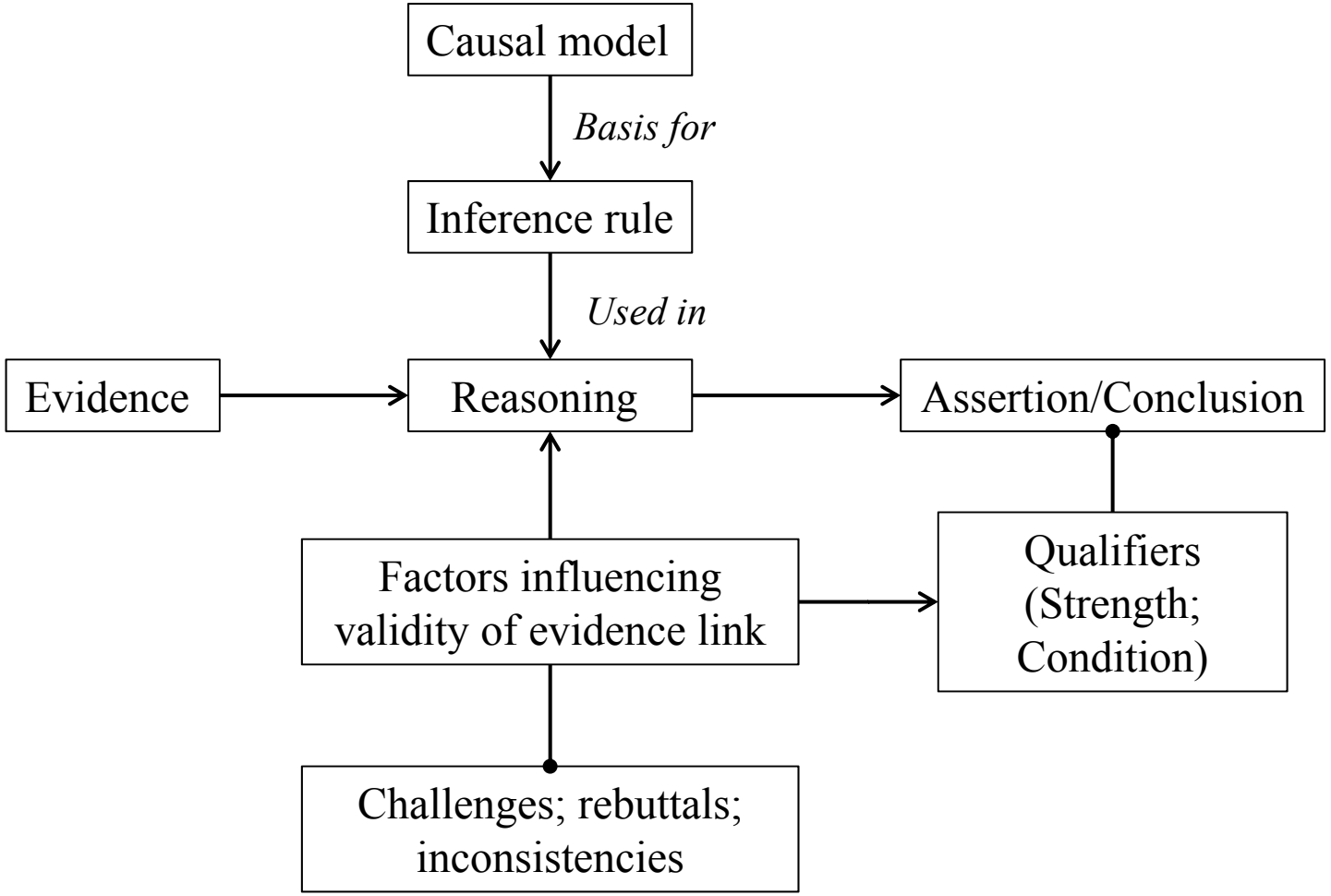
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Key factors affecting HA Quality



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

Reasoning Model [*adapted from Toulmin*]

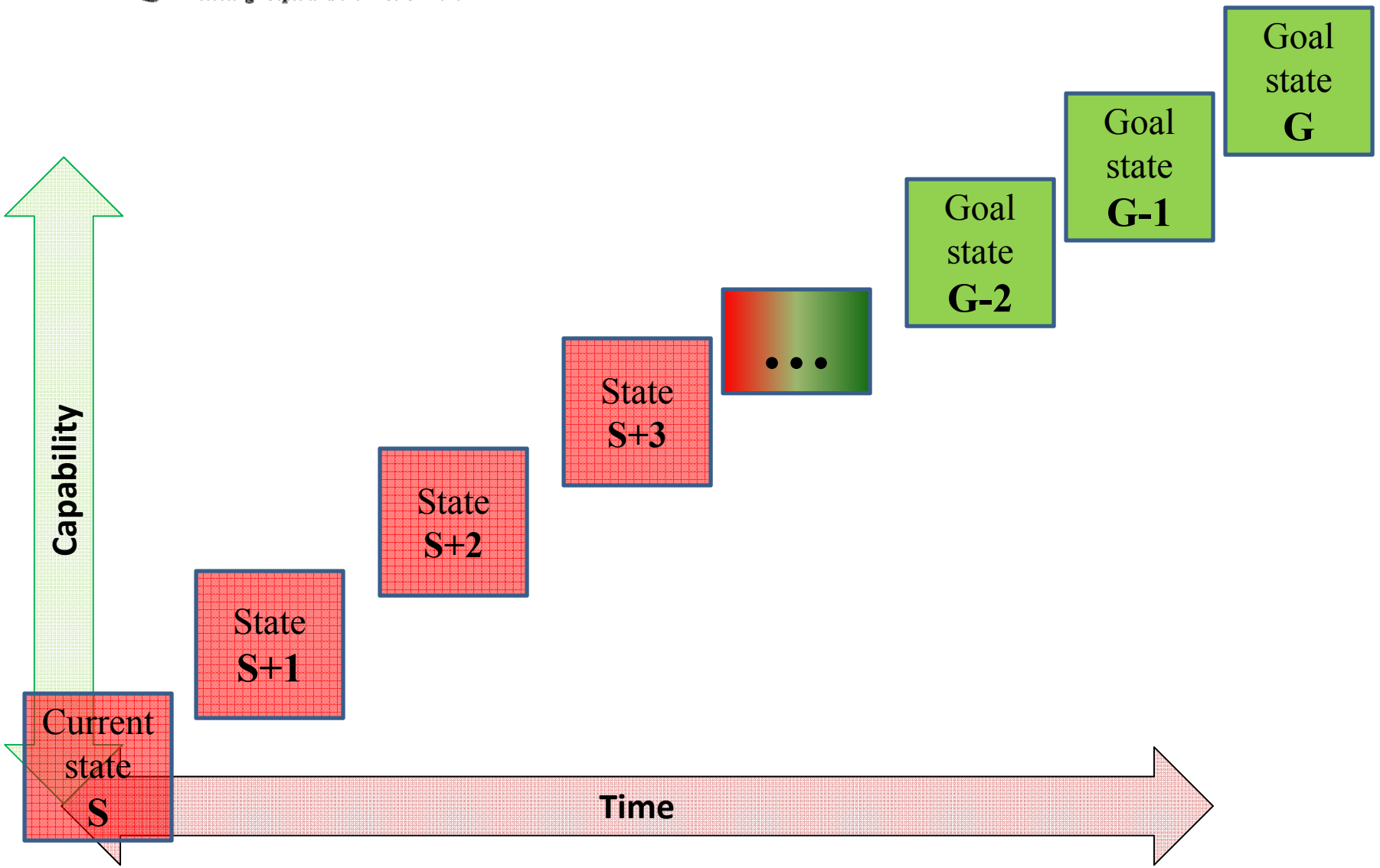


U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Incremental evolution of Assurance capability

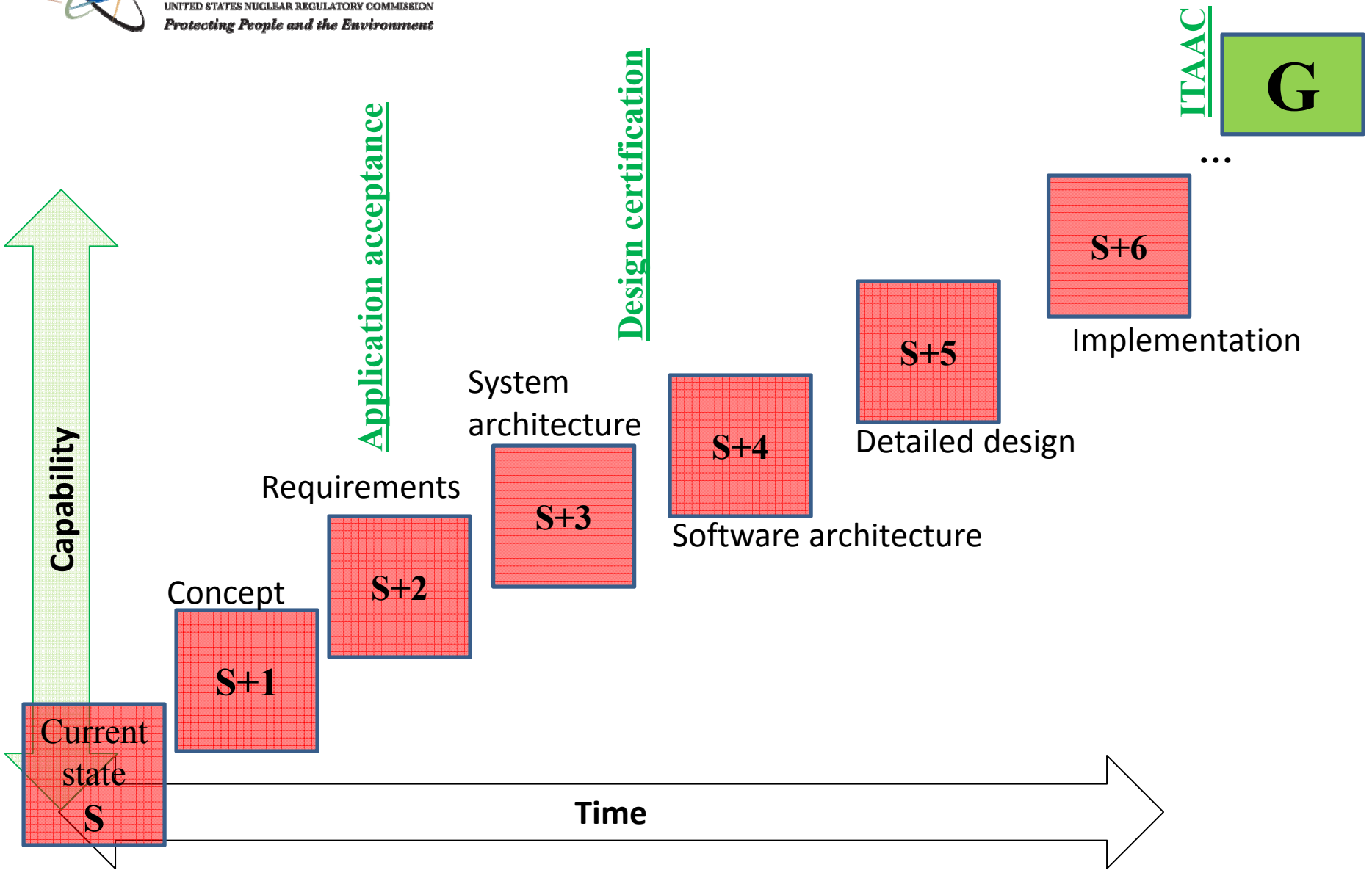
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Evolve Assurance capability: Concept



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

Evolve Assurance capability: NPP Case



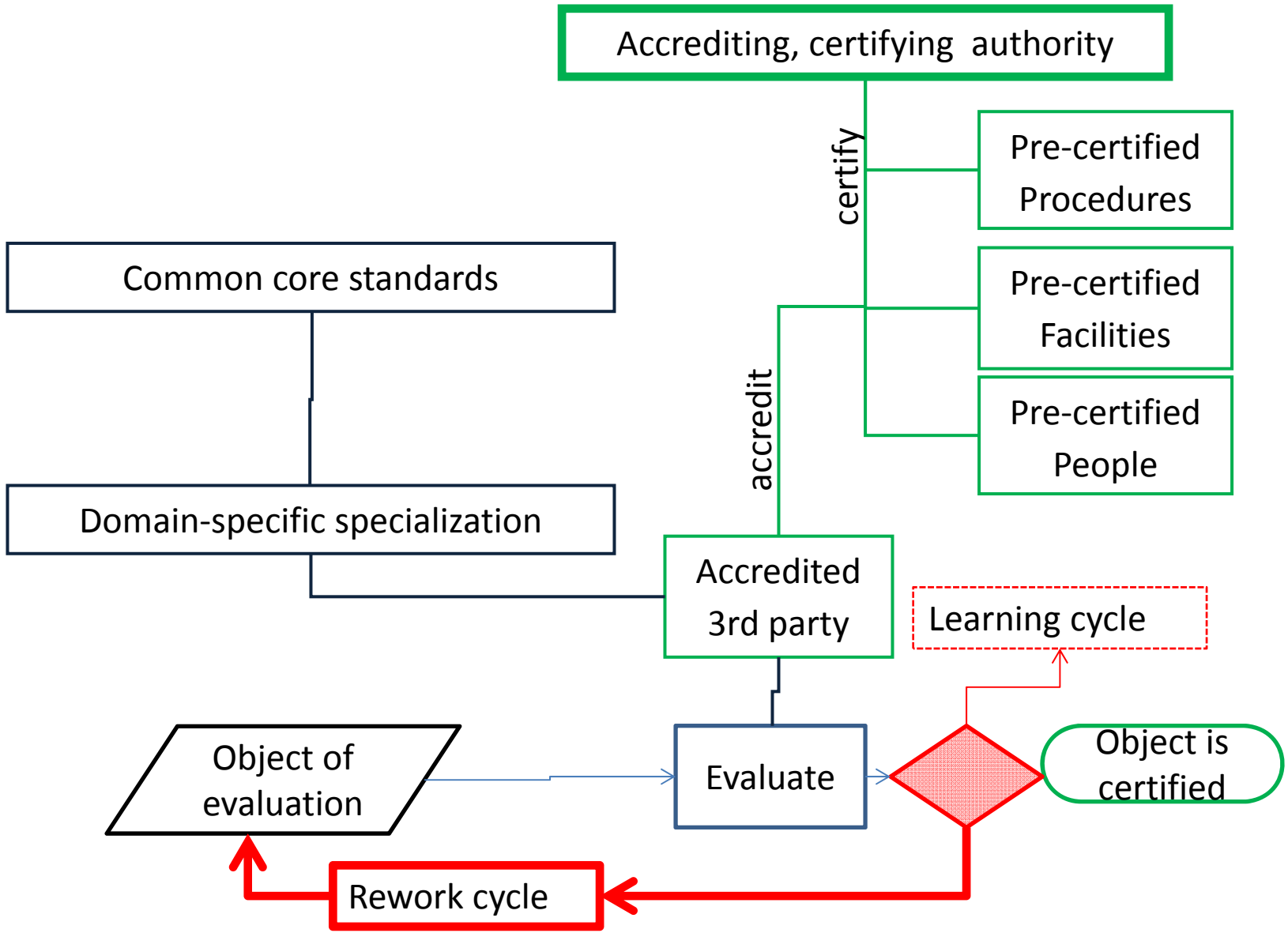
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Aspirational Assurance Process

for lifecycle economics

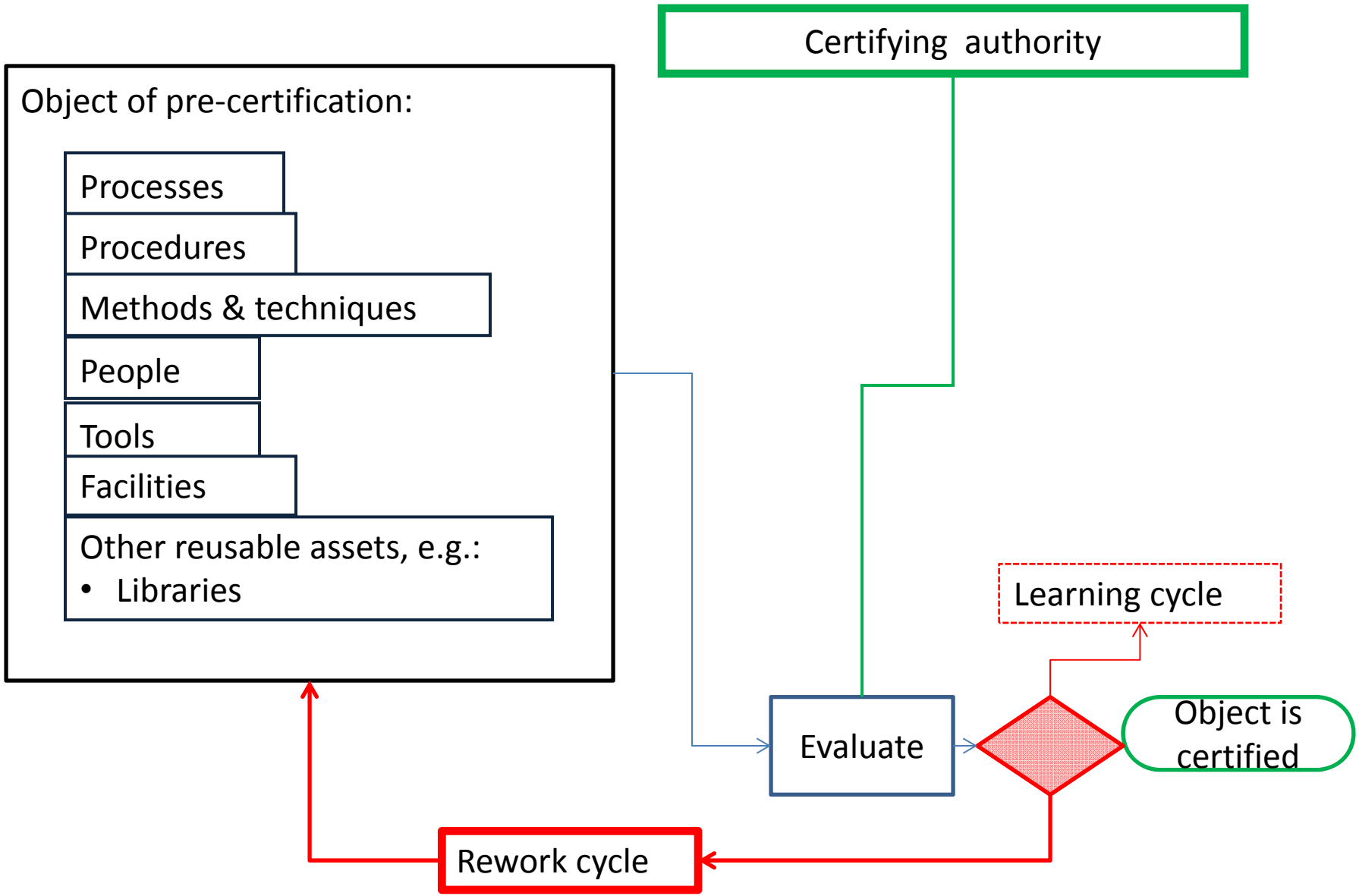
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Aspirational Assurance Process



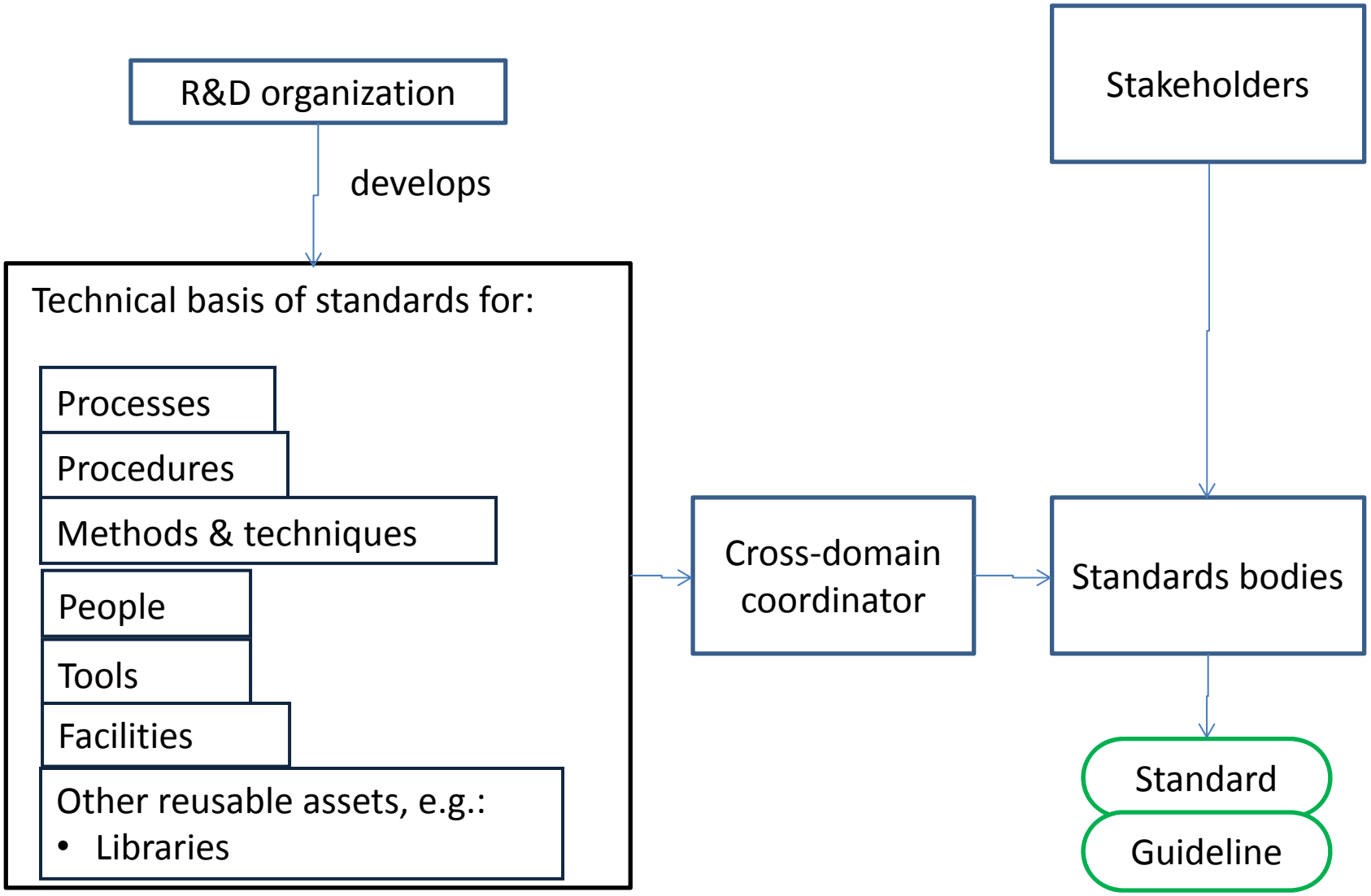
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Aspirational pre-certification activities



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

Aspirational standardization activities



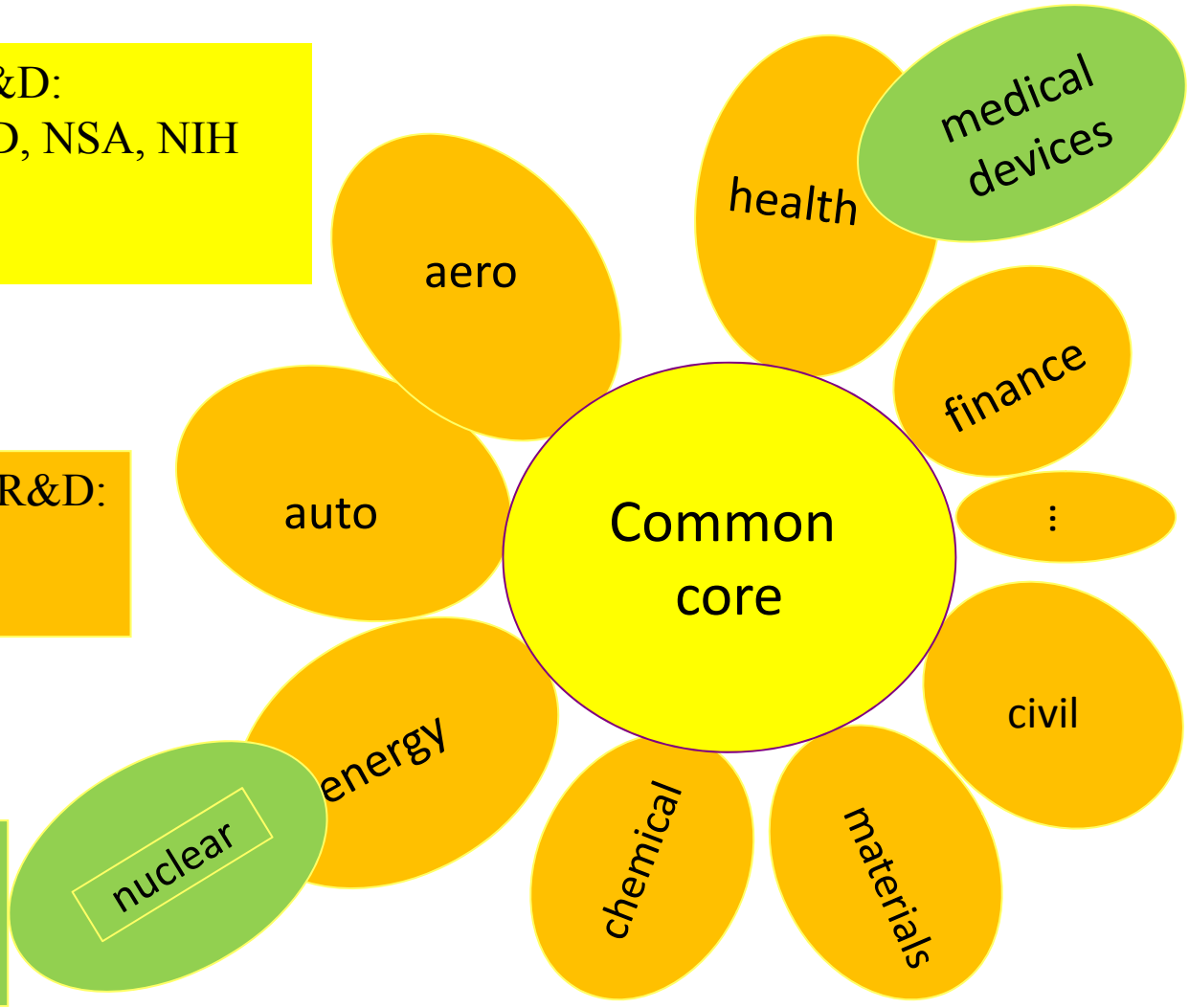
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cross-domain collaboration opportunity

Common core R&D:
- NSF, NIST, DoD, NSA, NIH
  …
- Academia

Domain-specific R&D:
- Industry
- Government

Pilot apps, e.g.:
- NRC, EPRI.
- FDA



Adapted from: CISE Overview of CPS R&D: Frontiers of Computing: A View from the National Science Foundation

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

Acronyms 1/3

ACRS	Advisory Committee on Reactor Safeguards
AERB	Atomic Energy Regulatory Board, India
AFRL	U. S. Air Force Research Labs
AMRDEC	U. S. Army Aviation & Missile Command Research Development & Engineering Laboratory
AP	Advanced Passive (1000)
APR	Advanced Power Reactor (1400)
APWR	Advanced Pressurized-Water Reactor
CCF	Common Cause Failure
CFR	Code of Federal Regulations
CGD	Commercial Grade Dedication
CMU	Carnegie Mellon University
DE	Division of Engineering
DG	Draft Guide
DHS	U. S. Department of Homeland Security
DI&C	Digital Instrumentation and Control
DFMEA	Design Failure Mode and Effects Analysis
DOD	Department of Defense
DOE	Department of Energy
DSRS	Design Specific Review Standard
EDD	Embedded Digital Device
EPR	Evolutionary Pressurized Reactor
EPRI	Electrical Power Research Institute
ESBWR	Economic Simplified Boiling Water Reactor
FAA	U. S. (Department of Transportation) Federal Aviation Administration
FAT	Factory Acceptance Test
FDA	U. S. (Department of Health and Human Services) Food and Drug Administration
FTA	Fault tree analysis
FY	Fiscal Year
HA	Hazard Analysis
HCU	High Cost and Unpredictability
HFE	Human Factors Engineering

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

Acronyms 2/3

I&C	Instrumentation and Control
IA	International Agreement (report)
ICEEB	Instrumentation, Controls, and Electrical Engineering Branch
IEEE	Institute of Electrical and Electronics Engineers
Info	Information
INPO	Institute of Nuclear Power Operations
IRSN	Institut de Radioprotection et de Sûreté
ITAAC	(NRC) Inspections, Tests, Analyses, Acceptance Criteria
KAERI	Korea Atomic Energy Research Institute
KSU	Kansas State Univesity
Lab	Laboratory
LAR	(NRC) License Amendment Request
MDEP	Multinational Design Evaluation Programme
MIT	Massachusetts Institute of Technology
MoU	Memorandum of Understanding
NASA	(U.S.) National Aeronautics and Space Administration
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NPEC	(IEEE Power & Energy Society) Nuclear Power Engineering Committee
NRL	(U.S.) Naval Research Laboratory
NRC	(U. S.) Nuclear Regulatory Commission
NRO	(NRC) Office of New Reactor
NRR	(NRC) Office of Nuclear Reactor Regulation
NSA	(U.S.) National Security Agency
NSF	(U.S.) National Science Foundation
NSIR	(NRC) Office of Nuclear Security and Incident Response
NUREG	(NRC) publication identifier (Nuclear Regulatory Commission)
OASD	(U.S. Department of Defense) Office of Assistant Secretary of Defense
OECD	Organization for Economic Cooperation and Development
OIS	(NRC) Office of Information Services
PLD	Programmable Logic Device

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

Acronyms 3/3

RES	(NRC) Office of Nuclear Regulatory Research
RG	(NRC) Regulatory Guide
RIL	(NRC) Research Information Letter
SC6	(IEEE/NPEC) Subcommittee Six (for Safety Systems)
SCC	
SEI	(CMUSoftware Certification Consortium) Software Engineering Institute
SERC	Systems Engineering Research Center
SMR	Small Modular Reactor
SRM	(NRC) Staff Requirements Memorandum
SRP	(NRC) Standard Review Plan
STUK	Radiation and Nuclear Safety Authority (Säteilyturvakeskus), Finland
TF SCS	Regulators' Task Force on Safety Critical Software for nuclear reactors
UNR	(NRC) User Need Request (a form of new research work request
U. S.	United States of America
UVA	University of Virginia
V&V	Verification and Validation