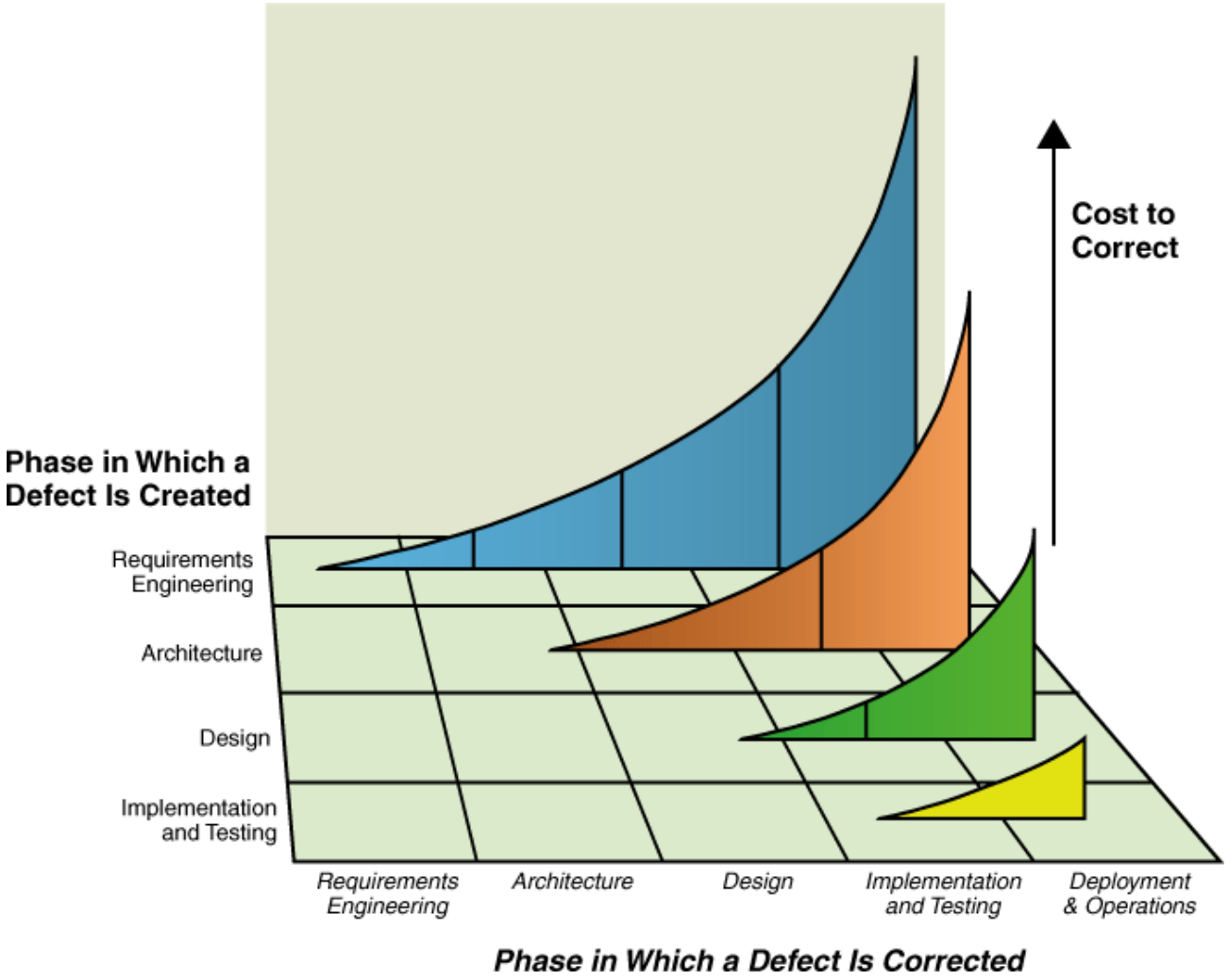
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Addressing hazards from common causes in engineering DI&C systems without diverse designs – State-of-the-Art

Enlarged Halden HTO Programme Review Group (EHPRG) meeting
September 25-28, 2023

Presenter: Sushil Birla
Office of Nuclear Regulatory Research
Division of Engineering

Understanding the Cost of Correcting Defects

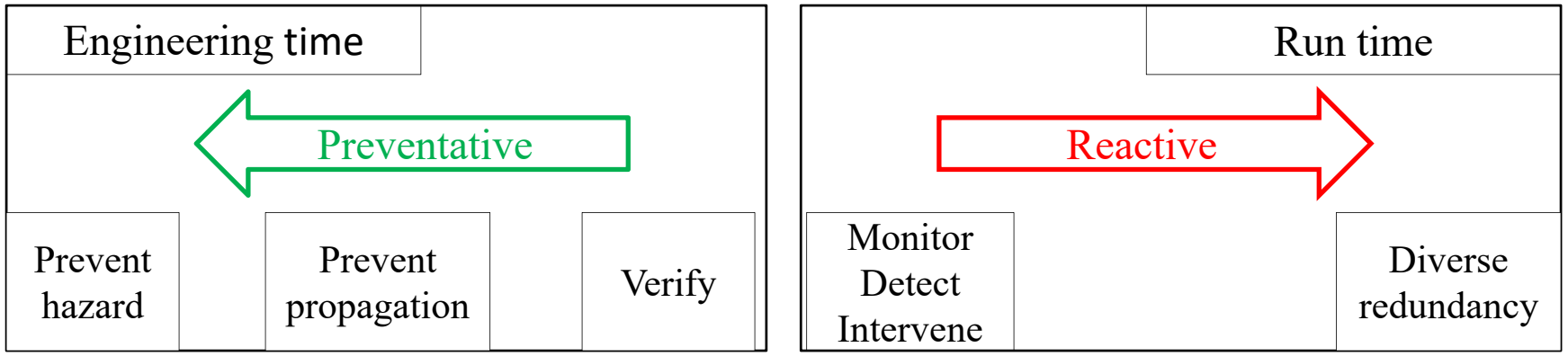


McConnell, Steve. “Software Quality at Top Speed.” August 1996.

http://www.stevemcconnell.com/articles/art04.htm

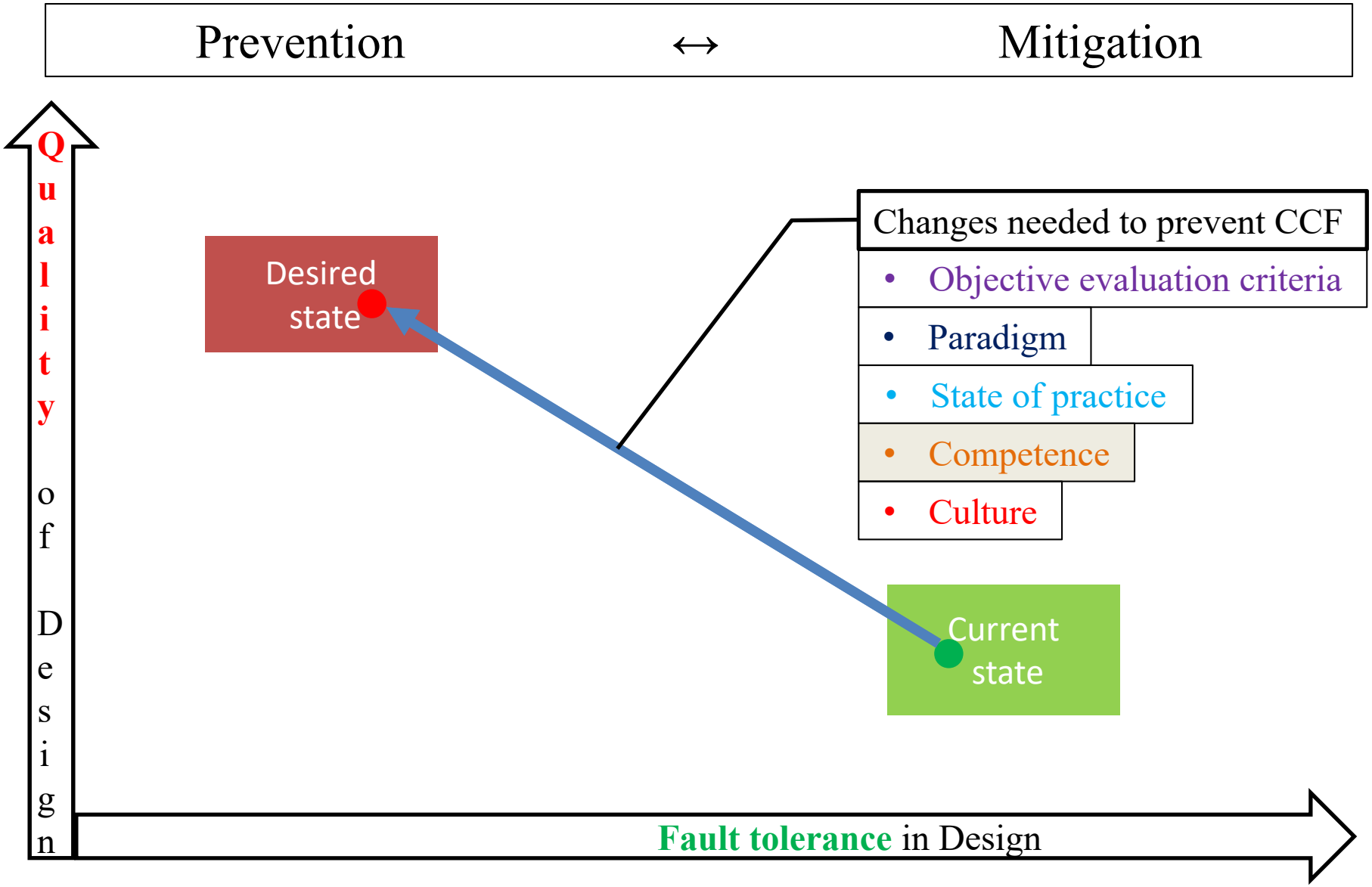
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Economics!



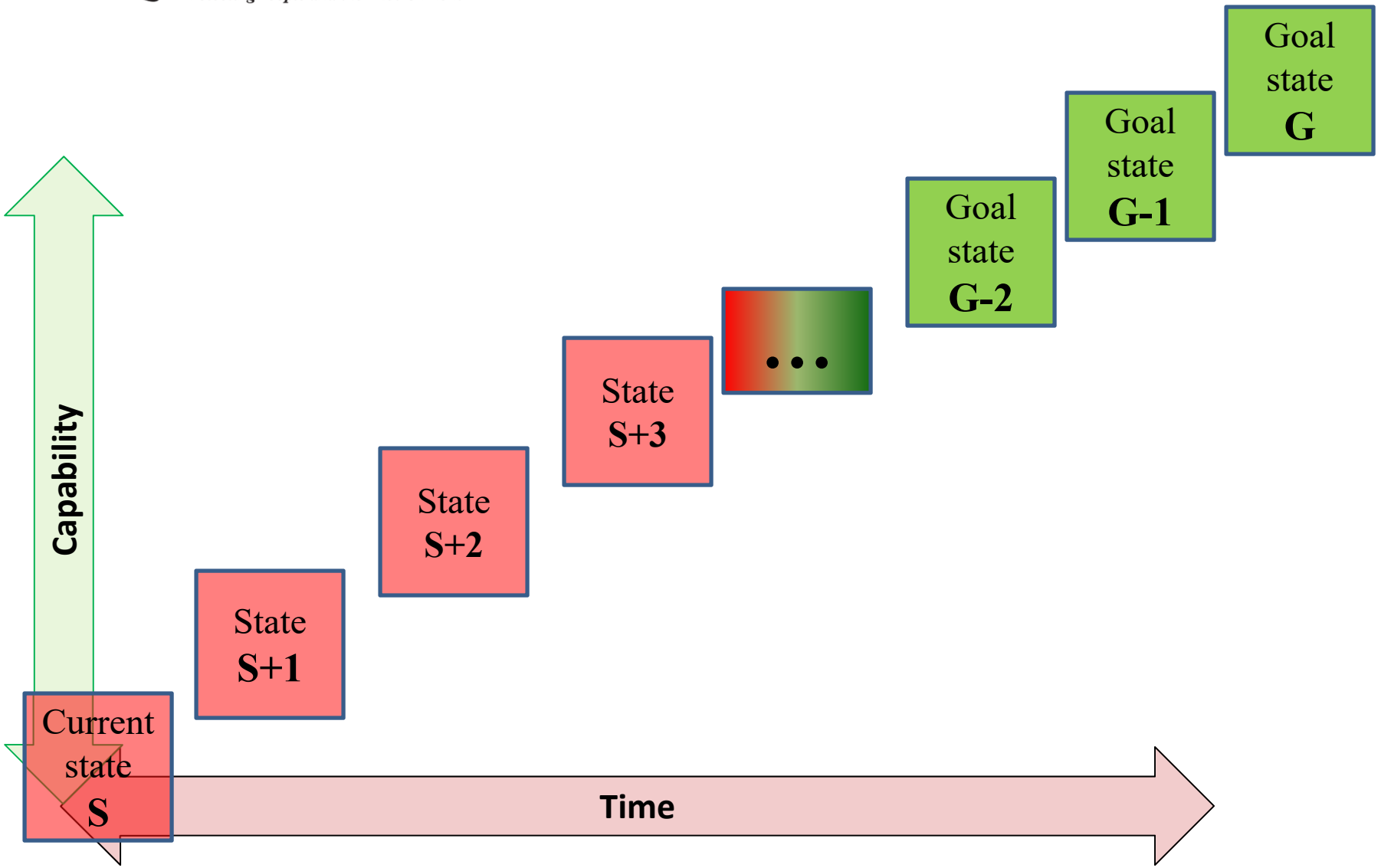
Potential to decrease intrinsic cost

Cost increases


Prevention ↔ Mitigation
Quality of Design
Desired state
Changes needed to prevent CCF
• Objective evaluation criteria
• Paradigm
• State of practice
• Competence
• Culture
Current state
Fault tolerance in Design

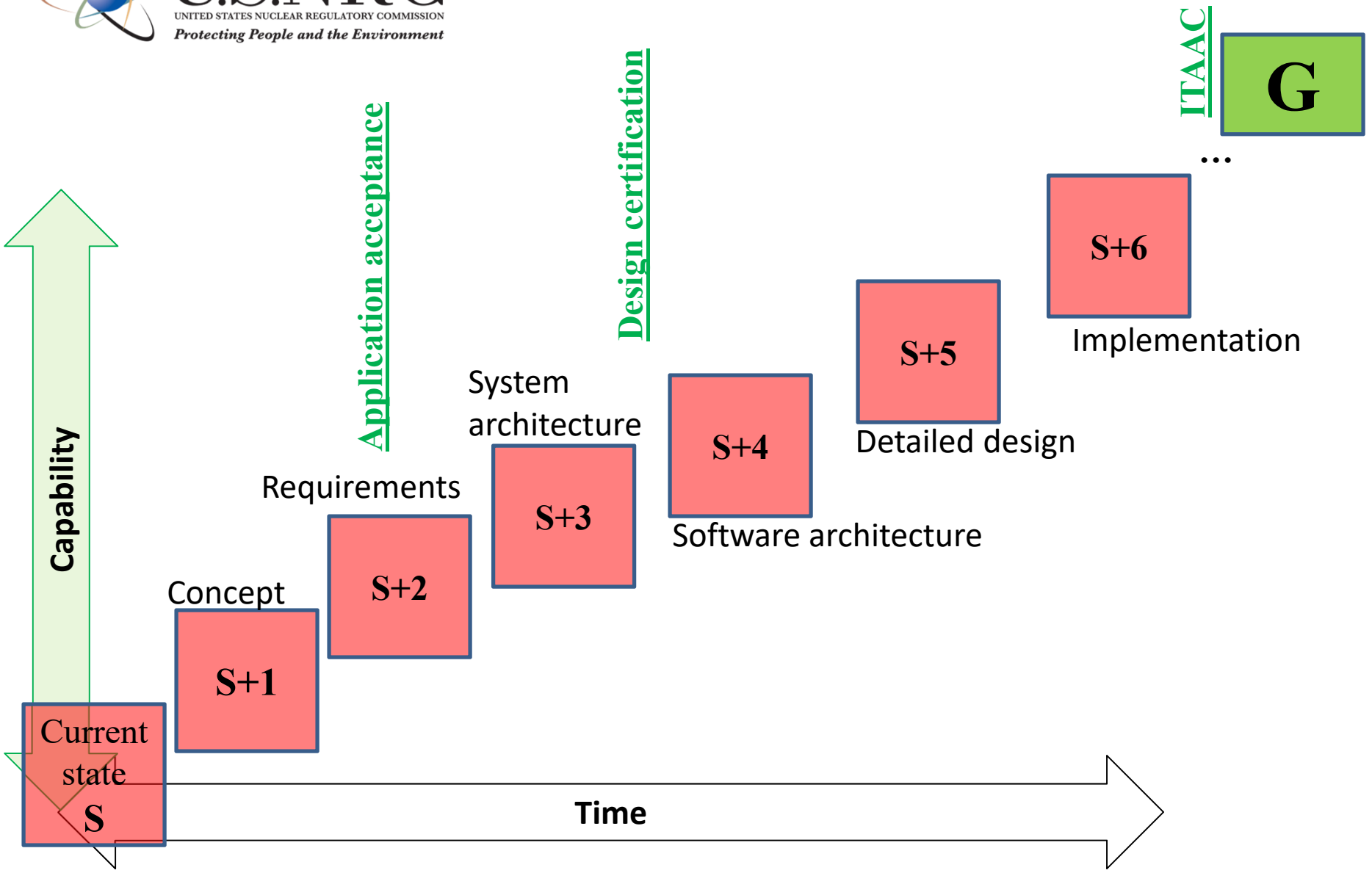
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Evolve Assurance capability incrementally



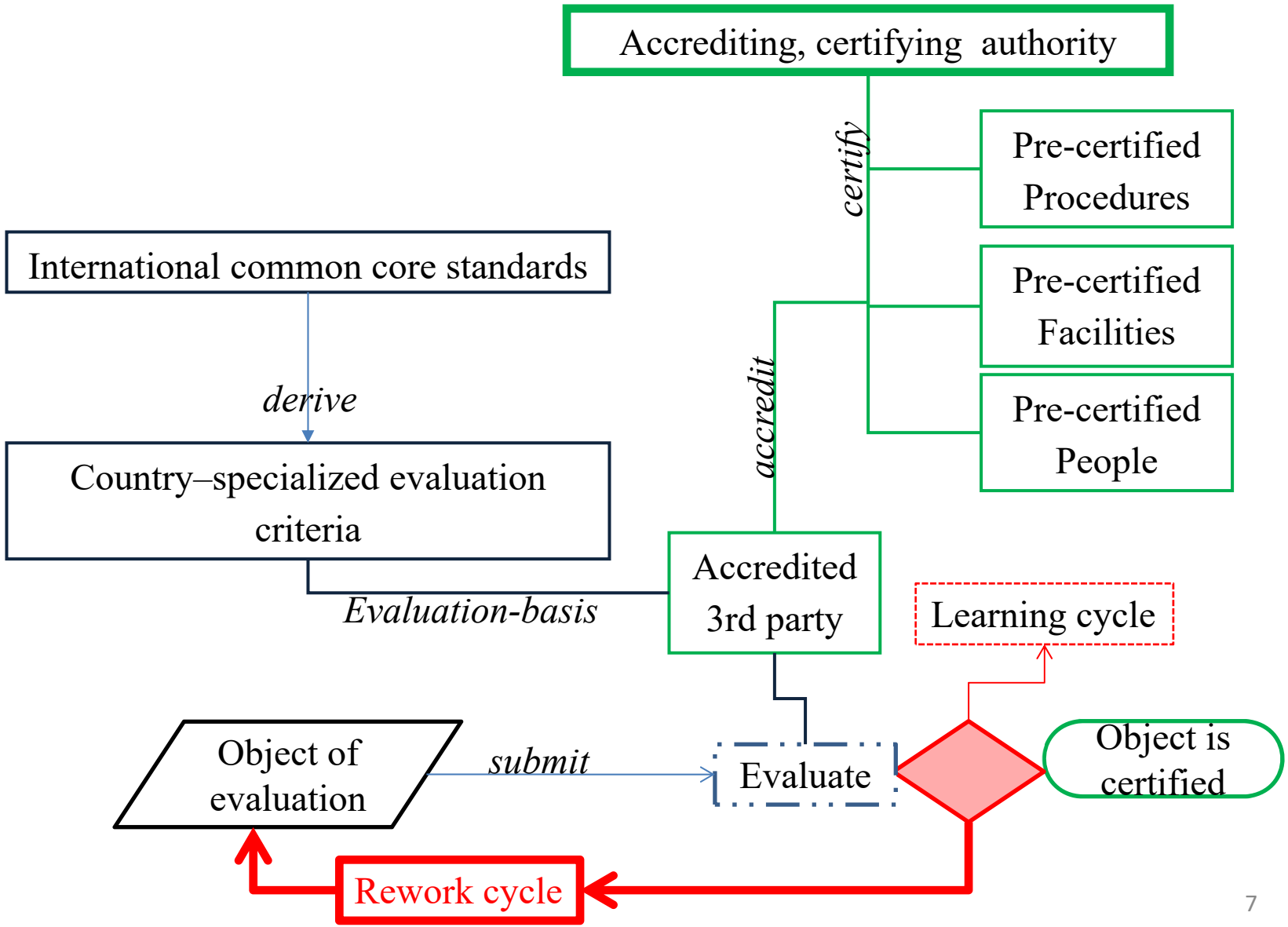
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Evolve Assurance capability: NPP Case



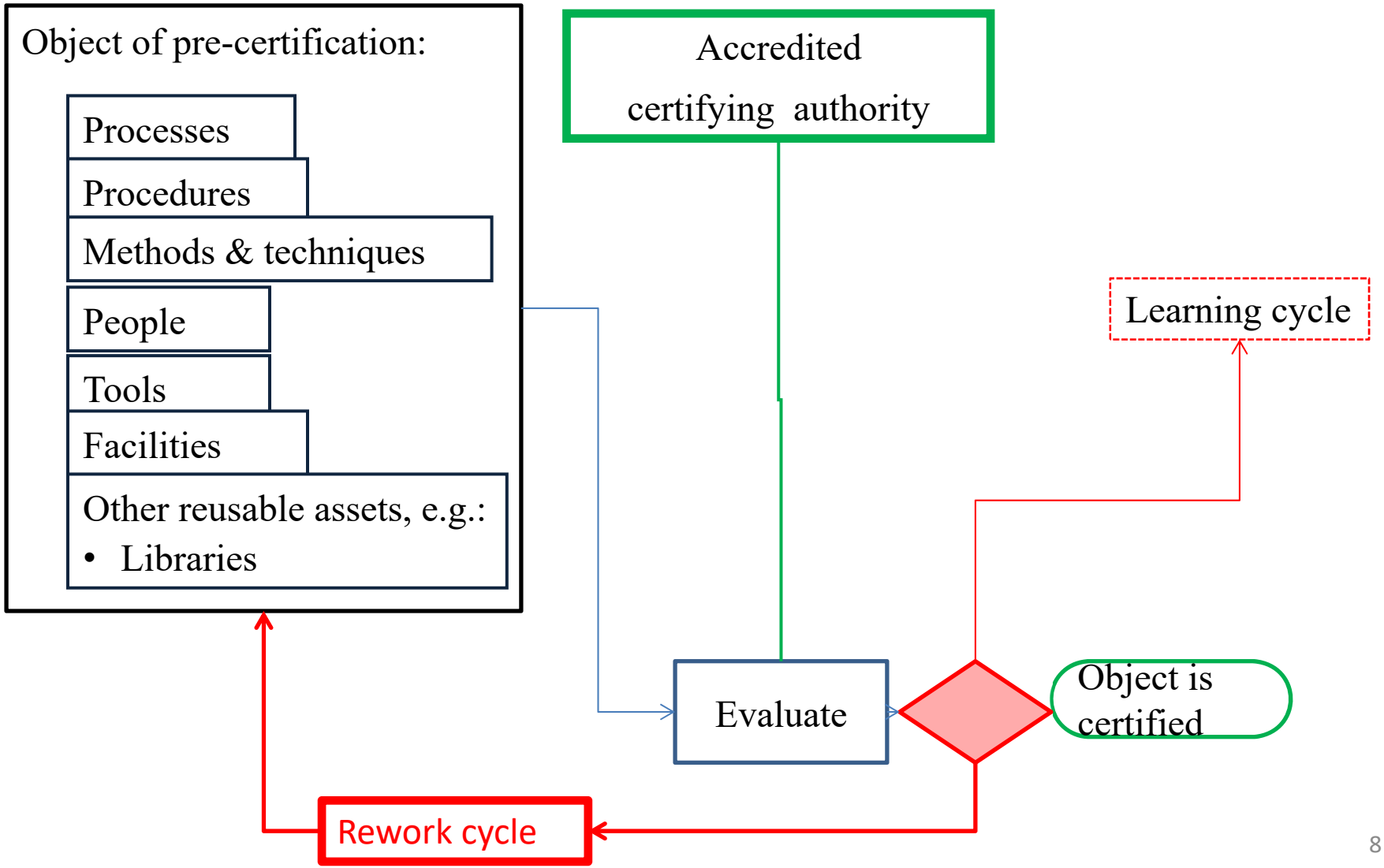
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

One vision of the Assurance Process



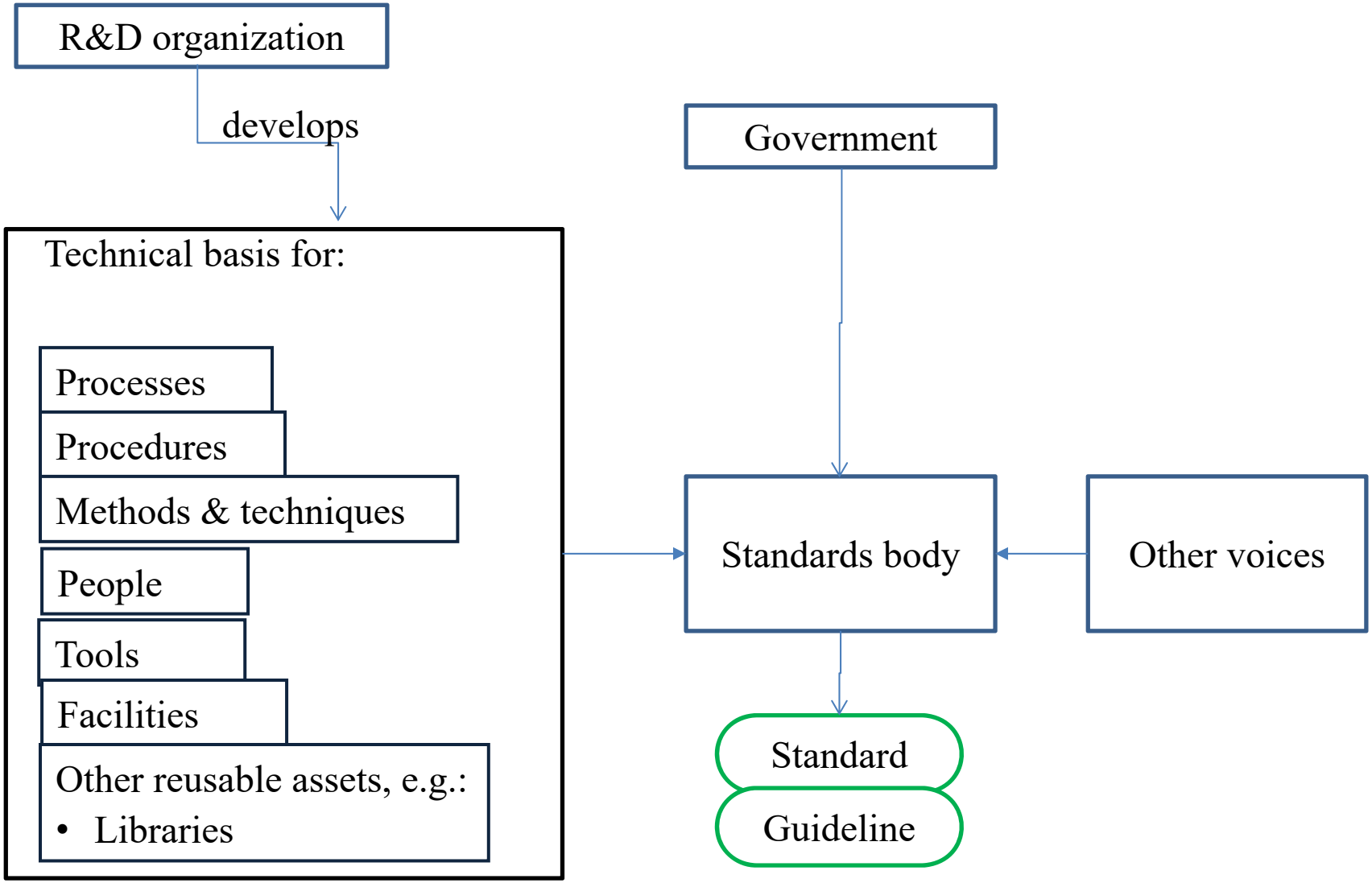
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Envisioned pre-certification activities

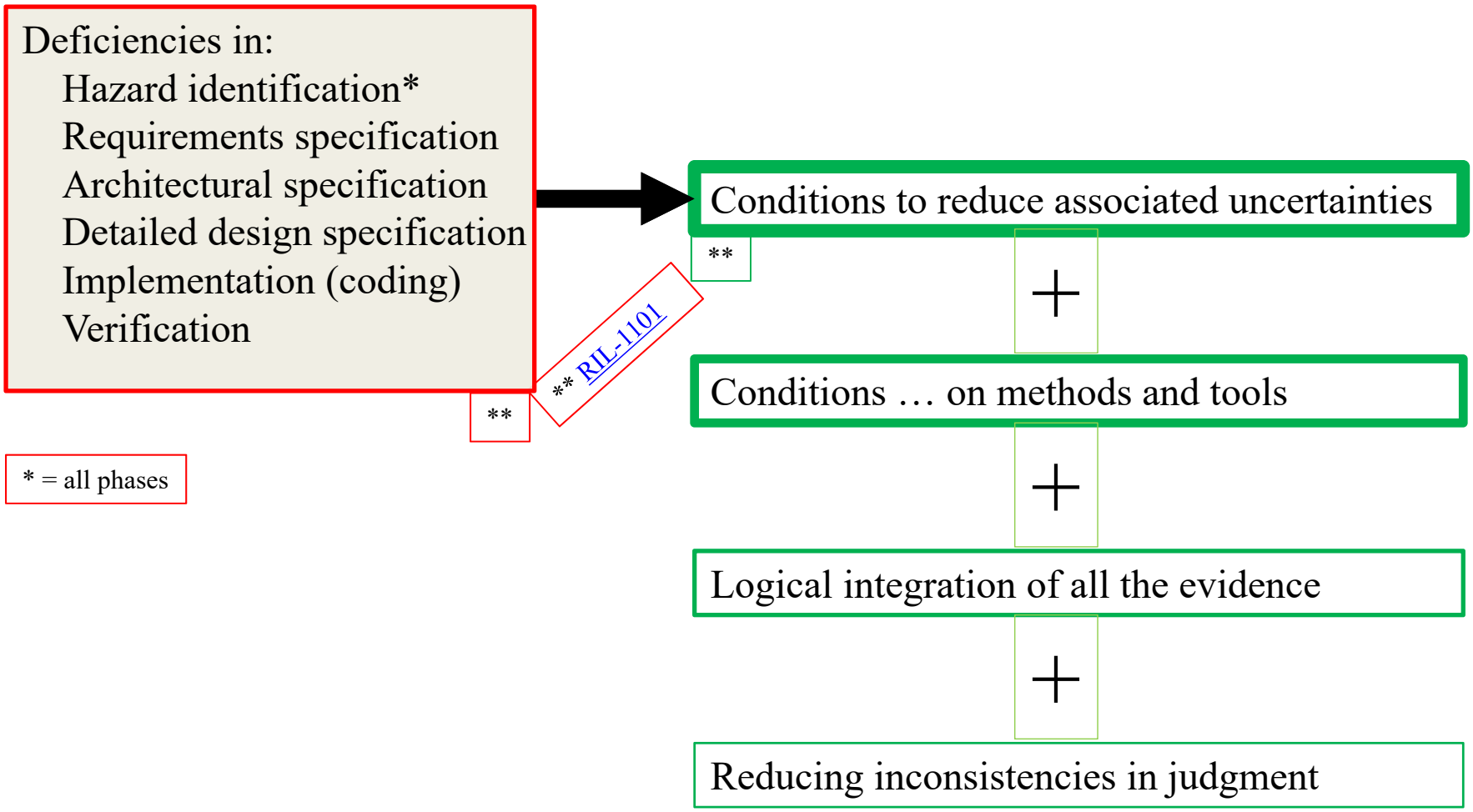


U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

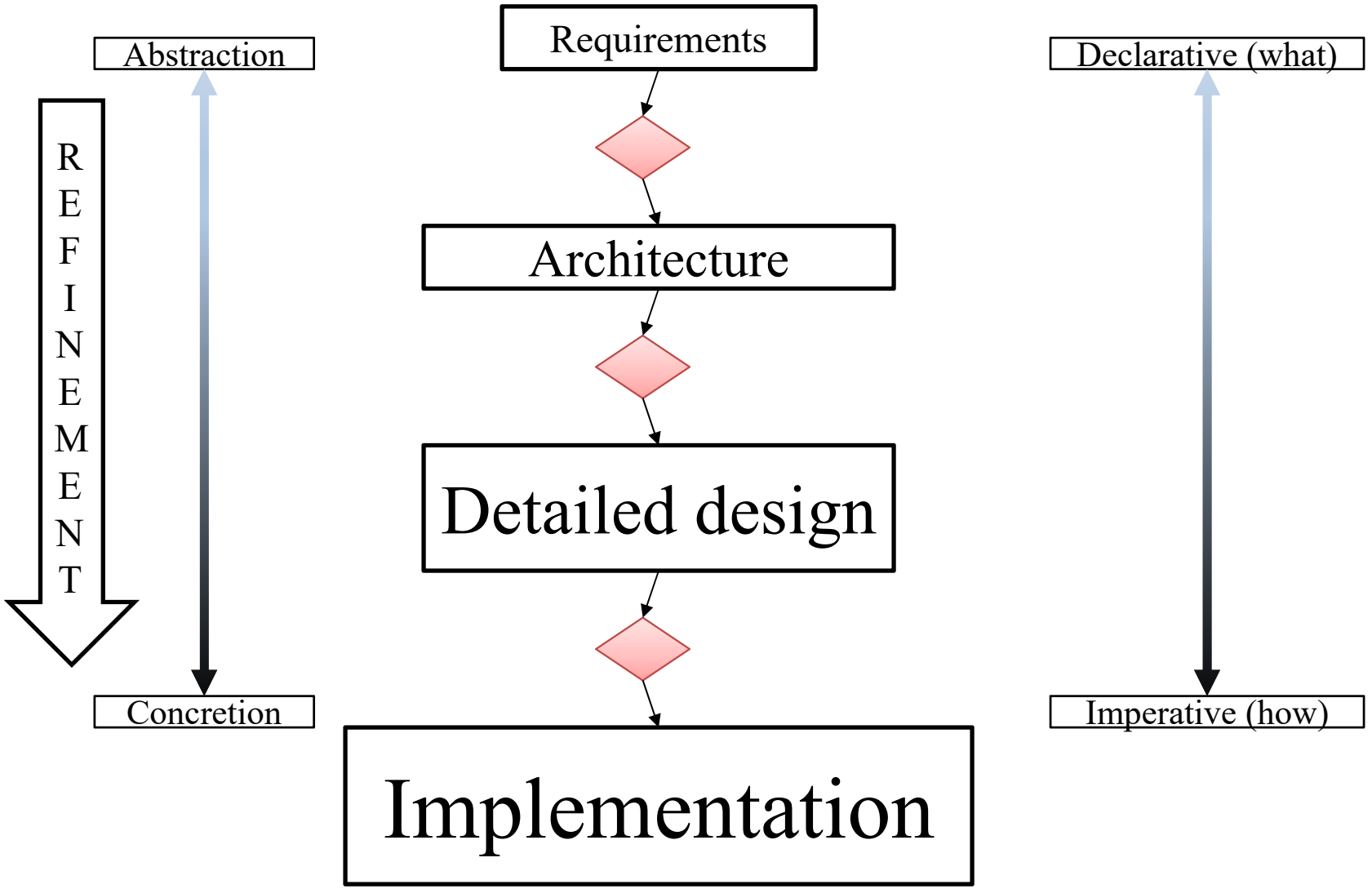
Creating the appropriate standards: One vision



Research to reduce the uncertainty space

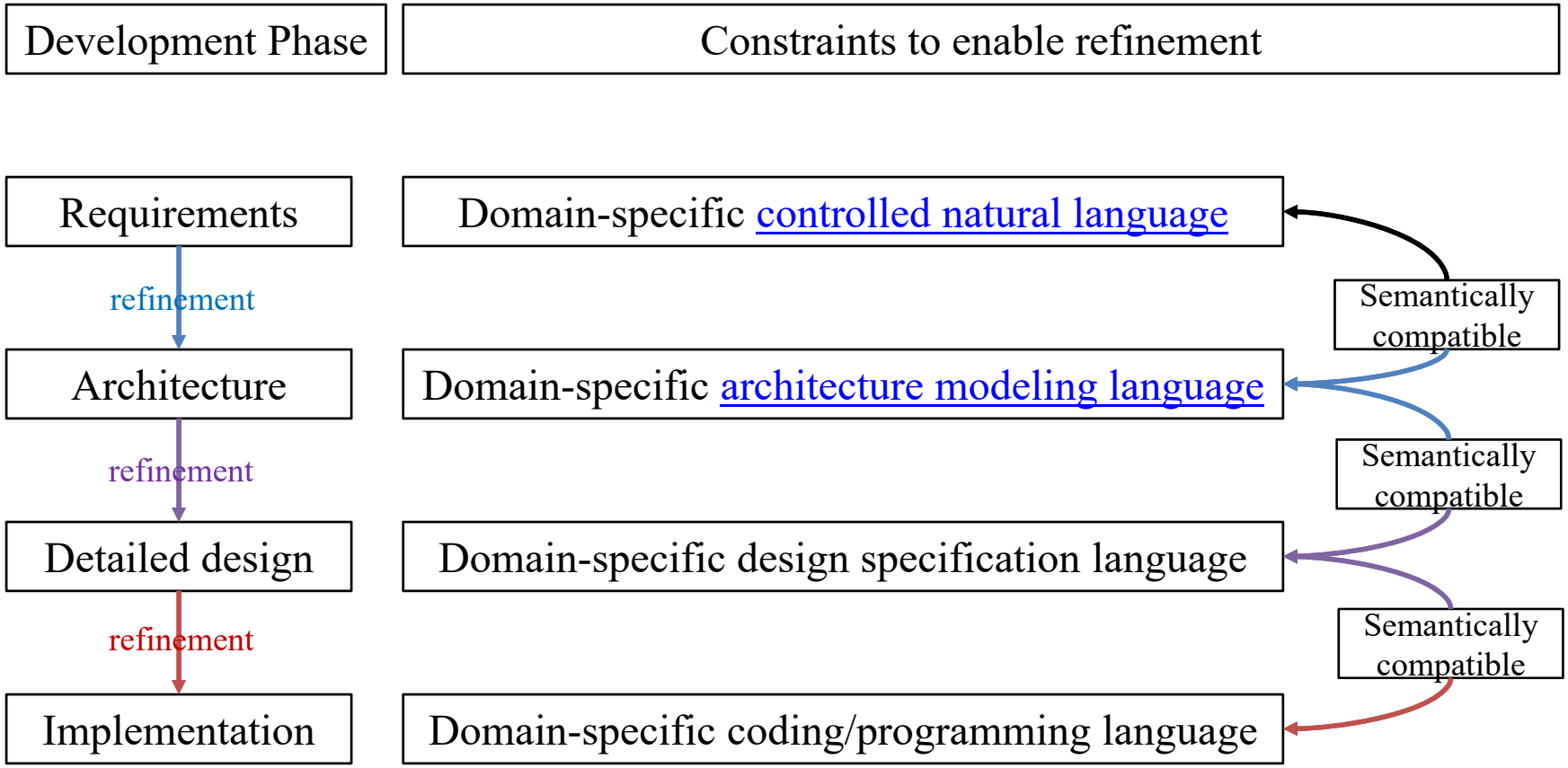


Defect-prevention through Refinement



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

Leverage domain engineering



Create pre-certified reusable assets

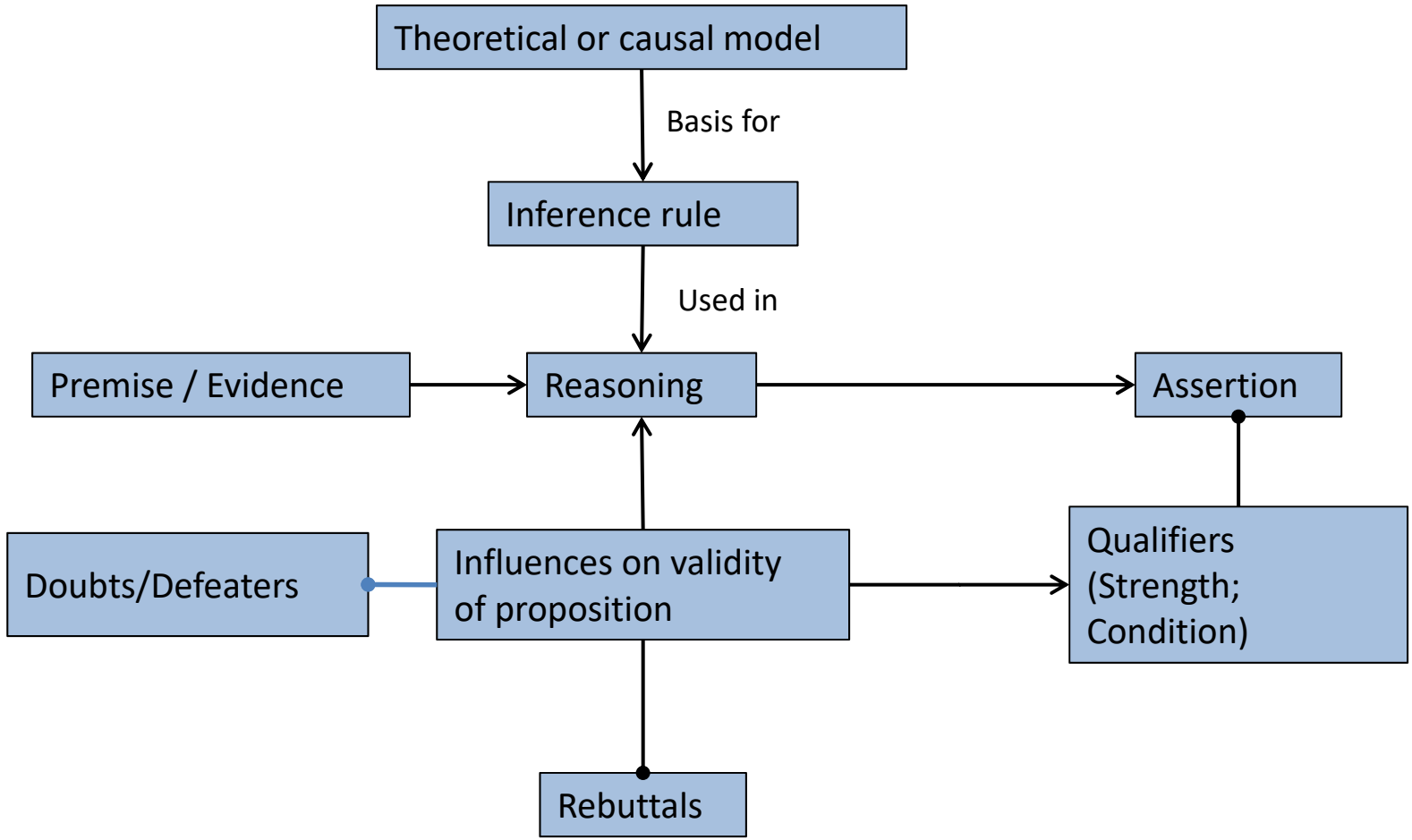
- Domain modeling
- Domain engineering

(see NUREG/CR-6263; IEEE Std 1517:2010; ISO/IEC 26550)

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

Reasoning Model to support performance-based evaluation

(based on the Toulmin model[1])



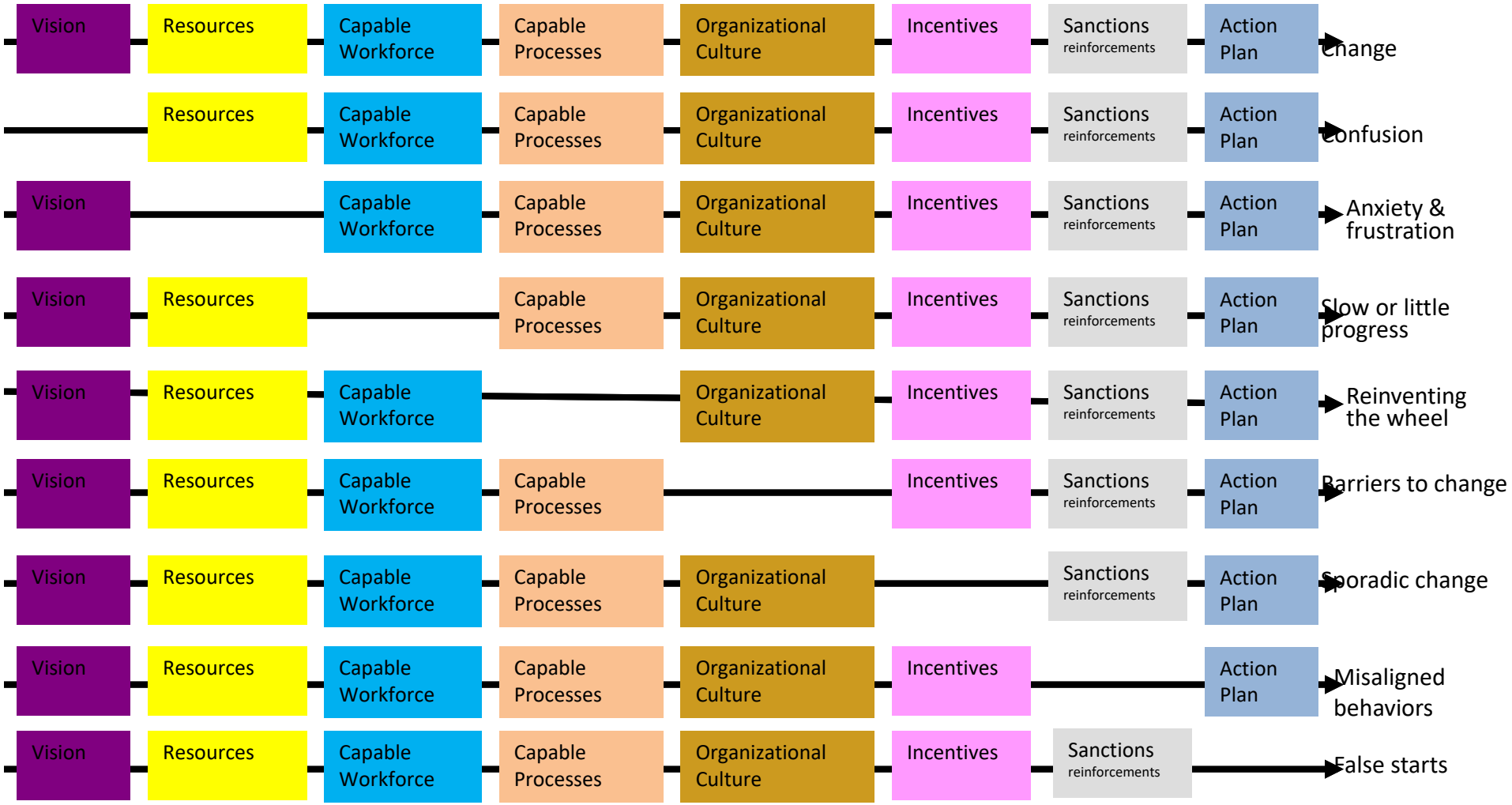
[1]Toulmin, S., The Uses of Argument, Cambridge, UK: Cambridge University Press, 1958

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

Some known technical limitations

- Validating results of hazard analysis
  - Did it really identify all causes that could degrade the safety function?
- Validating assumptions about the environment of the safety system, e.g.:
  - Conditions of operation and maintenance
  - Configuration control → change impact analysis
- Qualifying suite of tools from different sources
  - Libraries
  - Underlying languages
- Infrastructure for independent V&V

Why holistic? Effects of Missing Elements of Change



Adapted by Dr. Palma Buttles-Valdez, SEI from: Delorise Ambrose, 1987

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

Acronyms & Abbreviations 1/2

AADL	Architecture Analysis and Design Language
CCF	Common cause failure
Dev	Development
Engrg	Engineering
DI&C	Digital Instrumentation and Control
EPRI	Electrical Power Research Institute
esp.	Especially
FSM	Finite state machine
HA_p	Hazard analysis of plans
HA_r	Hazard analysis of requirements
HA_a	Hazard analysis of architecture
HA_{dd}	Hazard analysis of detailed design
HA_i	Hazard analysis of implementation
HA_t	Hazard analysis of testing (including test specifications and oracles)
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
IV&V	Independent Verification and Validation
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
OWL	Web Ontology Language
RIL	Research Information Letter
RPS	Reactor Protection System
RWI	Review, Walkthrough, and Inspection

Acronyms & Abbreviations 2/2

R&D	Research and Development
Reqmts	Requirements
RIL	Research Information Letter
RPS	Reactor Protection System
SCR	Software Cost Reduction (set of techniques for designing software systems)
spec	specification
SQuaRE	Systems and Software Quality Requirements and Evaluation
STPA	System Theoretic Process Analysis (method of hazard analysis)
Std	Standard
V&V	Verification and Validation
V_p	V&V of plans
V_r	V&V of requirements
V_a	V&V of architecture
V_{dd}	V&V of detailed design
V_i	V&V of implementation
V_t	V&V of testing (including test specifications and oracles)