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

DI&C systems safety demonstration framework research planned

Software Certification Consortium
November 11, 2011

Sushil Birla
Division of Engineering
Office of Nuclear Regulatory Research
(301-251-7660, Sushil.Birla@nrc.gov)

Safety demonstration framework

Approach to evaluate integrated effect of known uncertainties

- Structured argument integrating complementary evidence items
- Shows how safety goals are met despite presence of uncertainties
- Makes explicit the impact of known uncertainties

Some issues to be addressed

Typical safety review in current practice

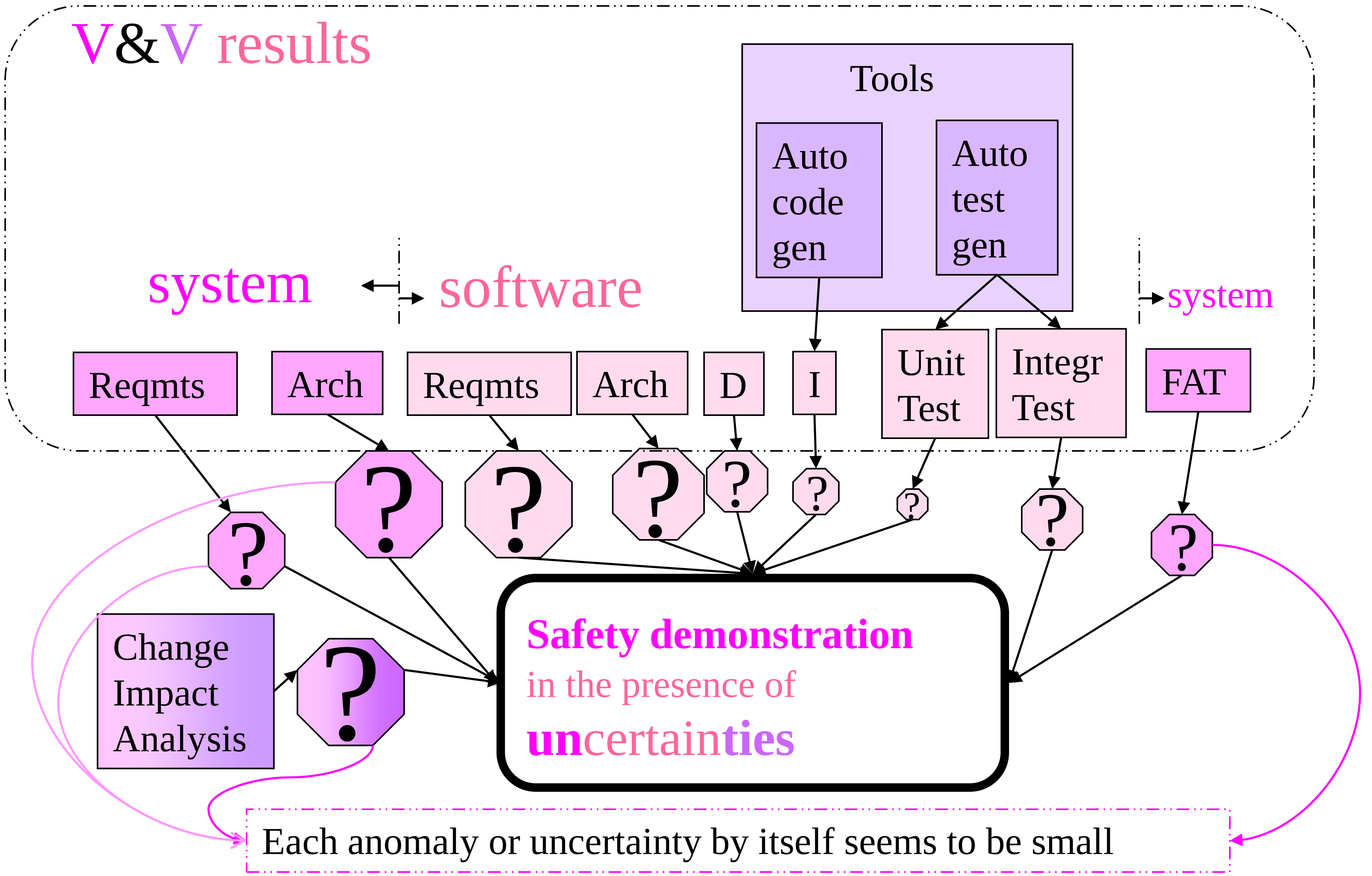
- Checks against requirements and guidelines clause by clause (or item by item)
- Applies judgment to decide about effect of any deviation item by item
- Issue: Individual deviation items are often inter-dependent; combined effect unclear

Some “complaints” about current safety case practice

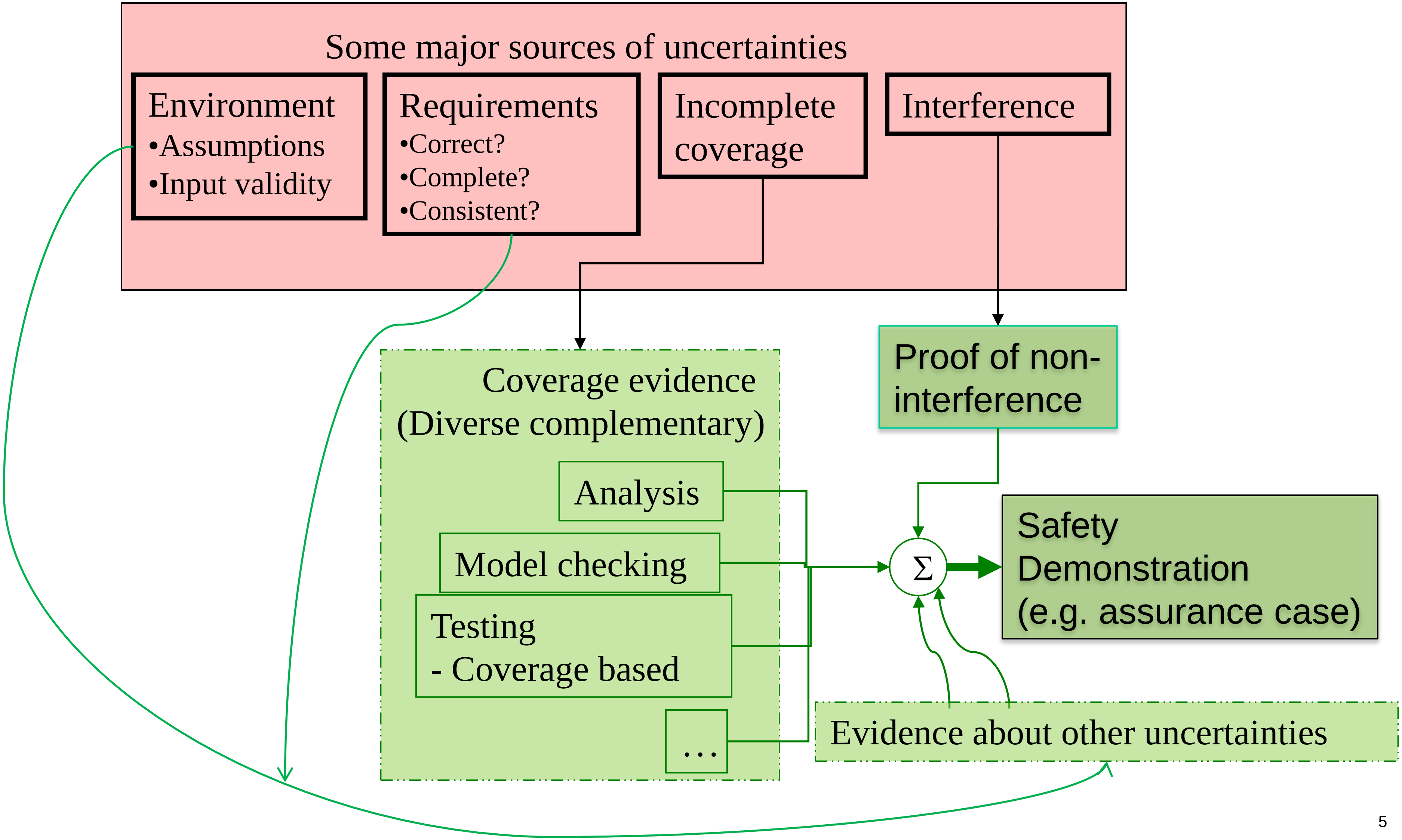
- “Merely boiler plate” – not useful (Nimrod Report)
- Too voluminous to be comprehensible (Nimrod Report)
- Sometimes a “safety case” is used in lieu of good quality evidence
- Analyzed design does not reflect actual run-time behavior, e.g. fault propagation paths
- Arguments connecting claims and evidence may contain logical fallacies
- Current mathematical logic (as in GSN) does not support the qualitative reasoning needed
- Inadequate scientific foundation to integrate effects of uncertainties on overall safety

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

Integrating effect of uncertainties in software assurance



V&V Uncertainties: Evidence needed



Some major sources of uncertainties

Environment
- Assumptions
- Input validity

Requirements
- Correct?
- Complete?
- Consistent?

Incomplete coverage

Interference

Coverage evidence (Diverse complementary)

Analysis

Model checking

Testing
- Coverage based

…

Proof of non-interference

Σ

Safety Demonstration (e.g. assurance case)

Evidence about other uncertainties

Experts' recommendations to NRC: What to look for

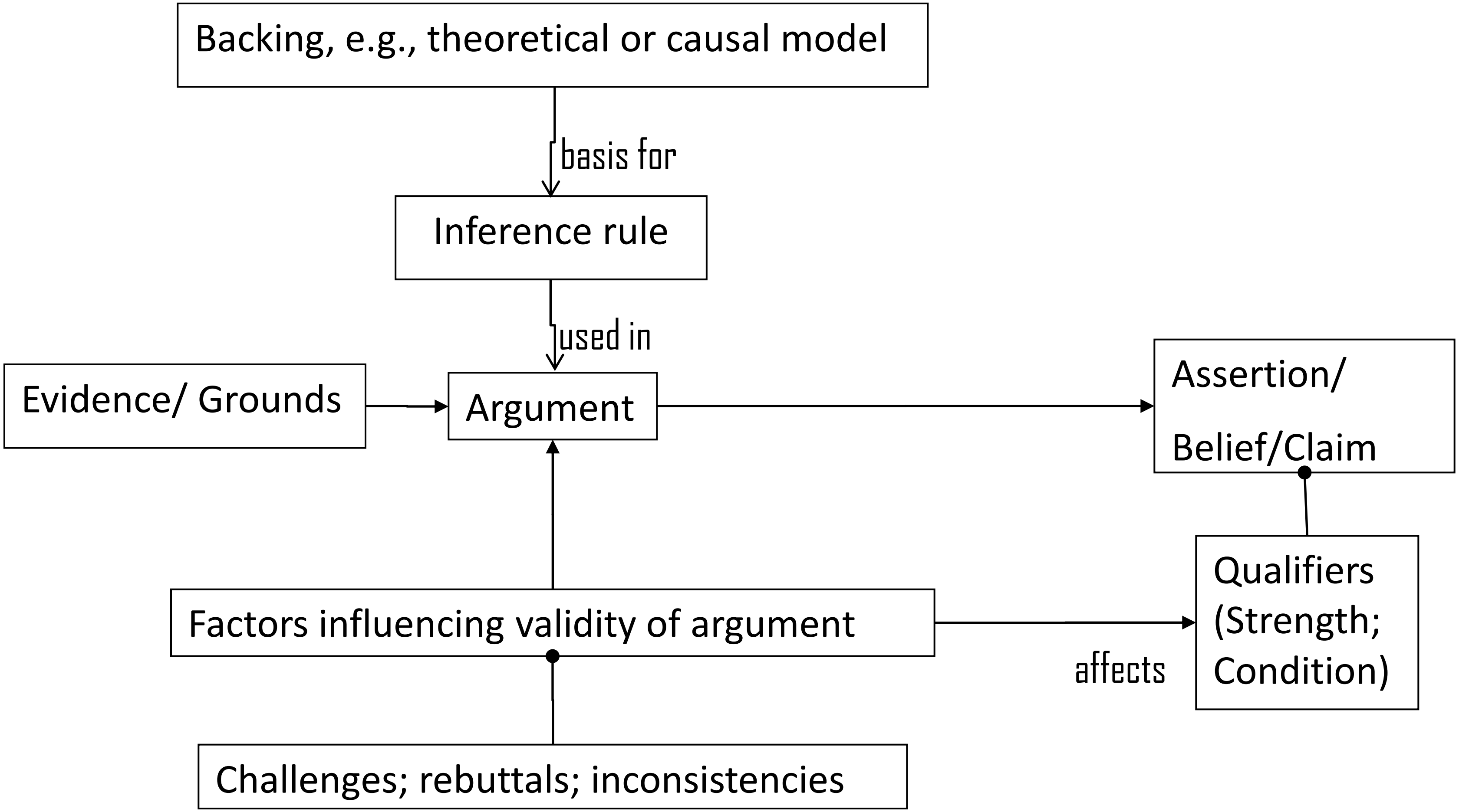
Safety demonstration should include the following:

- **Diverse, complementary evidence**
- **Explicit evaluation of sufficiency of evidence and argument to expose weaknesses, fallacies, and limitations**
- **Explicit reasoning about uncertainties in the evidence and how these have been managed and mitigated**
- **Evidence that the rigor in analysis and proof is commensurate with the strength of the claim made**
- **Explicit identification of system aspects, features, characteristics, or other items or of process activities or competencies upon which the safety argument depends**
- **Modular structure with modular evidence**

Experts' recommendations to NRC: How to improve evaluation process

- **Understanding, principles and techniques drawn from other fields, e.g., philosophy, law, linguistics for evaluating the quality of arguments and evidence**
  - **Strive for a scientific foundation, e.g., devise a calculus for reasoning about:**
    - **Uncertainties**
    - **Degrees of validity**
    - **Degrees of confidence**
- **Understanding of the limitations in evidence and how to combine different types of evidence such as testing, model-checking and analysis, including a theory of coverage**
- **Understanding of where in a process uncertainties can arise (e.g., when creators of the architecture misunderstand the requirements)**
- **Integrating the contribution of interdependent factors, such as the complexity⬄competence nexus**
- **Learning more about the specific limitations or conditions experienced in licensing reviews, including:**
  - **Review of safety cases and assurance cases, where available**
  - **Review of operational experience**

Adaptation from Toulmin’s model



Backing, e.g., theoretical or causal model

basis for

Inference rule

used in

Evidence/ Grounds

Argument

Assertion/ Belief/Claim

Factors influencing validity of argument

affects

Qualifiers (Strength; Condition)

Challenges; rebuttals; inconsistencies

Exploring research collaboration

- **Exchange lessons learned**
  - **Licensing reviews**
  - **Operating experience**
- **Share information available on actual safety cases**
- **Share information on related research activities**
- **Seek common understanding on:**
  - **Knowledge gaps (research needs)**
  - **Their relative contribution or impact**
- **Identify leading sources of knowledge**

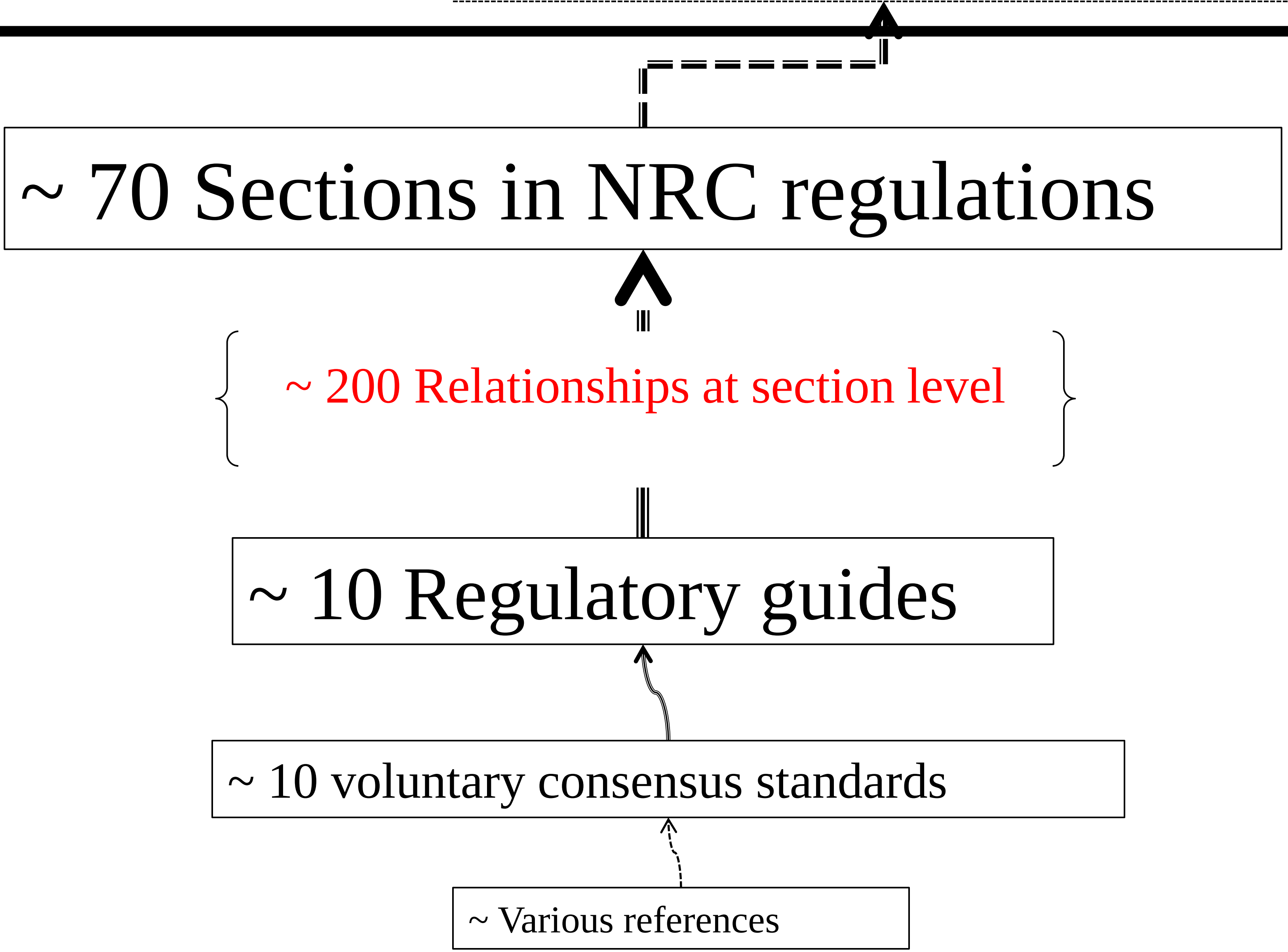
NRC Request for Information (RFI)

Request for Information (RFI): A mechanism to find interested, knowledgeable parties

- **Seven responses received:**
  - **Outside USA: Belgium, Canada, United Kingdom**
  - **Inside USA: Government agencies, private companies, universities**
- **Potential NRC follow-up:**
  - **Request for Proposal in FY 2012**
  - **Contract award in FY2013**

BACKUP SLIDES

DI&C Assurance



~ 70 Sections in NRC regulations

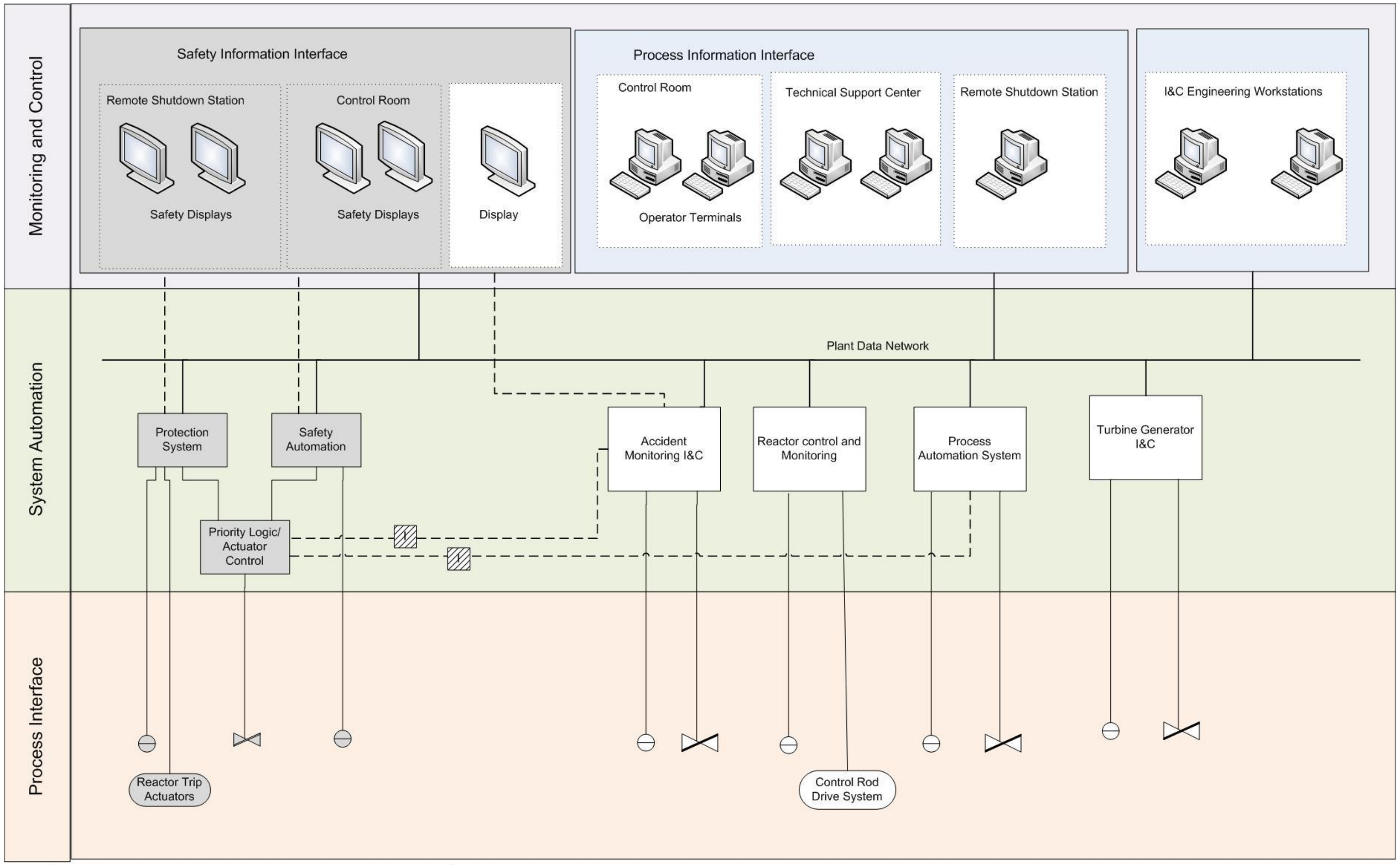
~ 200 Relationships at section level

~ 10 Regulatory guides

~ 10 voluntary consensus standards

~ Various references

System complexity



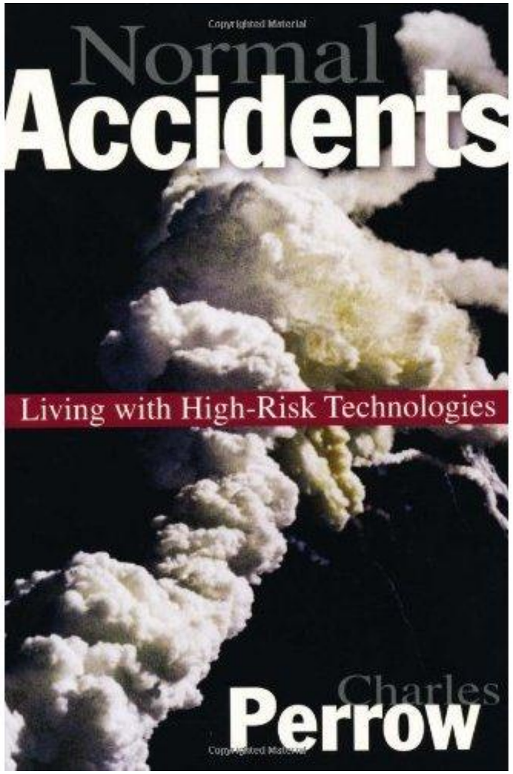
NOTE

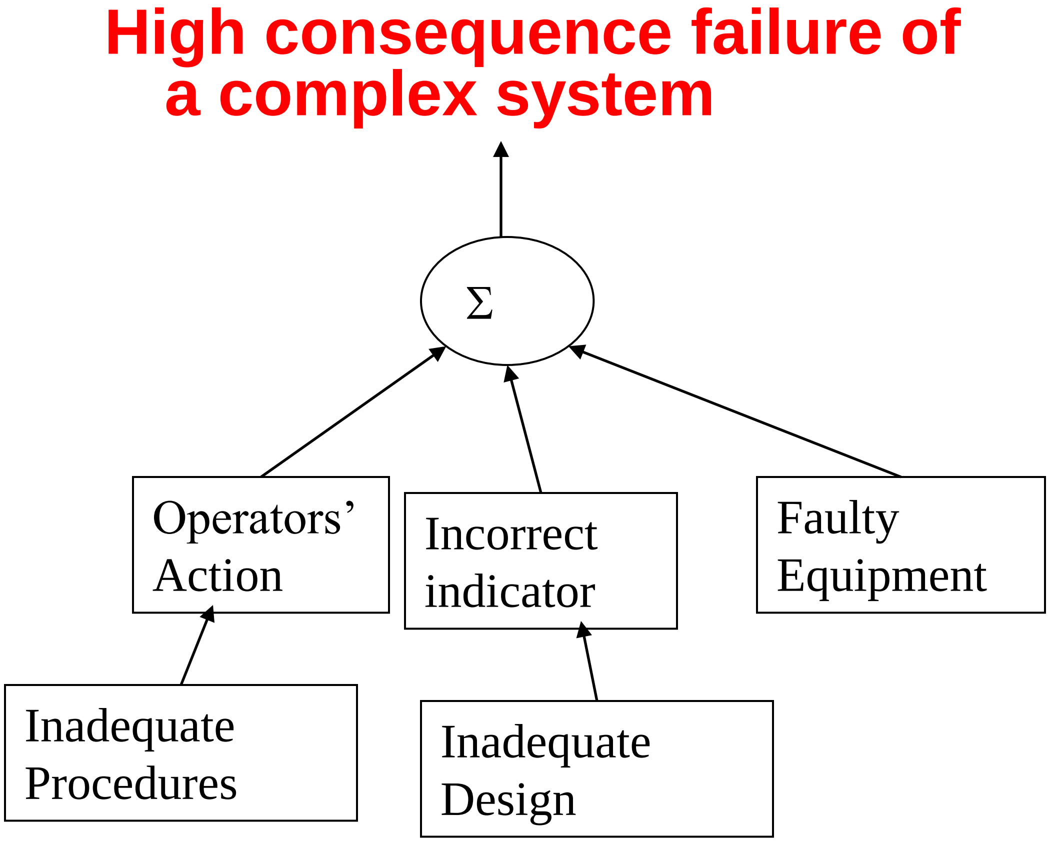
▨ Shaded items are safety related equipment

□ Unshaded items are non-safety related equipment

▨ Safety isolation barrier

Combined effects of seemingly insignificant deviations





High consequence failure of a complex system

Σ

Operators' Action

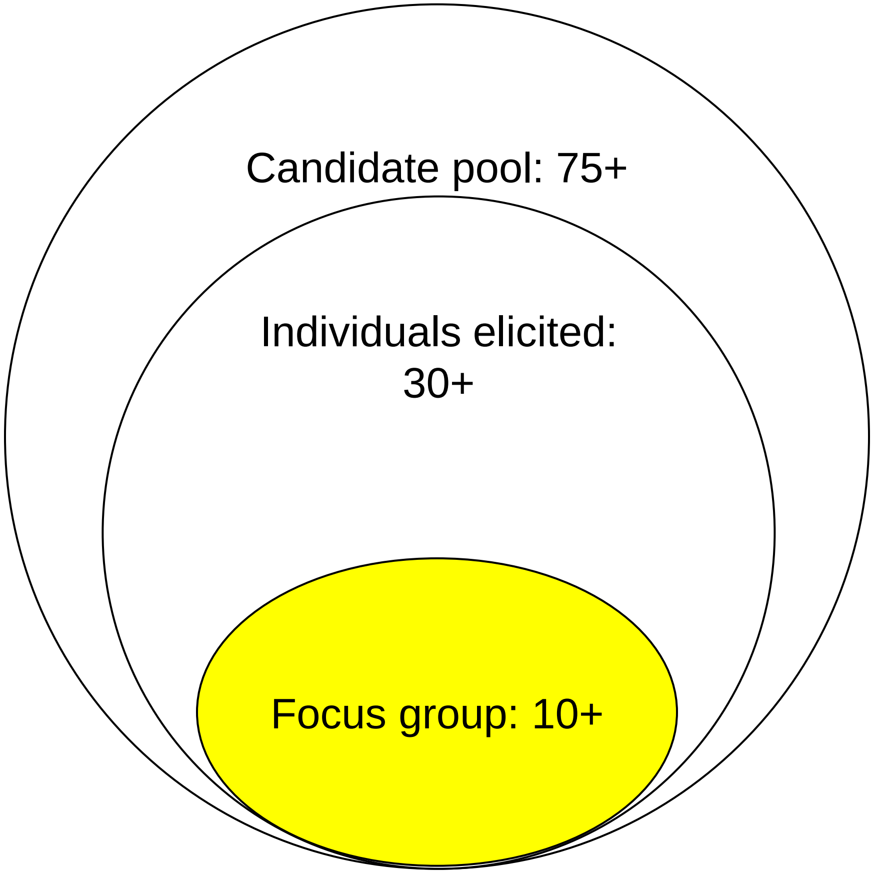
Incorrect indicator

Faulty Equipment

Inadequate Procedures

Inadequate Design

Engagement of experts

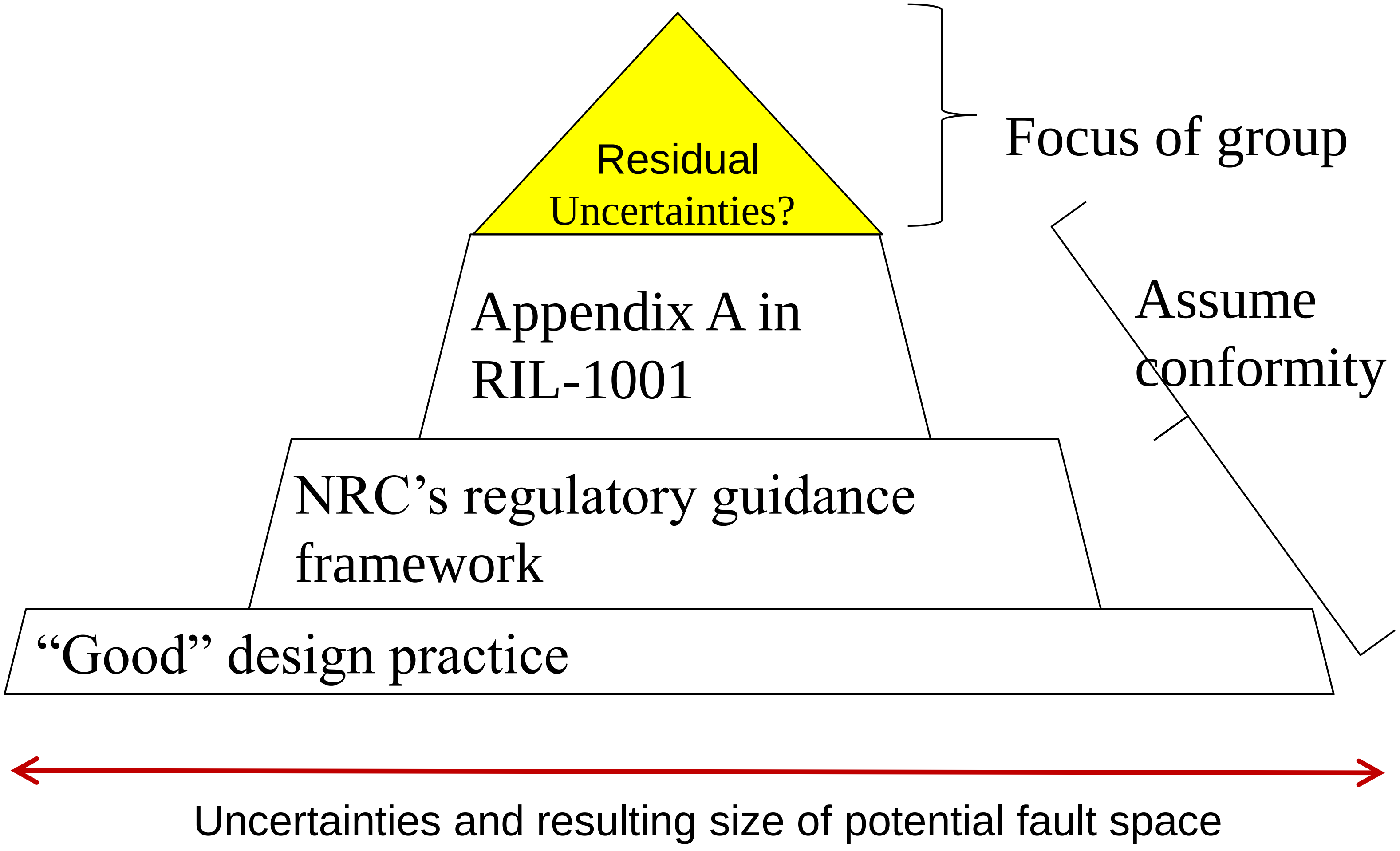


Candidate pool: 75+

Individuals elicited: 30+

Focus group: 10+

Starting point given to focus group


Residual Uncertainties?
Focus of group
Appendix A in RIL-1001
Assume conformity
NRC's regulatory guidance framework
"Good" design practice
Uncertainties and resulting size of potential fault space