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

Identifying Hazards from Engineering Digital I&C Systems: State of the Art

July 27, 2023
Halden (HTO) Workshop:
Modern Hazard Analysis for Safety Assurance

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

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

Objective

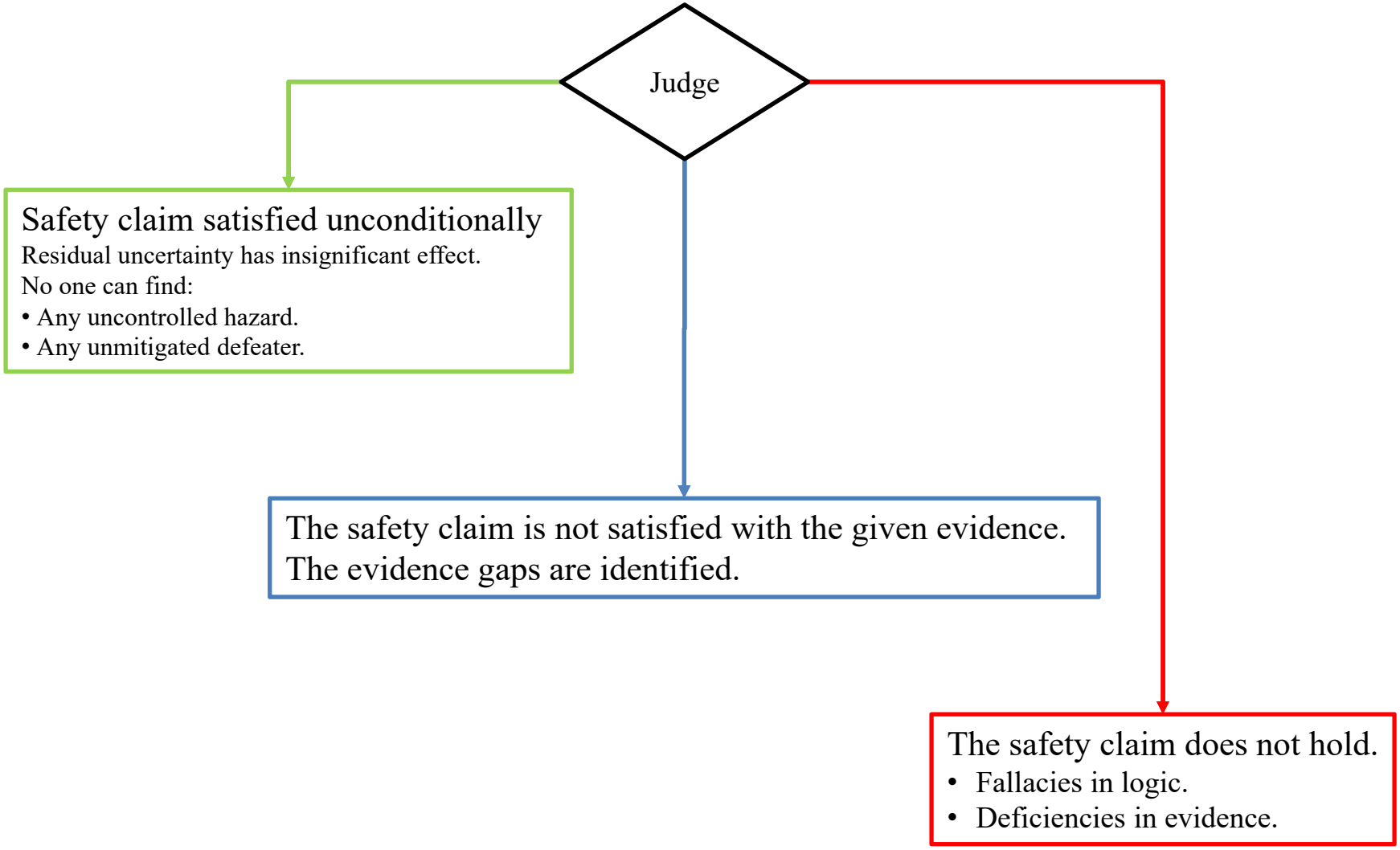
Assess through discussion:

1. Can the state-of-the-art techniques identify all significant hazards in the design of a cyber-physical system as simple as a nuclear reactor protection system?

2. If not:
    1. Limitations?
    2. Promising directions to overcome these limitations?

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

Insignificant: Support consistent judgment



State-of-the-art: Meaning

State-of-the-art

Capability demonstrated in leading-edge implementations.

- Not yet scaled up.

State-of-the-practice

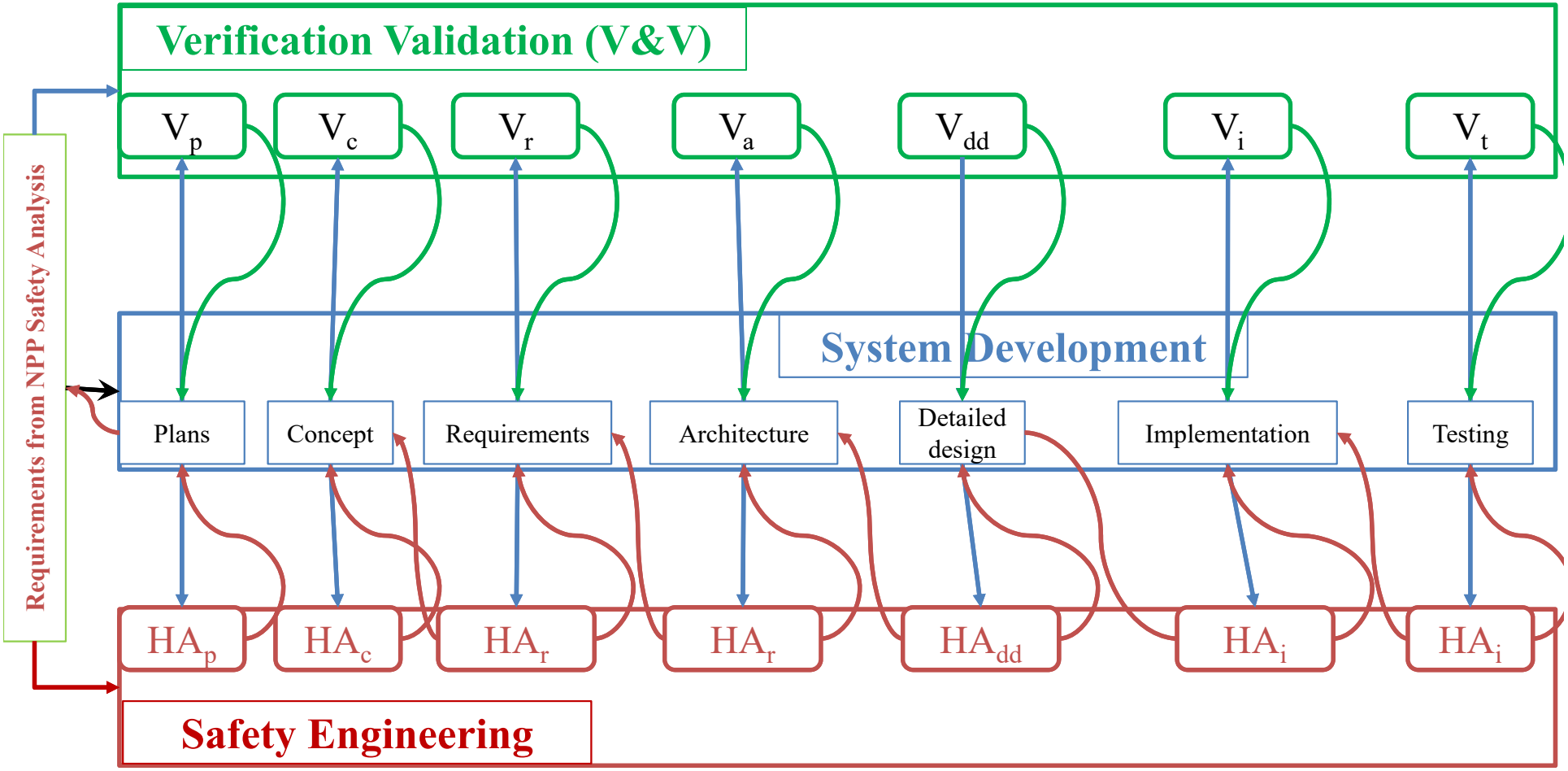
Best-in-class; best practices, e.g.:
as seen in leading-edge industry consensus standards

Current practice

Prolific in many organizations

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

Reference Framework



Adapted from IEEE Std 1012

Acronyms

- 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)
- IEEE – Institute of Electrical and Electronics Engineers
- NPP – Nuclear Power Plant
- NRC – U.S. Nuclear Regulatory Commission
- 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)