HESTIA: High-level and Extensible System for Training and Infrastructure risk Assessment

Ananth A. Jillepalli, University of Idaho

Introduction – Transition

- Transition of Industrial Control Systems (ICS) into Cyber Physical Control Systems (CPCS).
  - Digital / analog equipment of ICS is being replaced by cyber-enabled equipment.

Introduction – New Vector of Vulnerabilities

- Increased connectivity of CPCS to the internet.
- Open-source applications are purchased commercially off-the-shelf (COTS), without consideration of applying current standard patches.

Introduction – Change in Attack Framework

- Until recently, CPCS attacks originated from an insider threat.
- In the recent years, attacks originating from outside are becoming frequent.

Introduction – Financial Impact

- Cyber-attacks on CPCS are occurring at an ever-increasing rate, incurring financial loss to both governments and industries.
- Estimates project losses as high as $1.87 billion by 2018, due to cyber-attacks on CPCS infrastructure.

Problem – Identifying Vulnerabilities

- For a Chief Security Officer (CSO):
- Identifying vulnerabilities specific to a particular CPCS infrastructure can be a challenge, if there is no high-level security policy specification.

Problem – Designing best hardening strategy

- Obtaining the high-level security policy specification of the existing CPCS state is not sufficient by itself.
- A CSO should be able to design the best hardening strategy for their particular CPCS system.

Problem – Designing best hardening strategy

- Obtaining the high-level security policy specification of the existing CPCS state is not sufficient by itself.
- A CSO should be able to design the best hardening strategy for their particular CPCS system.

Problem – Required Investigation

- Such a design process includes investigating:
  - “where to best use defense resources, which parts to harden, and in which particular order?”

Problem – Investigation Factors

- Several factors come into play:
  - Completeness and consistency of the CPCS infrastructure policies;
  - Likeliness of attacks and respective defenses against the particular system;
  - Overall cost of possible attacks versus overall cost of possible defenses.
    - Overall cost = Time and money.

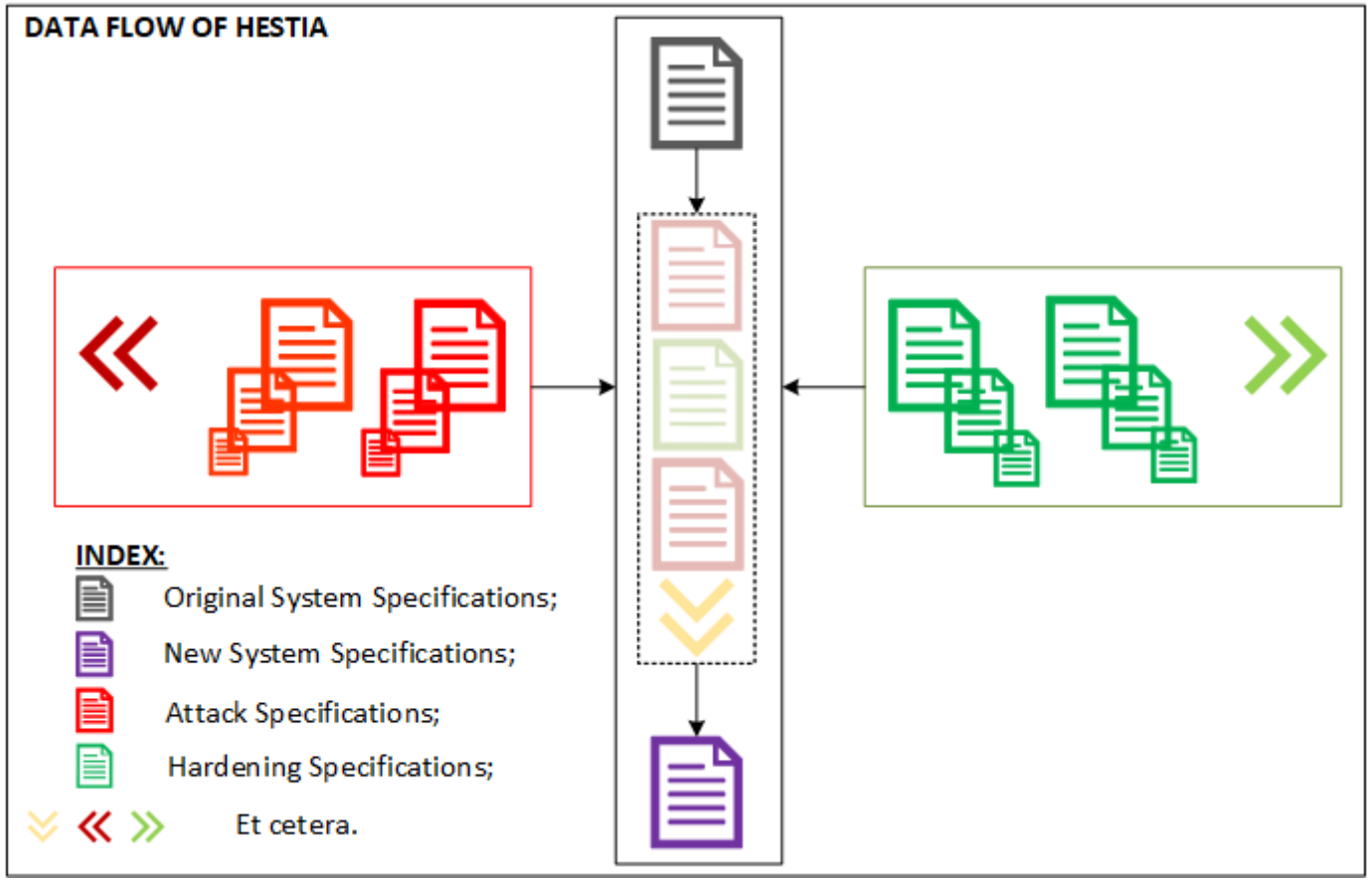
Problem – Investigation Factors

- Several factors come into play:
  - Completeness and consistency of the CPCS infrastructure policies;
  - Likeliness of attacks and respective defenses against the particular system;
  - Overall cost of possible attacks versus overall cost of possible defenses.
    - Overall cost = Time and money.

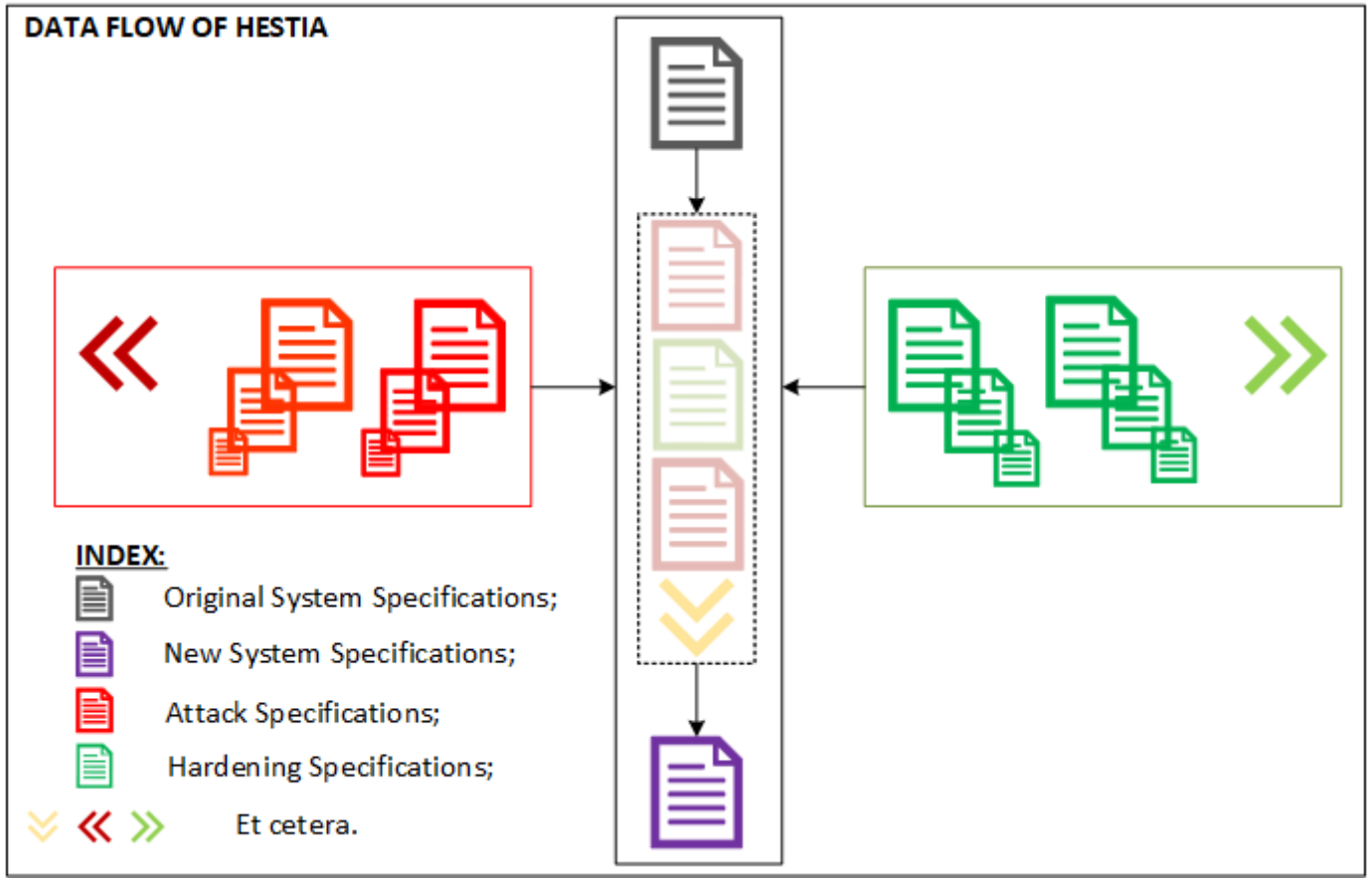
Proposed Solution – HESTIA

- HESTIA: High-level and Extensible System for Training and Infrastructure risk Assessment.
  - Work in progress.

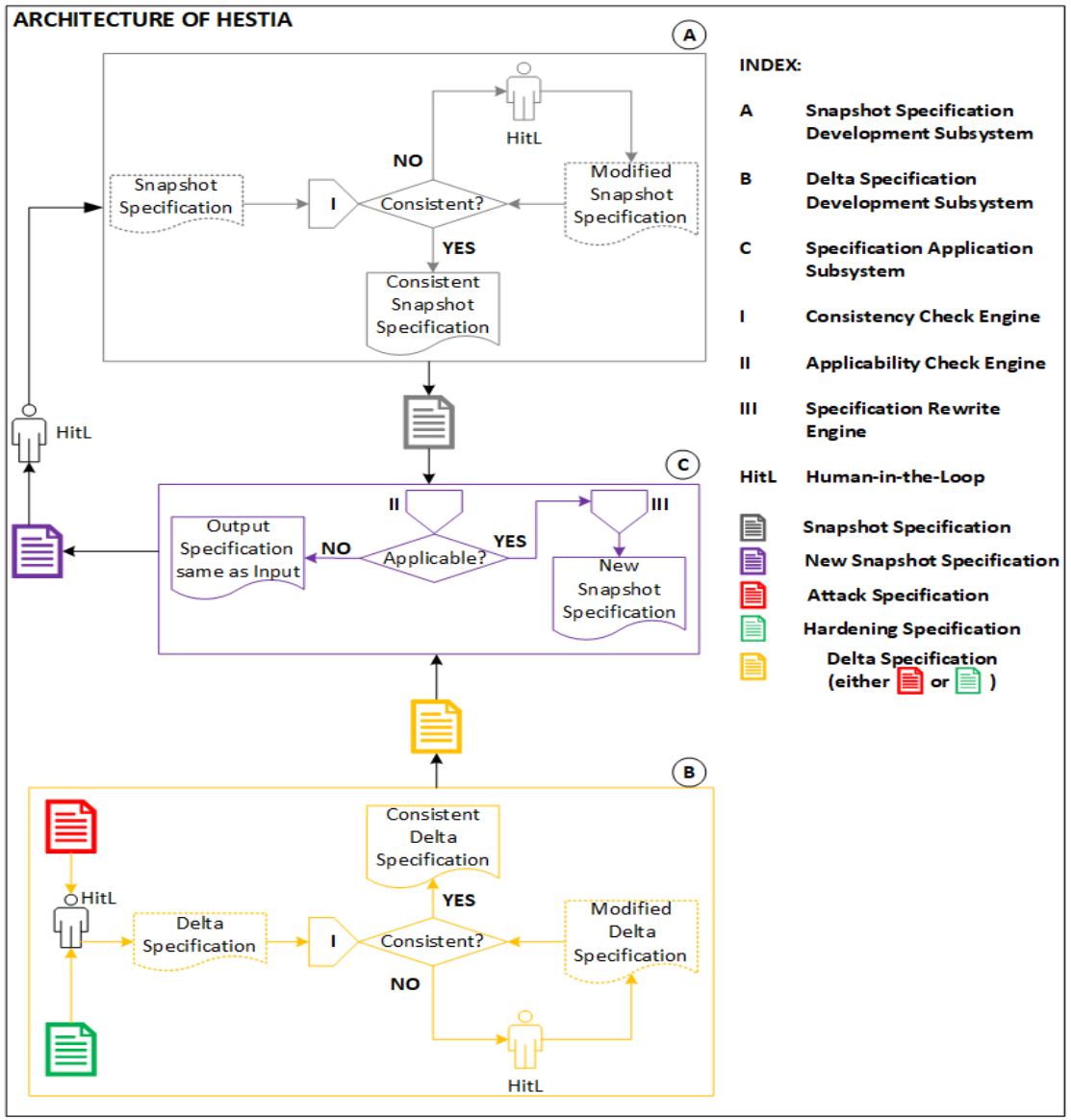
Data Flow of HESTIA



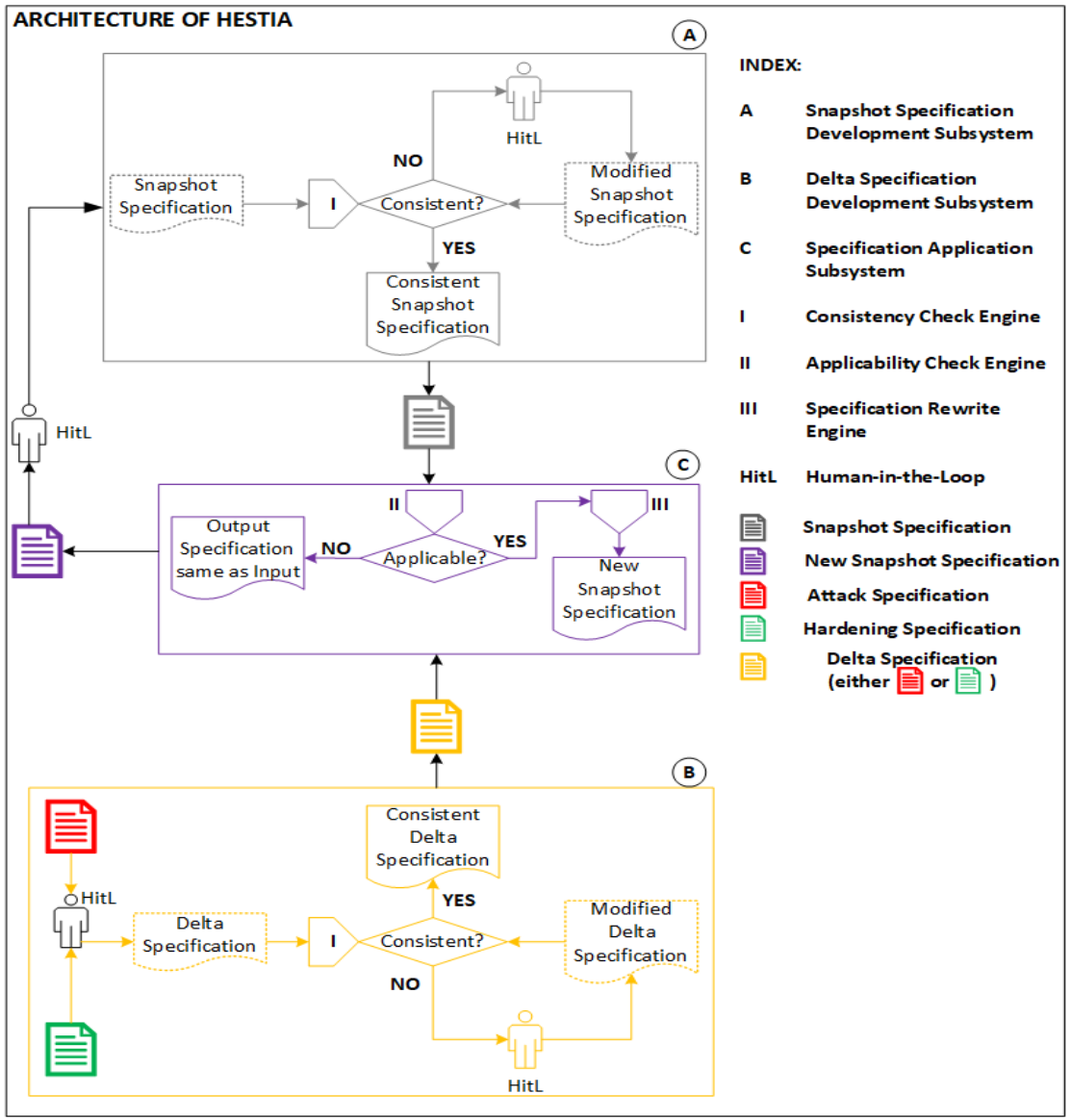
Data Flow of HESTIA



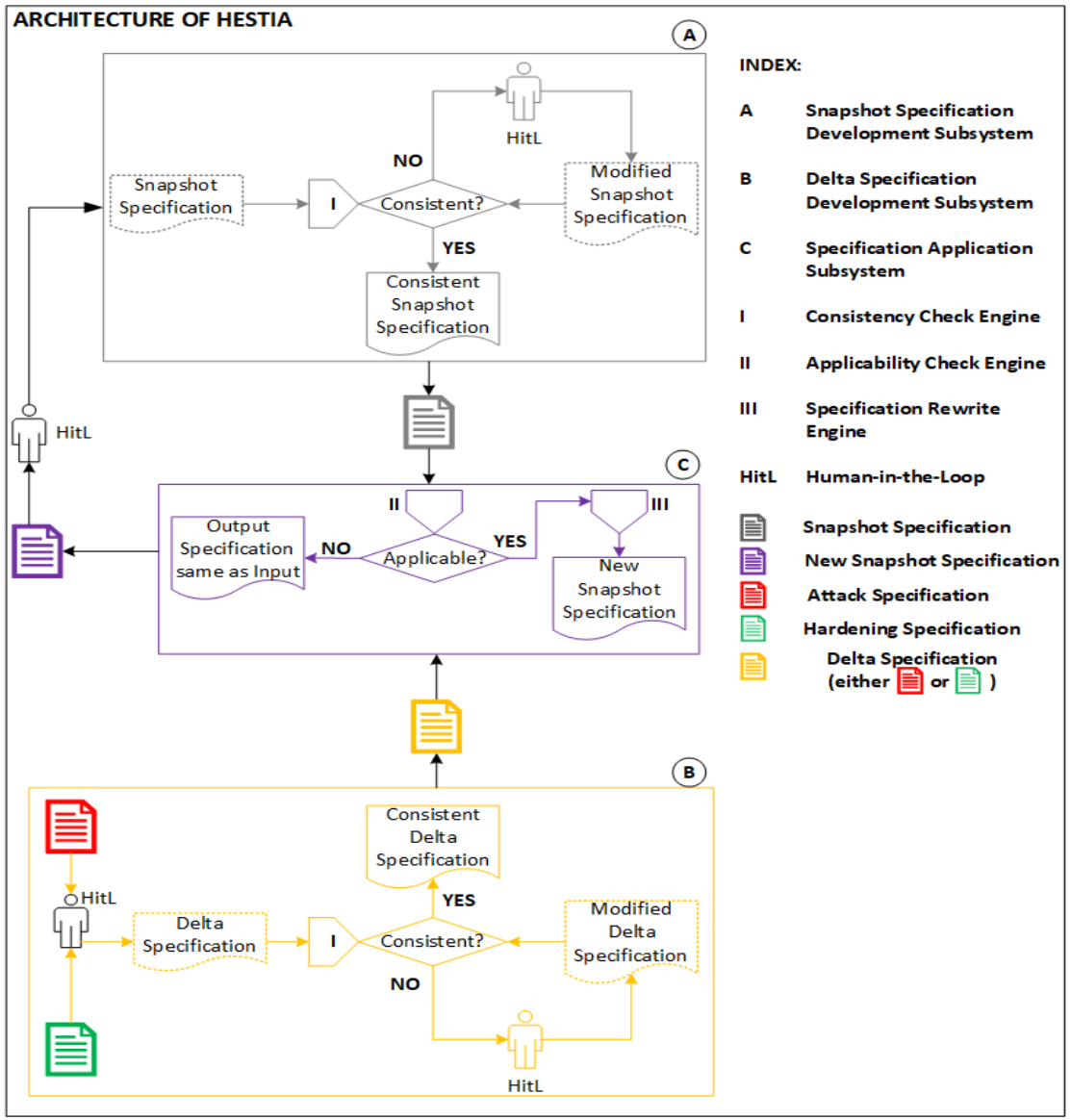
Architecture of HESTIA



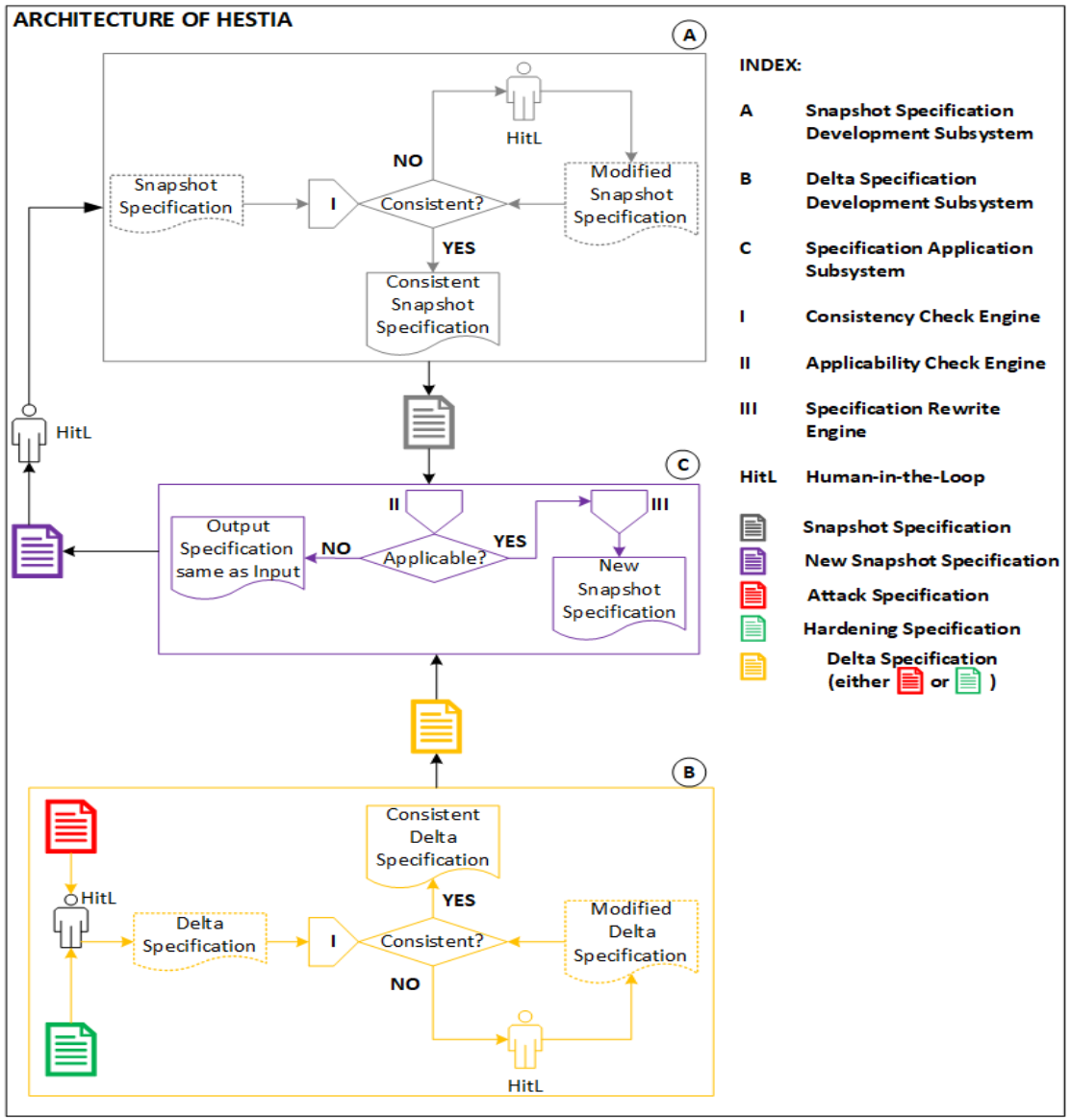
Architecture of HESTIA



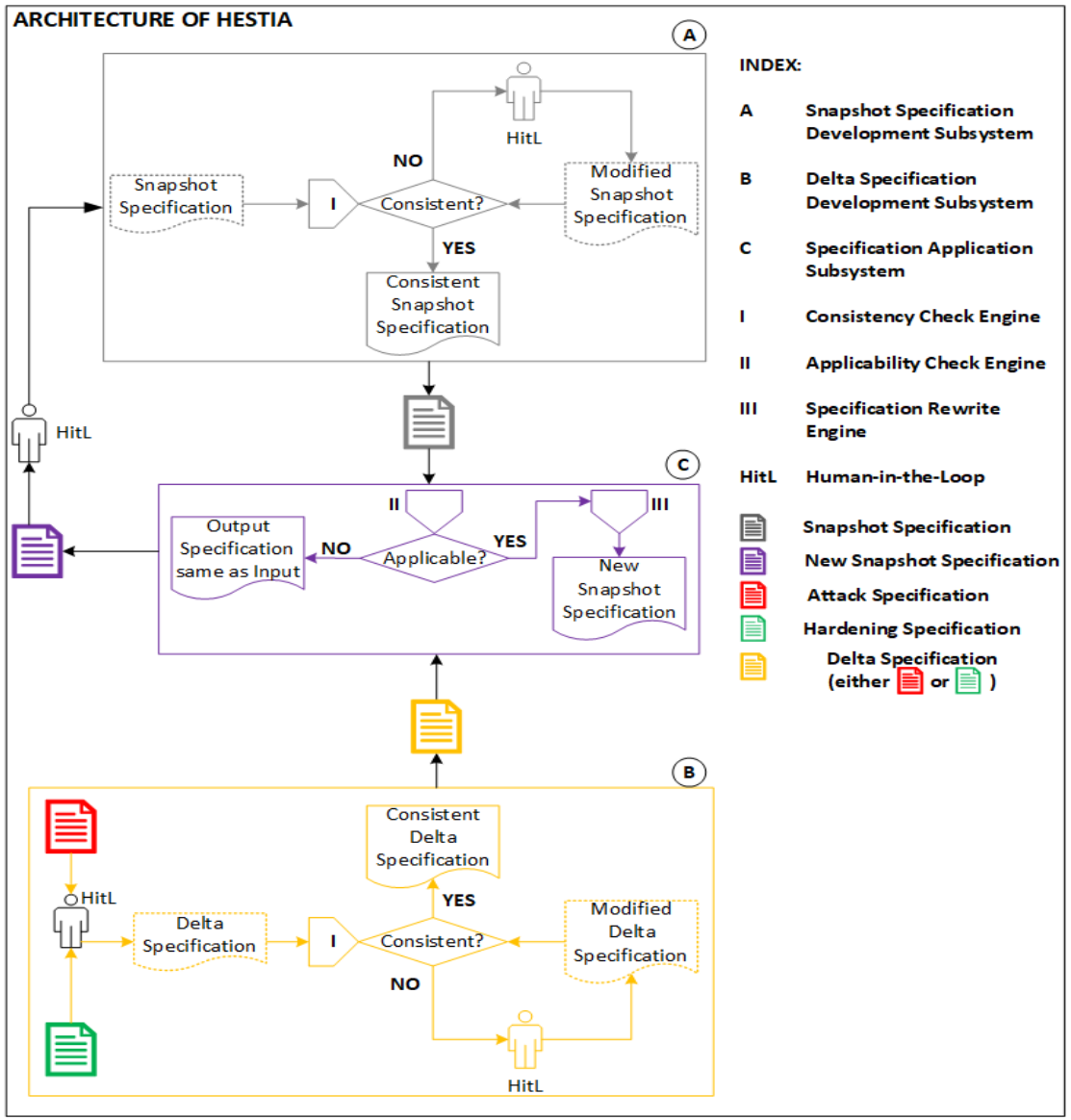
Architecture of HESTIA



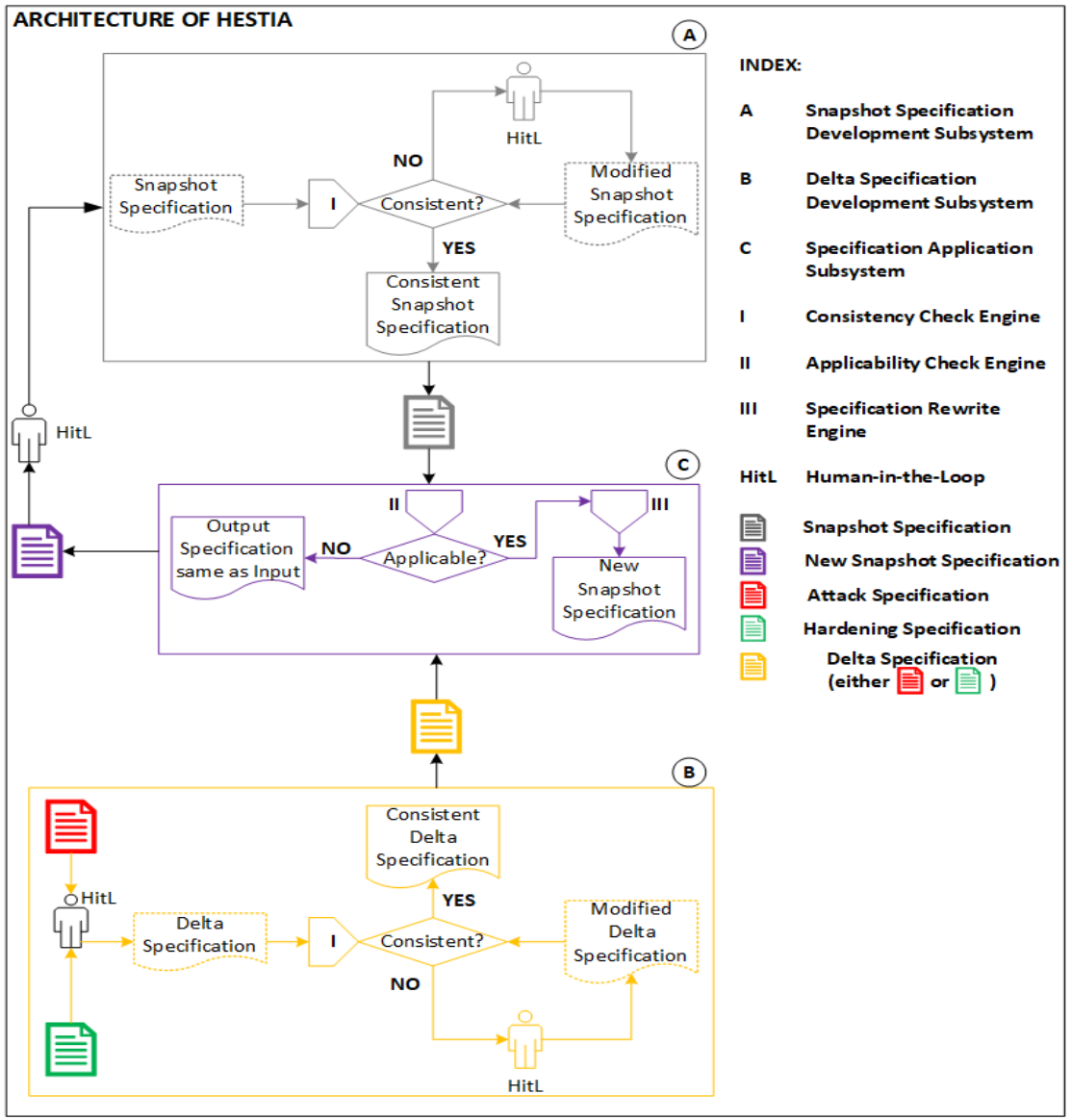
Architecture of HESTIA



Architecture of HESTIA



Architecture of HESTIA



Current Research Status and Conclusion

- Developed a specification language called HERMES.
  - In process to develop the ‘Consistency check engine’.
- We hope that this endeavor will contribute to solving the problem of enabling a CSO to design the best hardening strategy.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security