On Understanding and Contrasting Certification Review Processes for Software and Hardware Components: An Industrial Case Study

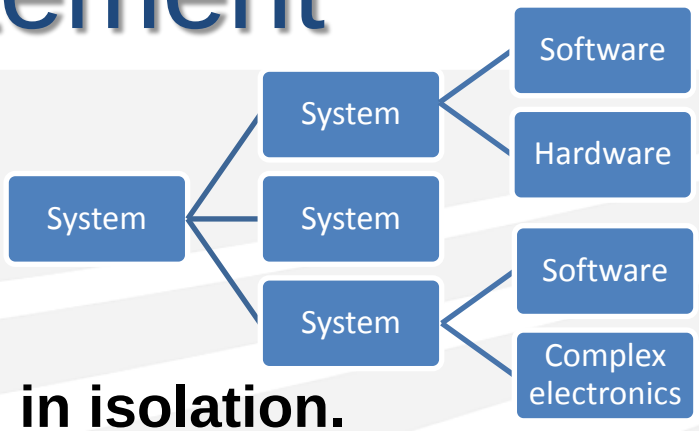
NDIA 2012

Madeline Diep, Forrest Shull, and Carolyn Seaman*
Fraunhofer Center for Experimental Software Engineering
**Department of Information Systems, UMBC, Baltimore, MD*

Fraunhofer USA
Center for Experimental Software Engineering

Problem Statement

- System development is often decomposed to handle complexity.



- Assurance activities often conducted **in isolation.**
  - Can allow a slippage of interface defects.
  - Software is increasingly more prevalent and more embedded in system
    - Research on system hazard analysis revealed that 51% of the hazards contained at least one software cause [Basili et al.].
    - Assuring system quality depends on a wide variety of domain expertise.
  - Missed opportunity from not being aware of proven best practices outside of its own domain.
- Need a more **integrated approach** to do quality assurance.

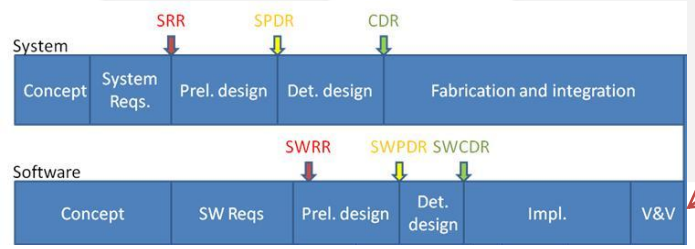
Our Approach

- Investigate **synergies** among assurance techniques.
  - Across all the developed components.
  - Across all the development phases.

- Compare and contrast readiness certification review processes for software (SRR) and hardware (HRR) components
  - Context: aerospace domain, development of highly critical and complex systems.

Readiness Certification Reviews

- What is readiness review?
  - The **last gateway check** performed prior to a component (and its supporting artifacts) being delivered for integration and test.
  - Uses a form with associated questions (to check for satisfaction of success criteria) and required data attachments.
  - Quality Assurance Engineers (QAE) are responsible for gathering and evaluating **evidence** prior to formal certification review meetings.
  - Output is a **delivery decision** along with **action items**.
- Why look at readiness review? It is:
  - Considered a highly critical activity - A mechanism for risk evaluation in the transfer of ownership.
  - The ultimate accumulation of other assurance activities occurring during the development of the equipment.
  - **A common assurance activity that is shared by multiple disciplines.**

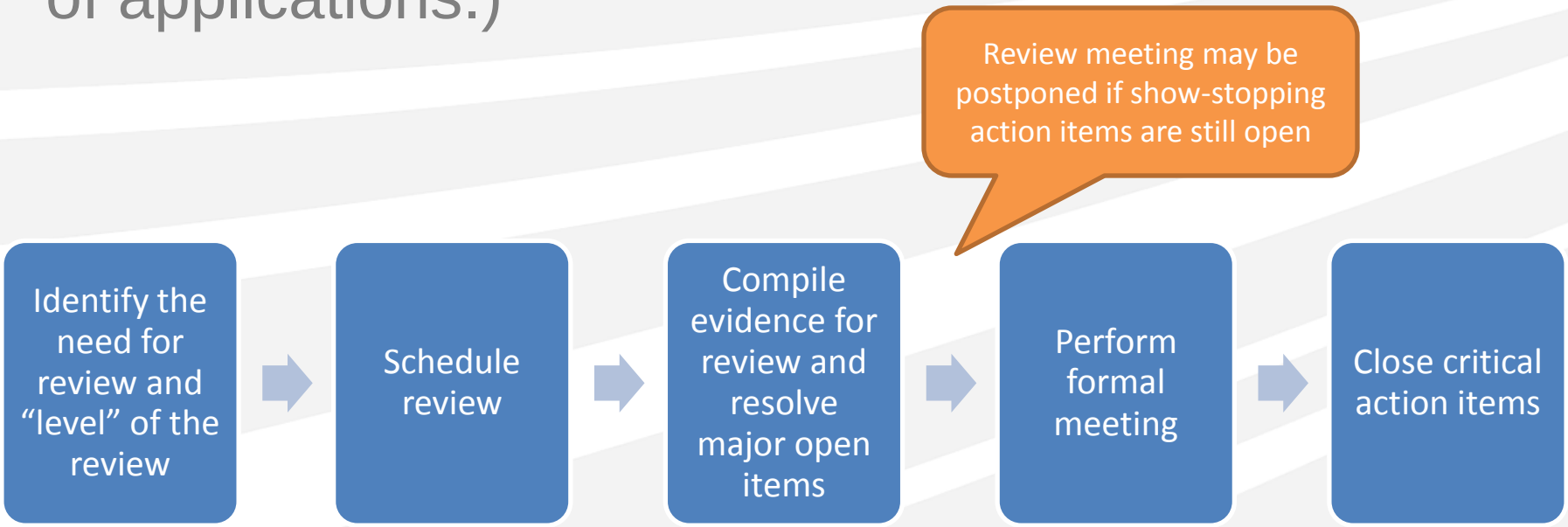


SRR – final review of documentation and open item closeout process

Fraunhofer USA
Center for Experimental Software Engineering

Overview of Readiness Review Process

(Review process may differ slightly between types of applications.)

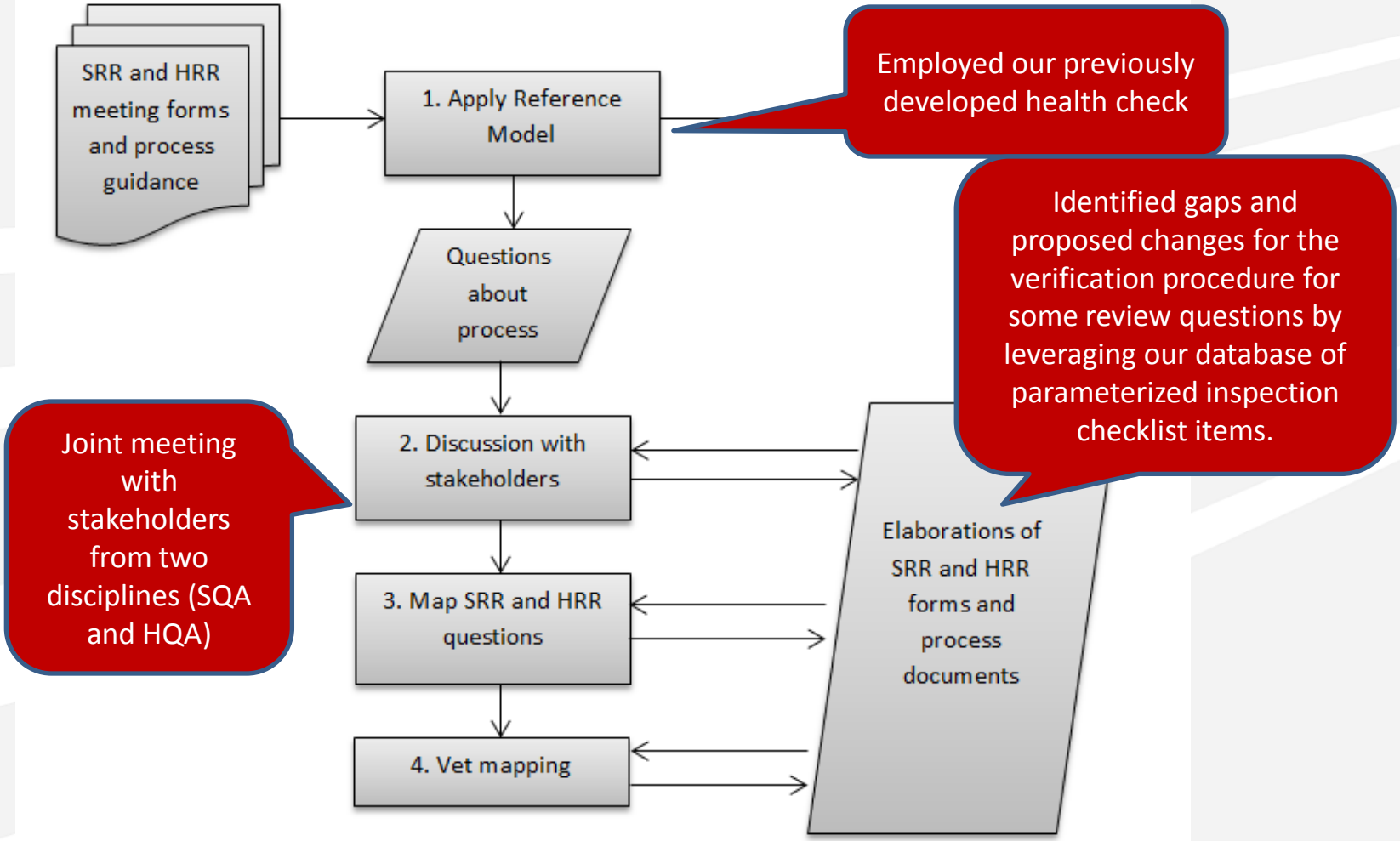


Fraunhofer USA
Center for Experimental Software Engineering

Objectives of This Work

- Apply and extend the Fraunhofer-developed method for assessing review/inspection activity.
- Work with the development organization to:
  - Update review processes to reflect current state-of-art practices.
  - Minimize variations in the way a review question may be checked depending on the QA Engineer expertise.
  - Increase the rigor of the process.
- **Opportunity to "align" the assurance activities performed independently by both HW and SW QA.**

Evaluation Process and Methodology

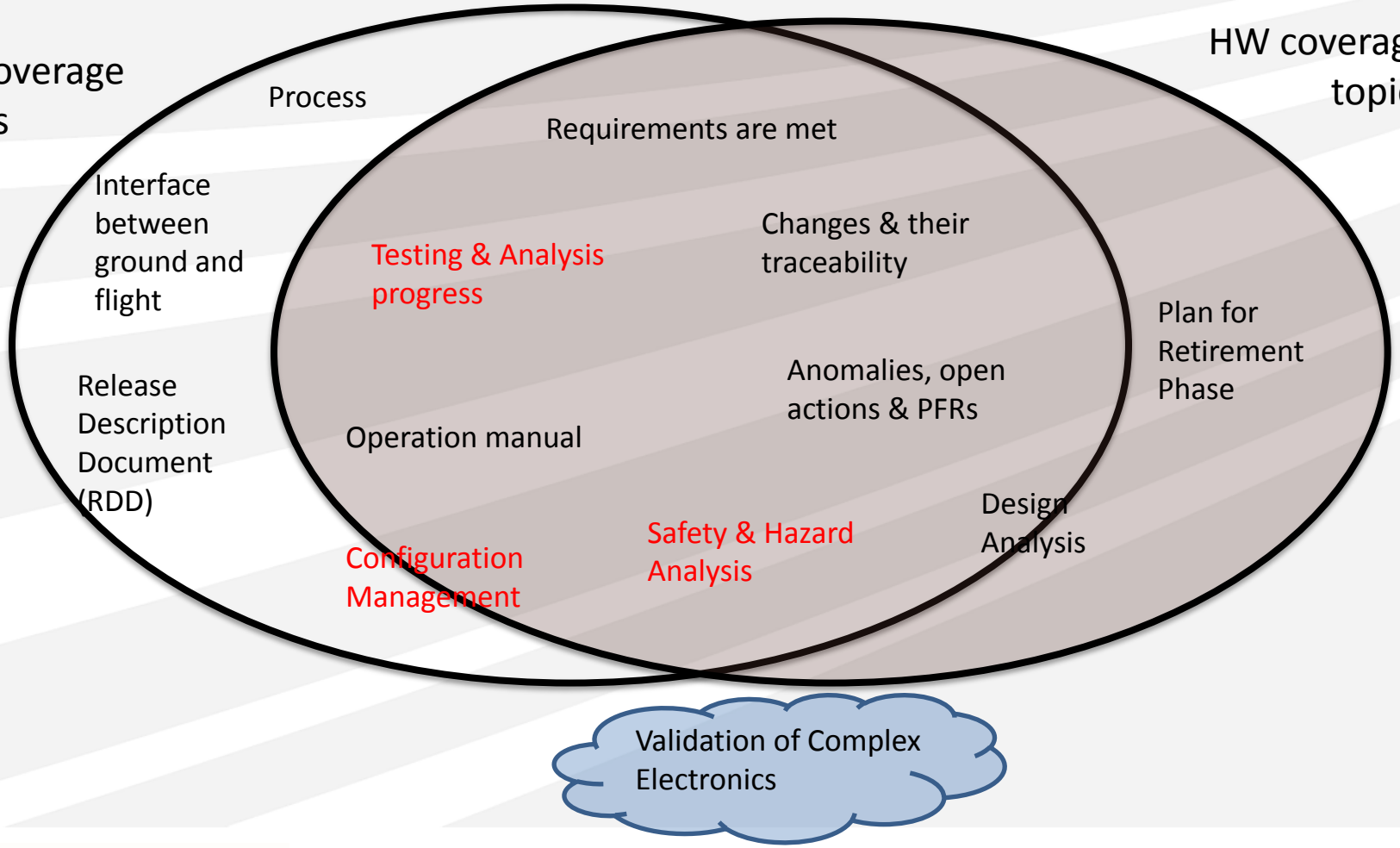


Gaps: the category focus that are not part of both SRR and HRR, the different level of rigor in how the category focus is examined between SRR and HRR

Fraunhofer USA
Center for Experimental Software Engineering

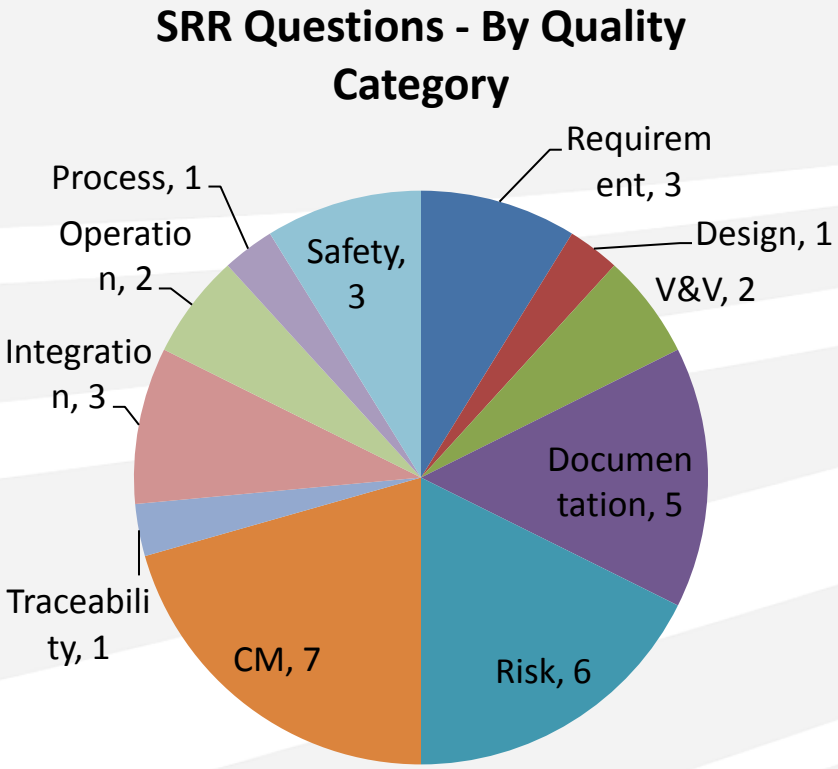
Readiness Review – Mapping Overview

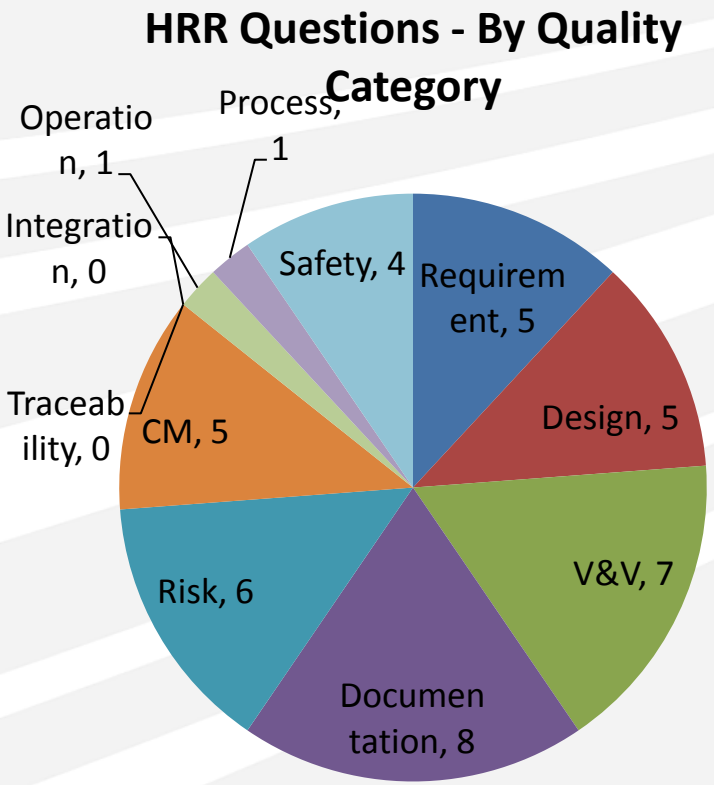
How does SW review relate to HW review?



Fraunhofer USA
Center for Experimental Software Engineering

Certification Review – Characterization





Readiness Review – Major Differences (1)

Category Focus	SW Review	HW Review
Requirement	Concerned with whether requirements are up-to-date, approved, complete, released, under CM, and implemented correctly	Much focus on non-functional requirements such as ones related to environmental and contamination control.
Design	Concerned with whether designs are up-to-date, complete, approved, and under CM.	Also look for evidence of design (tradeoff) analysis.
Safety	Concerned with the implementation of hazard mitigations and ensure that delivered component is safe for the hardware.	Explicitly requires system FMECA, and implementation of single point mitigations
Archival/CM	In addition to delivered software, also concerned with archiving of the supporting software and tool (e.g., compiler, operating system, etc.)	Mainly addresses the issue of hardware replication through documenting as-built-list (e.g., detailed list of parts that made up the delivered component).

Readiness Review – Major Differences (2)

Category Focus	SW Review	HW Review
Documentation	Focuses an operations manual that specifies sufficient information needed by the operator and tester. Also ensure latest changes are captured.	Also verifies instructions for safely handling, cleaning, testing, etc. the component
Risk (remaining anomalies, action items)	Ensures that anomalies or deficiencies with the delivered software are identified, documented, and accepted.	Additionally, requests shortages list, the documentation of existing open actions, waivers/deviations, any problem reports.
Interface with other systems	Relevant for certain projects only. Concerned with compatibility to other systems (e.g., ground/flight)	**None**
Process	Concerned with compliance to the defined process.	**None**
Retirement	None	Archival list is part of hardware component delivery.
Firmware and/or Complex Electronics	**All of the SW review questions are applicable to complex electronics that have been "assigned" as software.**	**Concerned with whether the firmware is the approved version.**

Readiness Review – Other Notable Points

- Both SRR and HRR revolve around compiling a structured delivery package (release document or build book).
- Both processes with a set of process guidance.
  - Guidance provided for the HRR process is more elaborate than the guidance provided for the SRR process.
    - HRR guidance spelled out the role responsible for each check.
- Though both reviews share many common quality focus – the extent of the rigor in the evidence verifying the check can be different.

Sample Recommendations to Mitigate Gaps

- HW review:
  - Place more artifacts and supporting tools into configuration management to ensure the delivered components can be reproduced.
- SW review:
  - Include discussion of remaining risks and open issues related to test support infrastructure.
- Both reviews:
  - Consider stronger interaction between the software and hardware personnel when assuring for hazard analysis, especially on the FMECA of system interface.

Other Recommendations (1)

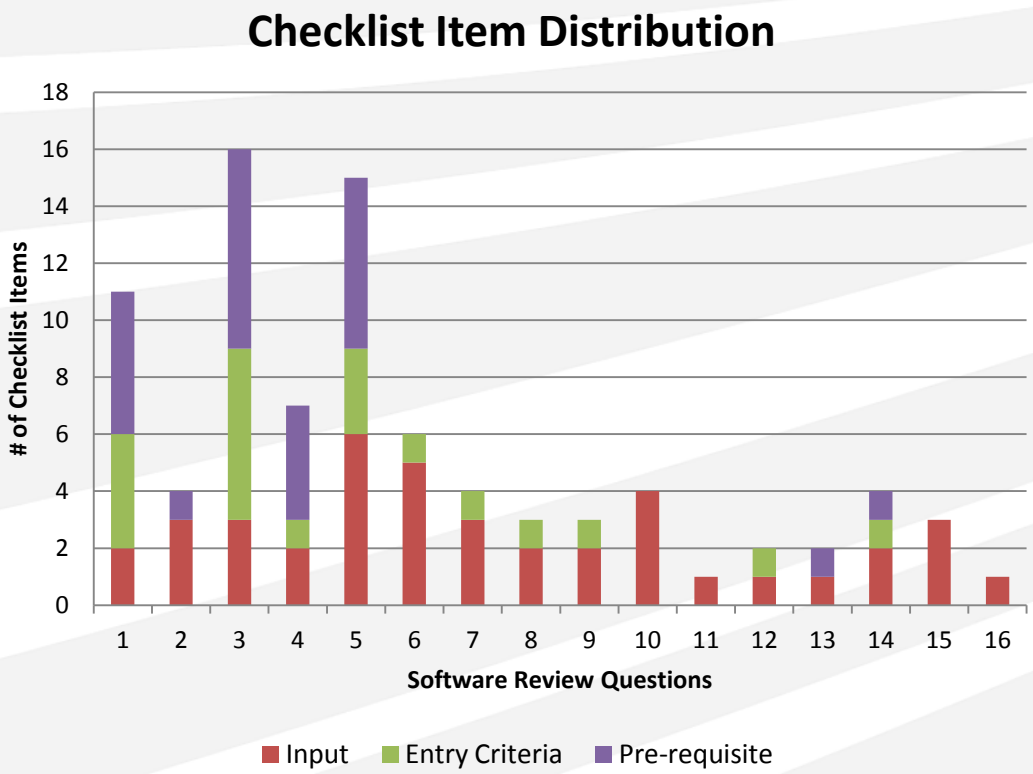
- Made explicit some aspects of quality that are assumed to be assured before the readiness review begins (e.g. pre-requisites)
  - Implications: Ensure that prior milestone reviews have sufficiently assured the pre-requisites.
- Identified conditions required in order to begin the review process.
  - E.g., completed activities, available artifacts.
- Refined the descriptions of the actual checks and their inputs (e.g., artifacts assessed in the course of the review process)

Other Recommendations (2)

- Added specificity to the HW/SW questions by providing sub-questions; i.e., any checklist items that we added under an existing review question and was at a finer level of detail than the review questions.
  - Identified other "gaps" – items that may not be checked consistently in all the reviews, e.g.,
    - Ensuring traceability of a change in a component.
    - Ensuring checks of limits and boundaries to non-functional requirements.
- Clarifications on the wording and terminology.

More on Adding Specificity

How much of the certification review work happens before the review?



Significant variation from question to question regarding how much to check.

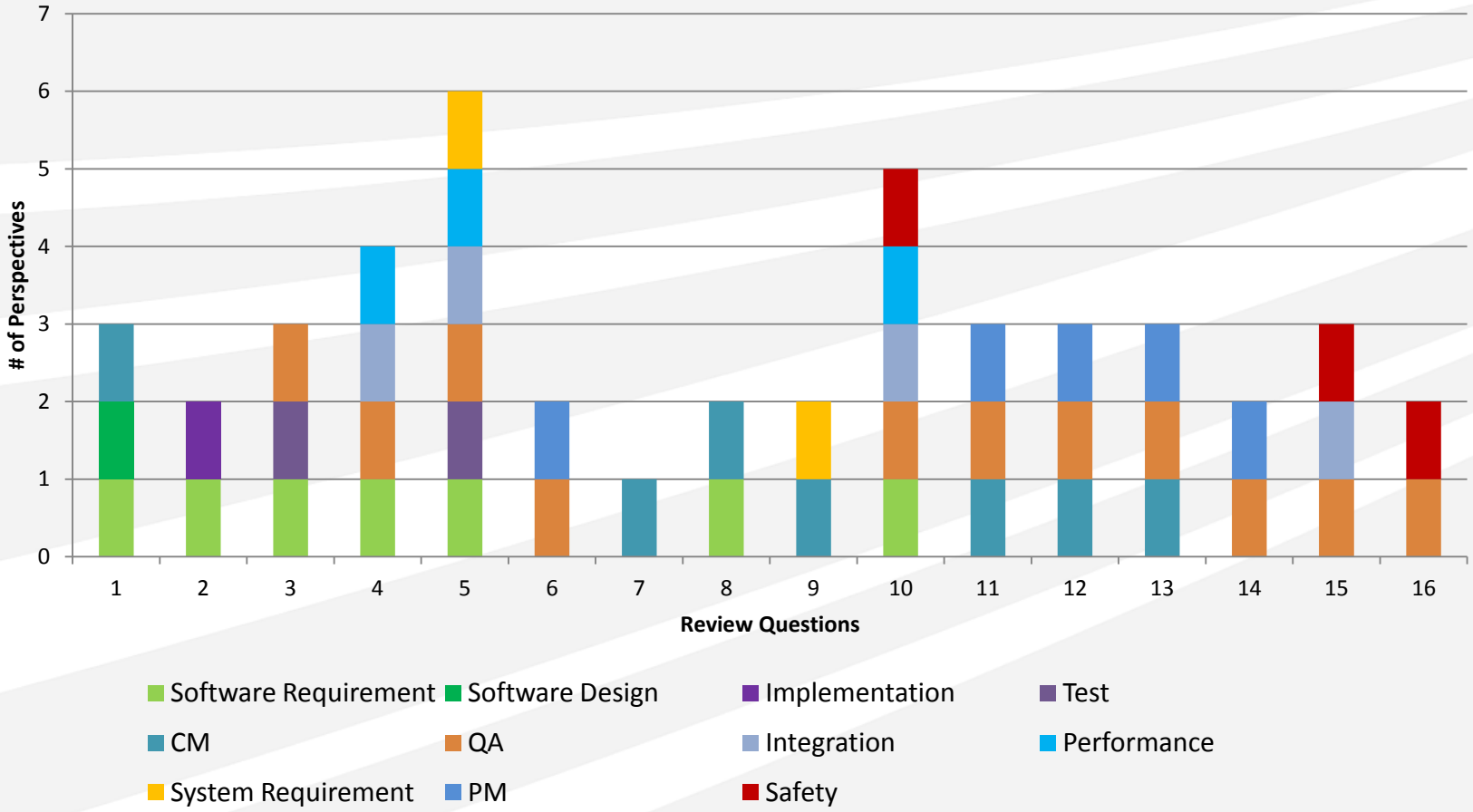
Have identified and made explicit the underlying QA process elements that support the review questions.

For some questions, the real work has to happen long before the reviews.

Fraunhofer USA
Center for Experimental Software Engineering

Characterization of Required Expertise

How does the software certification review incorporate domain expertise?



Fraunhofer USA
Center for Experimental Software Engineering

Current Status

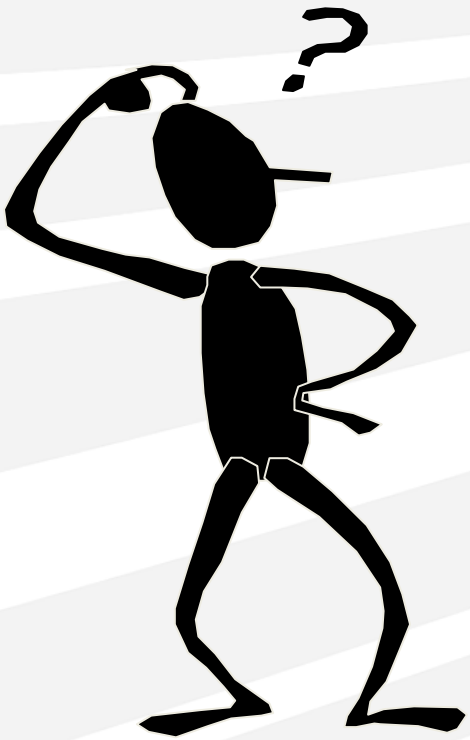
"The whole process was considered a great learning experience from both sides to learn about each others' work."

- Dissemination of work:
  - The SW readiness review process is being updated based on the observations and discoveries of this case study.
    - It is currently under modification to address the feedback from the team review.
    - The process guidance document is being updated.
  - HQA has updated the HW readiness process. Our analysis has fed into this process.

Future Directions

- We are currently applying a similar method to analyze the Support Equipment Readiness Review process .
- Evaluation of existing work:
  - Qualitative analysis to obtain baseline information about the state of the review processes (e.g., effort, perceived benefits, fitness to different delivery scenario, etc.)
    - Allows for measuring impact of changes when they are rolled out
    - Potentially reveals additional opportunity for improvements
  - Compare and contrast with other readiness certification reviews.
- Formulation of quality checks for new application domains, such as complex electronics (focusing on FPGA), mission simulators, etc.

Questions?



Contact Information

Madeline Diep

mdiep@fc-md.umd.edu

240-487-2937

Fraunhofer USA

Center for Experimental Software Engineering

Backup

Fraunhofer Center Maryland

- A not-for-profit ***applied research & technology transfer*** organization
- Mission: ***Advance real-world software practices*** via empirically validated research into software-engineering technologies and processes

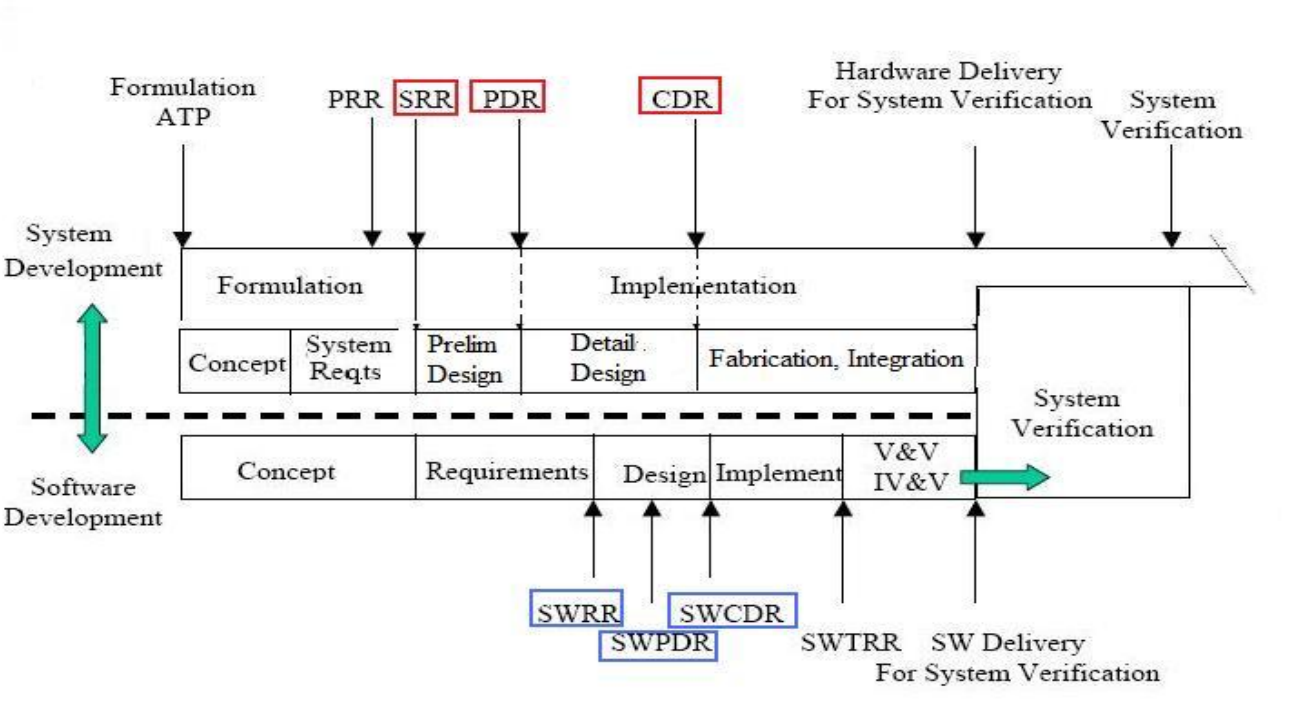
- Work closely with the customer to develop unique, ***innovative solutions*** within their business context
- Purveyor of ***best practices*** to organizations inside and outside of the software industry
- Affiliated with Fraunhofer-Gesellschaft in Germany and University of Maryland at College Park

Fraunhofer USA
Center for Experimental Software Engineering

UNIVERSITY OF 18 56 MARYLAND

Exploring Interactions between Software and System

- Reviews are “Key Decision Points” in both system and software development.
- Reference models allow us to define system and software reviews that:
  - Reason about *types of information* and how it is encapsulated in documentation at various phases ➔ What’s available as input?
  - Understand issues of timing, coordination, and communication across subsystems ➔ How do we assure that future activities can be done correctly?



Tailoring Checklists to Support the Review

- We have added a set of checklist for each review question:
- Each checklist item is parameterized by:
  - The artifacts that are/can be used to support its verification.
  - The type of release associated with the review (e.g., new functionality, bug fixes, flight or final delivery)
  - The perspective needed for its verification.