Presented to:

SAE G-48

Model Based Systems Engineering & Software Safety Workshop

SED Model Based Development Software Safety Guidelines

DISTRIBUTION STATEMENT A: Approved for public release. Distribution is unlimited.

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

2 May 2017

Presented by:

Josh McNeil

Chief Engineer, Aviation Division

U.S. Army Aviation and Missile Research, Development, and Engineering Center

US Army AMRDEC
SED MBSD Safety Guidelines

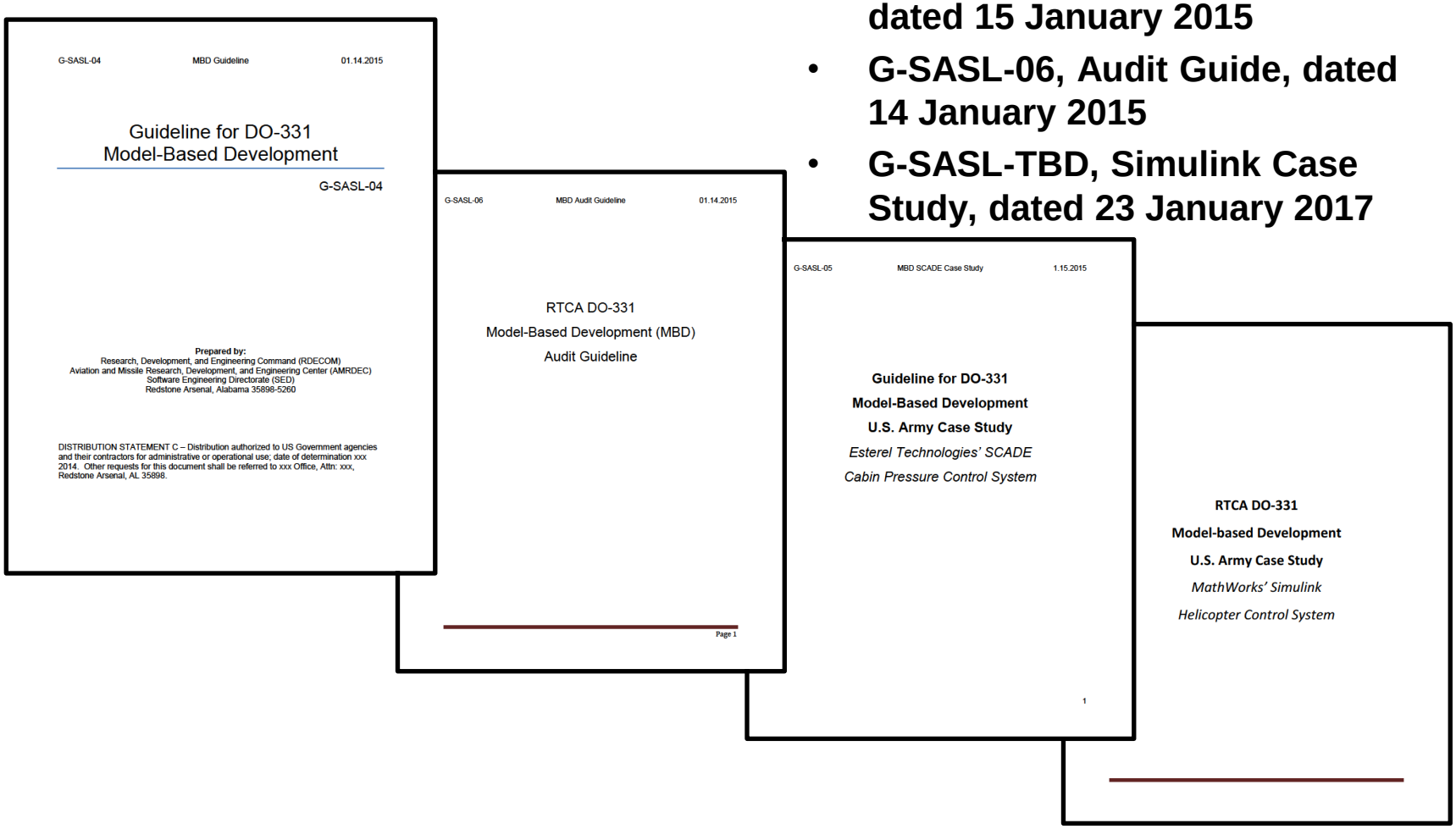
- The SED Aviation Division recognizes the effectiveness and utility of Model Based Software Development techniques for reducing system errors
- A majority of Software Safety as well as programmatic development risk issues caused by inadequate software requirements and design
- SED has developed a Model Based Software Development Safety Guidelines handbook.
- Purpose to provide guidance to the developer and Army assessor of safety related software systems on the underlying issues and concerns associated with meeting Software Safety requirements such as DO-178C objectives

US Army AMRDEC
SED MBSD Safety Guidelines

- Focus to provide guidance to the Army developer and Software Airworthiness and Software Safety approvers on Model-Based Development (MBD) process steps and artifacts
- Supports compliance with requirements and guidance
  - Army Aviation and Mission Command (AMCOM) Software System Safety Policy, AMCOM Reg 385-17
  - Software Engineering Directorate (SED) Software Engineering Evaluation System (SEES) Program Managers Handbook for Aviation Software Airworthiness (PMHASA)
  - RTCA DO-178C and DO-331
- Guide covers MB software requirements, design, code, verification, and tools as generic issues related to MB and in alignment with:
  - FAA/EASA/RTCA guidance material
  - Army Aviation Software Airworthiness
- Two case studies support the understanding of the role of the auditor for a SCADE project and a Simulink project

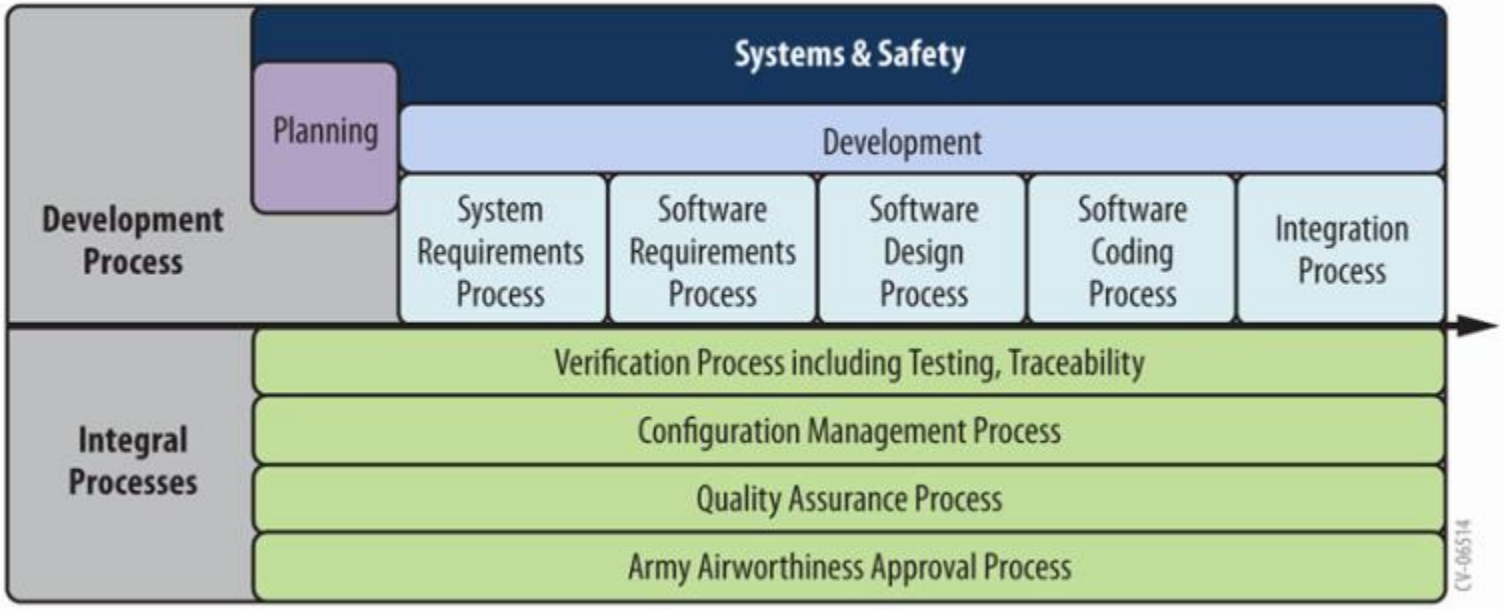
US Army AMRDEC SED Safety Guidelines

- **G-SASL-04 MBD Guideline Rev 1.0, dated 14 January 2015**
  - **G-SASL-05, SCADE Case Study, dated 15 January 2015**
  - **G-SASL-06, Audit Guide, dated 14 January 2015**
  - **G-SASL-TBD, Simulink Case Study, dated 23 January 2017**



The Army's Guideline for DO-331 Model-Based Development

- G-SASL-04 MBD Guideline Rev 1.0 outlines the use of DO-331 in the support of Army Regulations
- Key Items
  - Acquisition and Life Cycle Management of MBD Systems,
  - Planning and Standards
  - Requirements, Design, and Model Based Development
  - Verification with MBD



Army MB Guide and Case Studies

- The Case Studies are designed to be "real" but with certain common problems purposely included
- The Case Studies are coupled with the Army MB Guide to provide a foundation for:
  - Training & Auditing
- The Case Studies stand as a reference for interpretation of the guidance with respect to Army procurement activity
- SCADE case study is a cabin pressurization system
- Mathworks case study is a helicopter flight control system

SCADE & Mathworks Case Studies

- Esterel's SCADE and Mathworks Simulink are the two most widely used modeling languages for representing Low Level Requirements (LLR) in avionics software development
  - UML/SysML is not covered in either case study as it tends to be a look at system development from a different perspective
    - While it does supports software development, it is unlike the process used in SCADE or Simulink
- ULM/SysML are generally focused at a much higher conceptual level (SoS) but can support the creation of software requirements
- We are working at the Software Dev level, not the big-picture Model-Based Systems Engineering level that can be somewhat less proscriptive and less detailed

Why SCADE & Simulink were Chosen

- Simulink and SCADE are very mature products with similar stature in the development community.
- SCADE is know for its "qualified" compiler and rigorous methodologies to produce high quality source code.
- Other SCADE and 3rd party tools support the overall qualification of the entire toolset.
- Simulink is know for its extensive analysis and simulation tools to support requirements and source code development.
- Simulink does not claim to have a qualifiable compiler but does claim to have enough qualifiable support tools to approximately reach the same goals as SCADE
- Both SCADE and Simulink require the support of other verification and analysis tools in order to fully achieve certification assurance levels

Case Study: Topics of Focus

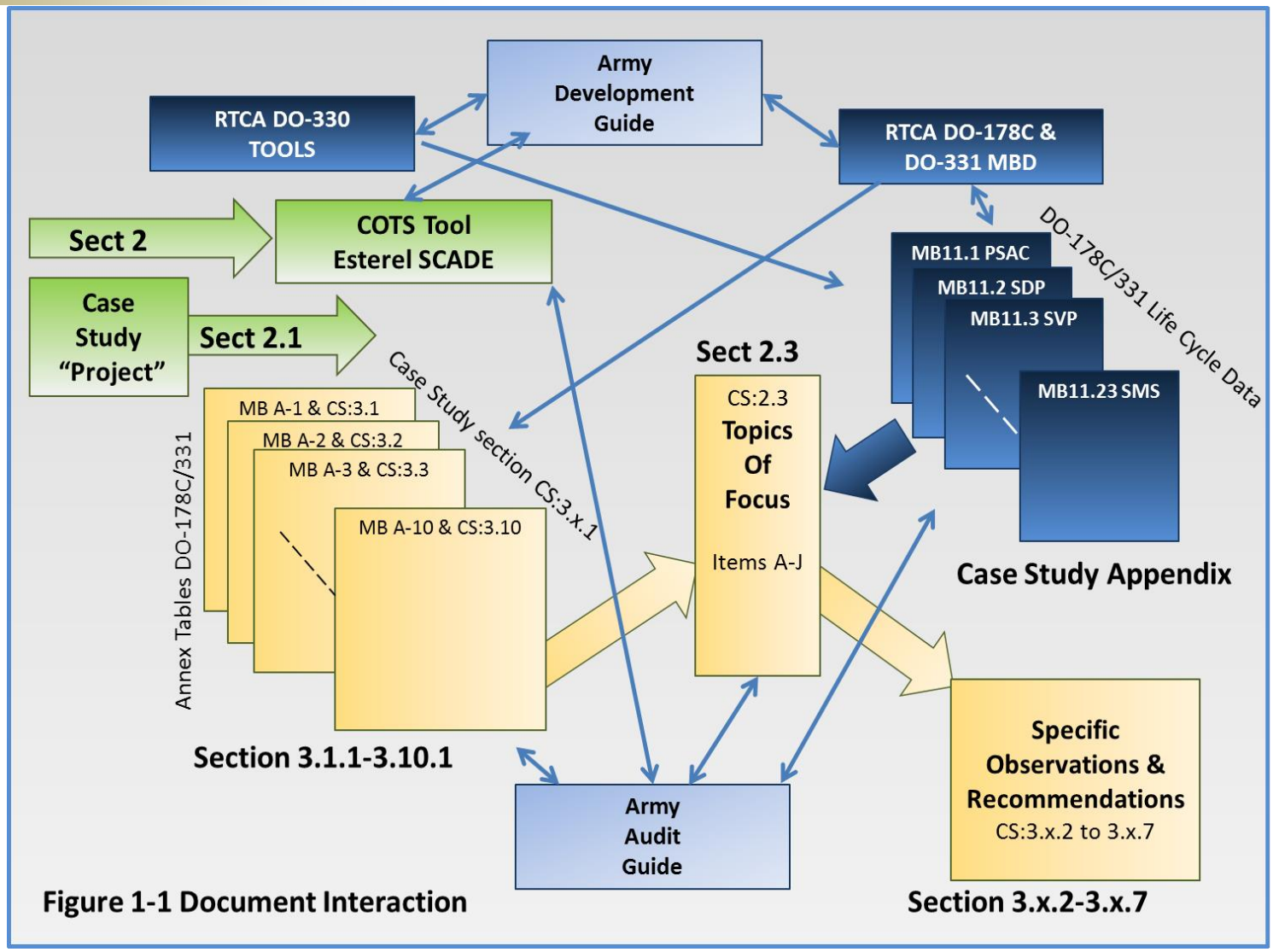


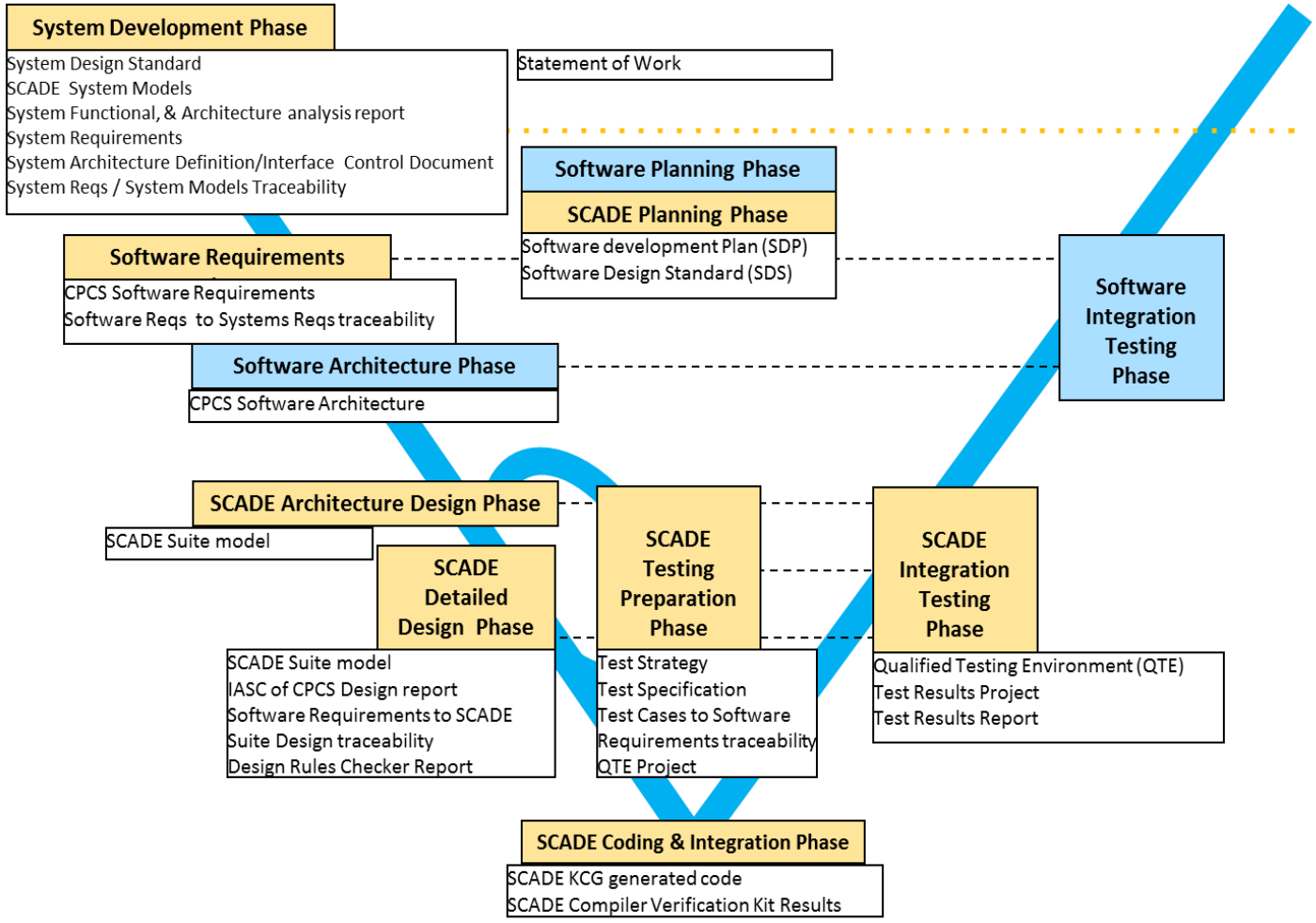
Figure 1-1 Document Interaction

Case Study: Topics of Focus

- System Linkage
- HLR vs LLR
- Importance of Architecture
- Standards & Libraries
- Ambiguous or Non-Deterministic Models
- Simulation
- Tools
- Isolated Function Testing
- Change Management & Control
- Under-Utilization of Tools
- Over-Reliance/Misuse of Tools/Methods
- Artifacts

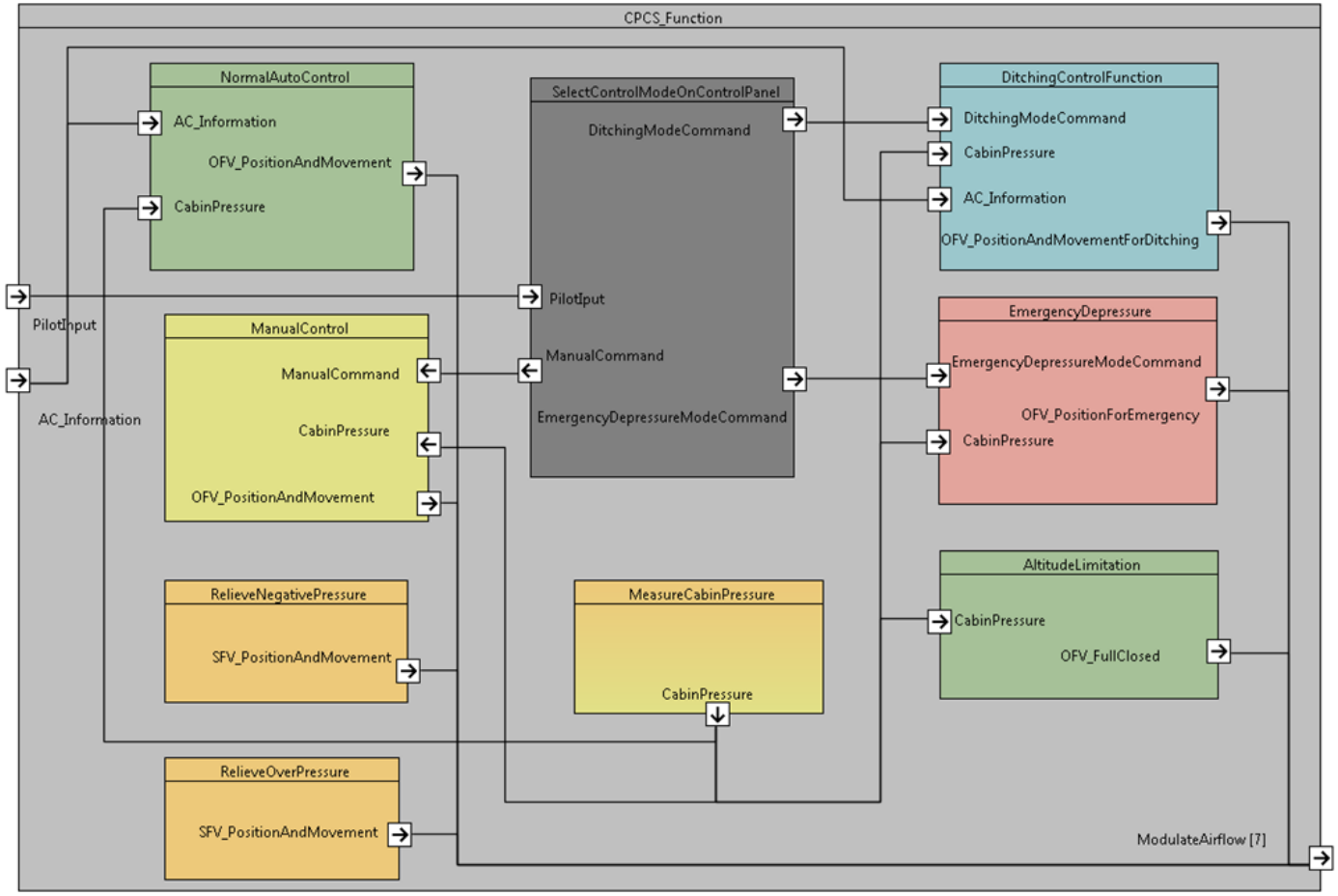
SCADE V-Style Life Cycle

CPCS V-Cycle: Artifacts



Case Study – Comprehensive Study

- **Highly detailed examples allow for a thorough understanding of the development process**



Summary

- The Army Guide & Case Studies provide a rich and extensive body of knowledge relative to MBD
- Written in a practical manner
- Moves well-beyond the static “objective & facts” found in the RTCA and FAA documents
- Valuable for both the developer and the auditor

AMRDEC Web Site
www.amrdec.army.mil

Facebook
www.facebook.com/rdecom.amrdec

YouTube
www.youtube.com/user/AMRDEC

Twitter
@usarmyamrdec

Public Affairs
AMRDEC-PAO@amrdec.army.mil