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.
• 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
  – 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
• 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
• 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
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 support 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.
Simulink and SCADE are very mature products with similar stature in the development community.

SCADE is known 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 known 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

Section 3.1.1-3.10.1

RMCA DO-330 TOOLS

COTS Tool
Esterel SCADE

Sect 2

Sect 2.1

Case Study
"Project"

Sect 2.3

Case Study section CS:3.x.1

MB A-1 & CS:3.1
MB A-2 & CS:3.2
MB A-3 & CS:3.3
MB A-10 & CS:3.10

Army Development
Guide

RTCA DO-178C &
DO-331 MBD

DO-178C/331 Life Cycle Data

Case Study Appendix

Specific
Observations &
Recommendations
CS:3.x.2 to 3.x.7

Section 3.x.2-3.x.7

Army Audit
Guide

Annex Tables DO-178C/331

Case Study section CS:3.x.1

MB11.1 PSAC
MB11.2 SDP
MB11.3 SVP
MB11.23 SMS
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

System Development Phase
- System Design Standard
- SCADE System Models
- System Functional & Architecture analysis report
- System Requirements
- System Architecture Definition/Interface Control Document
- System Reqs / System Models Traceability

Software Planning Phase
- Statement of Work

SCADE Planning Phase
- Software development Plan (SDP)
- Software Design Standard (SDS)

Software Architecture Phase
- CPCS Software Architecture

Software Requirements
- CPCS Software Requirements
- Software Reqs to Systems Reqs traceability

SCADE Architecture Design Phase
- SCADE Suite model

SCADE Detailed Design Phase
- SCADE Suite model
- IASC of CPCS Design report
- Software Requirements to SCADE Suite Design traceability
- Design Rules Checker Report

SCADE Testing Preparation Phase
- Test Strategy
- Test Specification
- Test Cases to Software Requirements traceability
- QTE Project

SCADE Integration Testing Phase
- Qualified Testing Environment (QTE)
- Test Results Project
- Test Results Report

SCADE Coding & Integration Phase
- SCADE KCG generated code
- SCADE Compiler Verification Kit Results

Integration Testing Phase
• Highly detailed examples allow for a thorough understanding of the development process
• 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