Presented to:

System Safety Society (SSS)

Tennessee Valley Chapter

SED Software Airworthiness & Safety Lab (SASL) SW Safety Analyses

AMRDEC

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Presented by:

Josh McNeil, Latoya Eggleston, & Rhonda Barnes

Software Airworthiness and Safety Lab

Software Engineering Directorate – Aviation Division

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

16 March 2016

Agenda

- SED Software Airworthiness and Safety Lab (SASL) Introduction
- SED SASL Experience
- SED SW System Safety Analysis Process (S^4AP)
- SED SASL Objectives
- The F-35
- SED F-35 Independent Software Safety Analysis Task (ISSAT)
- ISSAT Approach
- ISSAT Objectives
- Software Safety Analysis
  - SED Software Safety Analysis Database Schema Overview
  - SED SASL Criticality Analysis Report (Screenshot)
  - SED SASL Findings Report (Screenshot)
- SED SASL Conclusions

SED SASL Introduction

MISSION

- Provide independent supplemental software airworthiness and safety support for aviation and weapons systems, assisting the AED Airworthiness Release and AMCOM Safety Office Software System Safety Technical Review Panel (SSSTRP) processes.

CORE COMPERENCIES

- Analyze aviation and weapons system software life cycle processes, documents, and code to meet DoD and industry software airworthiness and safety requirements.

LOCATION

- Located at the SED Redstone Arsenal, Building 6263

SOFTWARE TOOLS

- Includes a growing set of tools for analyses across the software development lifecycle (LDRA, Simulink, Understand, FaultTree+,…)

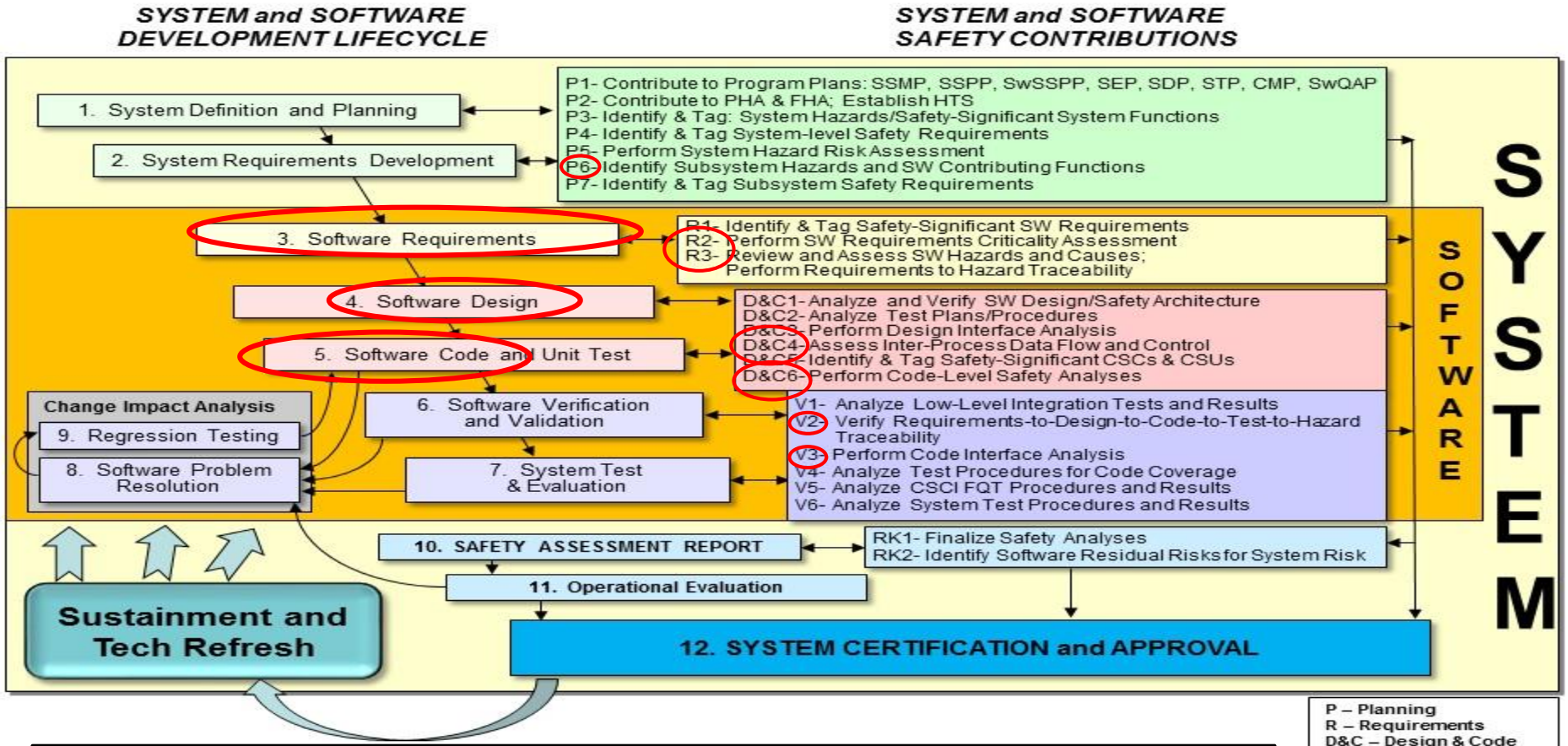
SED SASL Experience

CAPABILITIES

- SED SASL personnel participated in numerous industry working groups
  - MIL-STD-882 Rev E
  - RTCA Special Joint Committee, SC-205 for DO-178C
  - Joint Software System Safety Engineering Handbook Ver. 1.0
  - Joint MIL-HDBK-516 Rev C
- SED SASL has in-house specialized procedures and tools used specifically for analyzing safety-critical embedded software
  - Independent Software Safety Assessment Reports
  - Static Code Analyses, Structural Coverage Analyses
- SED SASL has performed MIL-STD-882 hazard analyses on numerous aviation platforms and weapon systems
  - PHL, PHA, SHA, SSHA, SRCA, FHA, FTA, FMEA
  - Apache, Hellfire, Longbow Launcher, Army UASs, THAAD, Sentinel, JLENS, F-35, IFPC, MML, CH-47

SED SW System Safety Analysis Process

SED Software SYSTEM SAFETY ANALYSIS Process (S⁴AP)



1 **SED SW System Safety Analysis Process provides discipline and rigor**

SED SASL Objectives

1. Disciplined approach
2. Hazard-based software safety analyses
3. Customer desire for active role/insight to analysis process and results
4. Repeatable analysis processes
5. Analyst consistency
6. Auditable results
7. Automated metrics reporting
8. Automated report generation
9. Consistent status reporting

F-35

- The F-35 is the world's most advanced multi-role fighter providing unmatched capabilities to military forces around the world.
- Designed with the entire battle space in mind, the F-35 is the most flexible, technologically sophisticated multirole fighter ever built. By combining advanced stealth designed in from the beginning with fighter speed and agility, fully fused sensor information, network-enabled operations and advanced sustainment, the 5th Generation F-35 delivers innovative capabilities to meet security needs for nations across the world.

Source: https://www.f35.com/about/fast-facts
https://www.f35.com/media/photos-detail/f-35-fires-first-aim-9x-missile

F-35

Video Source: http://www.jsf.mil/gallery/gal_video.htm#

SED F-35 Independent Software Safety Analysis Task (ISSAT)

- The F-35 Mission Systems Prime Software IPT requested the Software Engineering Directorate (SED) to perform Independent Software Safety Analysis of the Safety Evidence Assurance Level 1 (SEAL-1) F-35 Mission Systems Prime Software

SED SASL was selected by F-35 JPO for their experience, training, and documented processes

Source: http://www.jsf.mil/gallery/gal_photo_sdd_f35btest.htm

Task:

- SED SASL performed software safety analyses to identify software system safety critical anomalies within the software requirements, design, code, and/or interfaces on the Mission Systems Prime SEAL 1 Software comprised of four domains:
  - Pilot Systems Software (PSSW)
  - Fire Control Navigation and Stores (FCN&S)
  - Mission/Data Collection (MSN/DC)
  - Core Processing Software (CPSW)

Sources: http://www.jsf.mil/images/gallery/sdd/f35_test/a/sdd_f35testa_070.jpg
http://www.jsf.mil/images/gallery/sdd/f35_test/a/sdd_f35testa_147.jpg

ISSAT Approach

- **Fundamental Element - SED Software System Safety Analysis Process (S^4AP)**
  - **Satisfied Objectives:**
    1. **Disciplined approach**
    2. **Hazard-based software safety analyses**
    3. **Customer desire for active role/insight to analysis process and results**
- **Software Safety Analysis – Design & implementation of a database for use in recording all analyses**
  - **Satisfied Objectives:**
    4. **Repeatable analysis processes**
    5. **Analyst consistency**
    6. **Auditable results**
    7. **Automated metrics reporting**
    8. **Automated report generation**
    9. **Consistent status reporting**

ISSAT Objectives

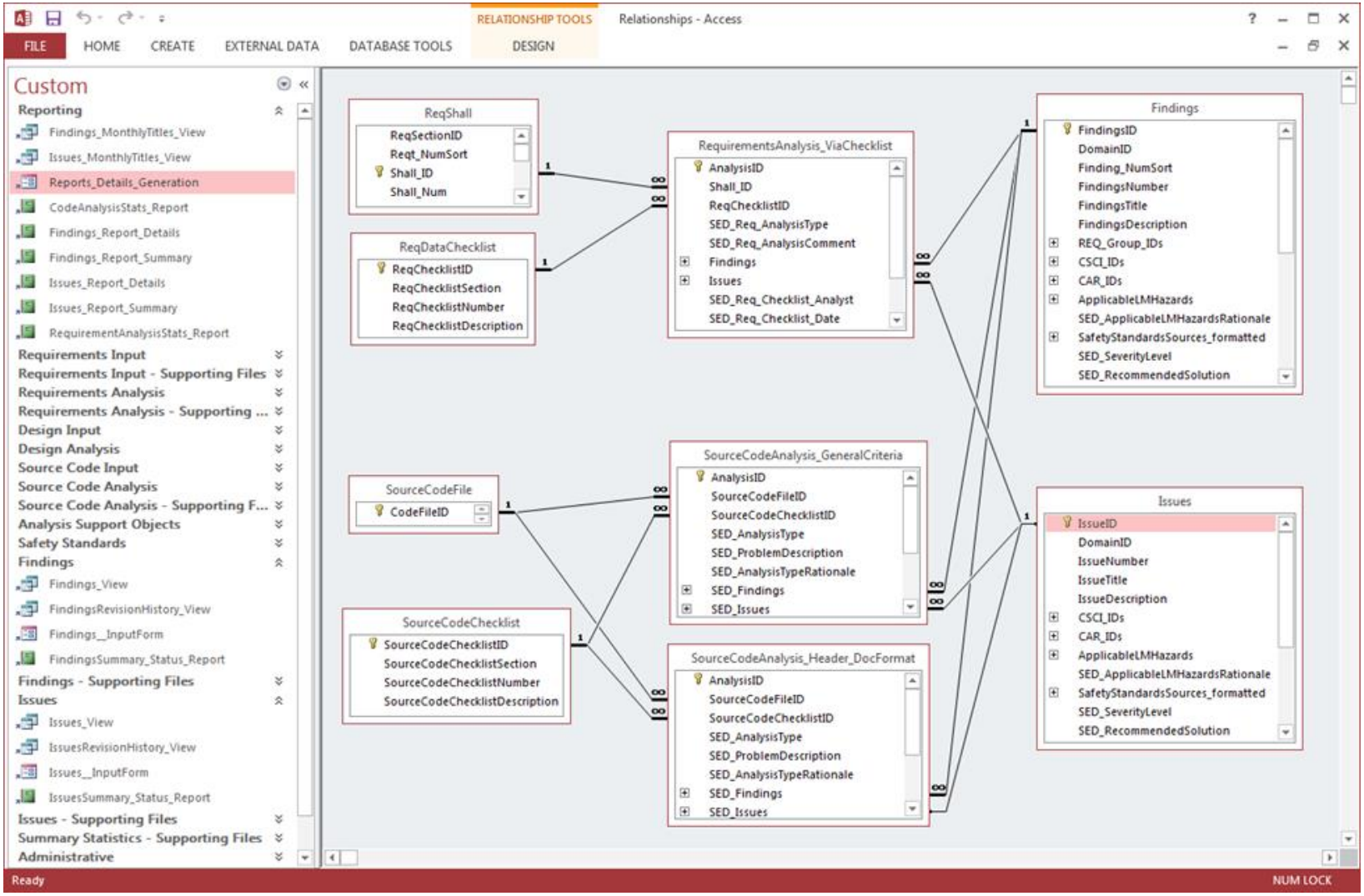
1. Disciplined approach – SED has been applying & evolving the S^4AP since 2003 with great success
2. Hazard-based software safety analyses – SED analyses focus on analysis of software within the context of software contribution & mitigation of system hazards
3. Customer desire for active role/insight to analysis process and results – SED produces an Independent Software Safety Assessment Report (ISSAR) to supplement/complement the Safety Assessment Report (SAR)

- SED SASL analysis focused on providing SW safety evaluation of:
  - Hazard records from the Hazard database
  - SW requirements
  - SW architecture and detailed design including models
  - Interface messages
  - Source Code

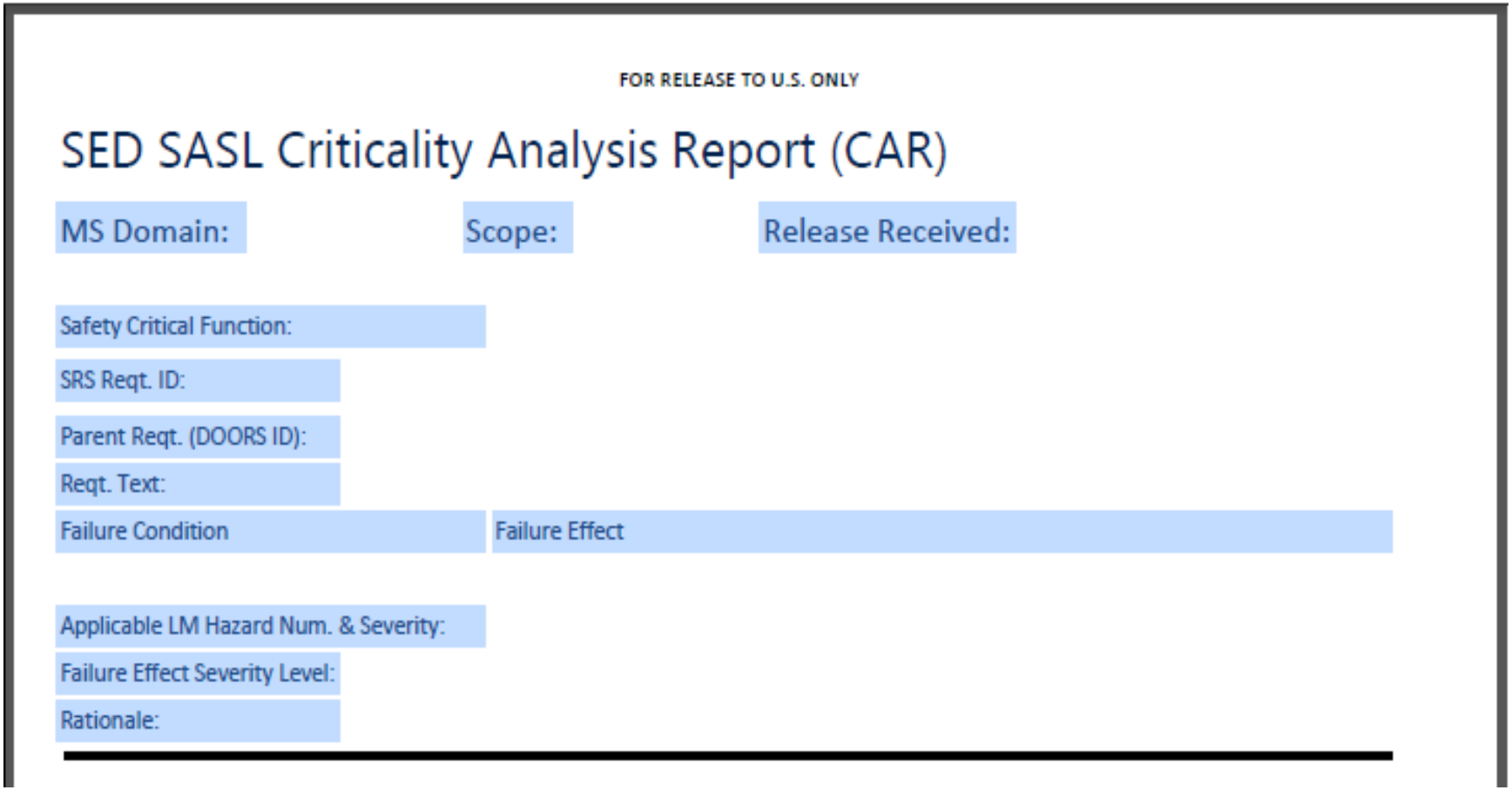
Software Safety Analysis

- Design & implementation of a MS Access database for use in recording all analyses performed
- Objectives this would satisfy:
    4. Repeatable analysis processes – rules were established as to how analyses would be recorded in various database elements
    5. Analyst consistency – checklists were established in the database to be applied to specific analyses
    6. Auditable results – analyst results were recorded in the database to include items such as specific code filenames & code lines evaluated
    7. Automated metrics reporting – the database design facilitated specific metrics such as classification/counts of recorded results
    8. Automated report generation – various reports were designed to export key information using fields from the database
    9. Consistent status reporting - the database was developed to provide “item” counts to be analyzed & % complete

SED Software Safety Analysis Database Schema Overview



SED SASL Criticality Analysis Report (Screenshot)



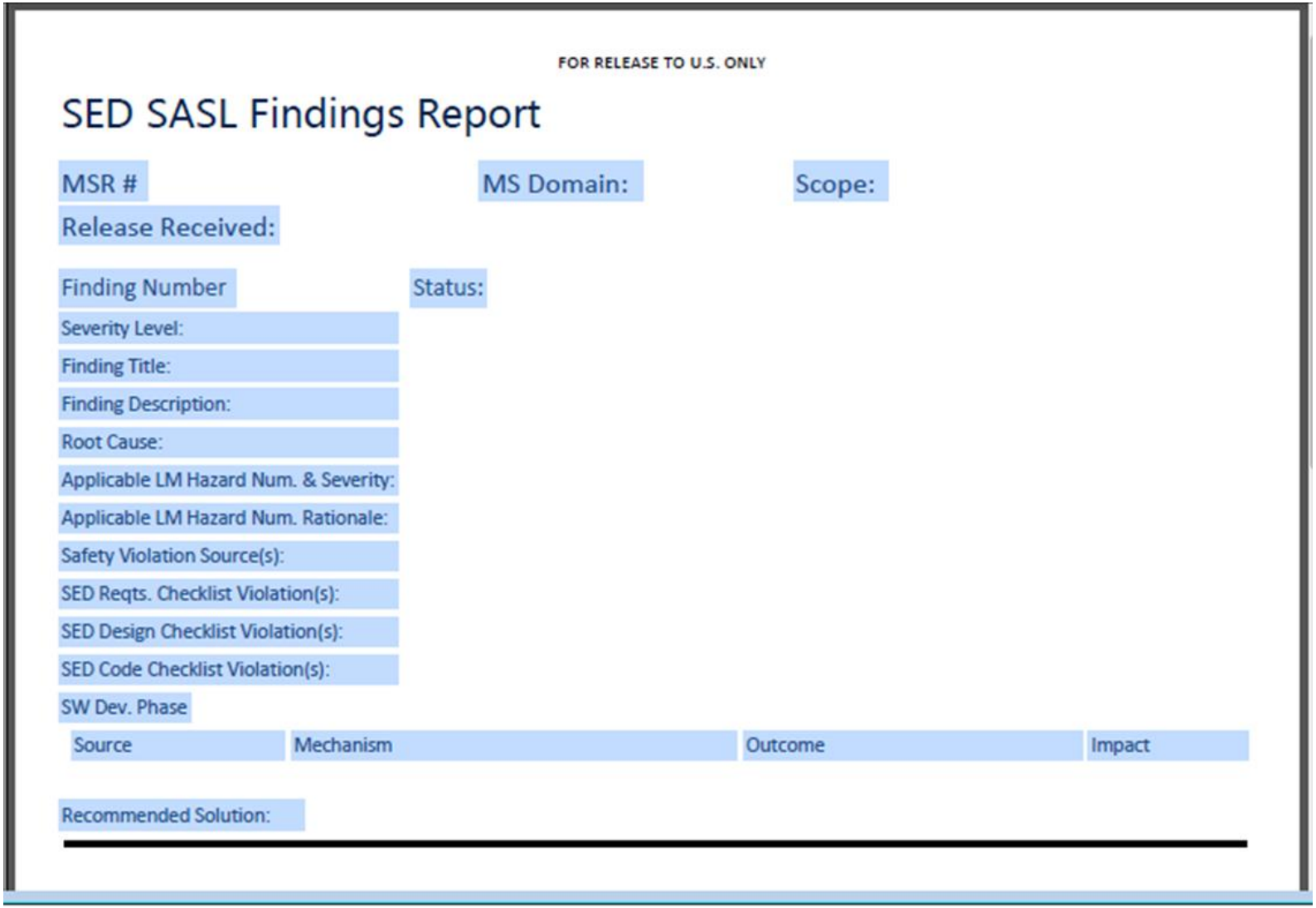
FOR RELEASE TO U.S. ONLY

SED SASL Criticality Analysis Report (CAR)

MS Domain:	Scope:	Release Received:

Safety Critical Function:	
SRS Reqt. ID:	
Parent Reqt. (DOORS ID):	
Reqt. Text:	
Failure Condition	Failure Effect
Applicable LM Hazard Num. & Severity:	
Failure Effect Severity Level:	
Rationale:	

SED SASL Findings Report (Screenshot)



FOR RELEASE TO U.S. ONLY

SED SASL Findings Report

MSR #

MS Domain:

Scope:

Release Received:

Finding Number

Status:

Severity Level:

Finding Title:

Finding Description:

Root Cause:

Applicable LM Hazard Num. & Severity:

Applicable LM Hazard Num. Rationale:

Safety Violation Source(s):

SED Reqts. Checklist Violation(s):

SED Design Checklist Violation(s):

SED Code Checklist Violation(s):

SW Dev. Phase

Source	Mechanism	Outcome	Impact

Recommended Solution:

SED SASL Conclusions

- All software safety analyses were presented within the context of the hazard it controlled or contributed to
- High quality reports were easily produced with sufficient detail to be understandable
- Quantifiable status reporting was easily produced
  - Customer appreciated having metrics as true indication of work performed & remaining
- Customer expressed recognition of the consistent, disciplined rigor being applied throughout the ISSAT
- Customer was impressed with the SASL personnel depth of analysis & understanding of the software achieved in a short time

SED SASL *successfully* applied their processes to perform in-depth software safety analysis

AMRDEC Web Site
www.amrdec.army.mil

Facebook
www.facebook.com/rdecom.amrdec

YouTube
www.youtube.com/user/AMRDEC

Public Affairs
AMRDEC-PAO@amrdec.army.mil