SAFETY CHARACTERISTICS IN SYSTEM APPLICATION SOFTWARE FOR HUMAN RATED EXPLORATION

8th IAASS Conference
Melbourne, Florida
May 2016

E. J. Mango
NASA/KSC
• Develop Human Rated capabilities for exploration class missions into our solar system
• Exploration System Directorate in NASA HQ
• Three separate Programs cross integrated
• JSC – Orion
• MSFC – Space Launch System (SLS)
• KSC – Ground System Development and Operations (GSDO)
  – Command and Control is a project under GSDO

Exploration Systems Enterprise Structure
• GFAS applications integrate the flight software packages of the Orion, the flight software of the SLS, and the ground control systems through the LCS
• Developing the integrated firing room console applications and displays for pre and post launch activities to support flight and ground processing and integrated ground subsystem processing as required for Orion, Core Stage, Booster and ICPS
GFAS Structure

- Over 1.5 Million Lines of Code
- 80,000+ measurements
- About 370,000 hours
- About 30% Complete-to-date

- Ten GFAS Teams
- 70+ Software Engineers, Operations Engineers, Safety and Quality Personnel

- 1200 + Displays

- 500+ Sequencers

- 500+ Routines

- Hundreds of Prerequisite Logic Sequences

- 500+ Sequencers

- 150 + Sequencers
GFAST Software Design Lifecycle

**Doc 45 Software DR**

Initial Software Requirements and Design Specifications – SRDS
Includes Systems Hazards controls and operational requirements

**Doc 90 Software DR**

Final Software Requirements and Design Specifications – SRDS
Initial Requirement Verification Test Matrix - RVTM

**Software Implementation**

Standardized software displays, sequencers, control logic and data fusions

Software Application put under Configuration Control

**Software Integration**

Final RVTM Accepted Integration with External Interfaces

Software Verified against RVTM

**Verification**

Software Validated with User Community
Launch & Processing Engineers, Test Controllers

**Validation**
GFAS Agile Development Process

- Requirements Type Sprint
  - Two Weeks

- Implementation/Integration Type Sprint
  - Two Weeks

- Verification/Validation Type Sprint
  - Two Weeks

A Sprint can be any of these types or a combination

Sprints 6 per Drop

Drops 1-14
Software Safety Characteristics

• **Five Overarching Software Safety Characteristics**

• Comply with NASA NPR 7150.2B Class A Classification for Human Spaceflight Systems

• GFAS system safety engineers embedded into the GFAS Teams to ensure proper implementation of hazard controls and operational safety requirements are included in the software code

• Software safety engineers concurrence on software displays, sequencers, control logic and data fusions are standardized

• Quality engineering supports the engineering reviews and verification/validation preparations to ensures each step of the SRDS is reflected in the RVTM and in the corresponding Verification and validation processes

• Software configuration control from initial implementation through final TCID Build with clear tractability
Questions?