Software Division

The Application of Software Safety to the Constellation Program Launch Control System

James Kania
NASA Kennedy Space Center

Janice Hill
NASA Software Assurance Research Program

ICSQ
International Conference on Software Quality

Purpose

- The purpose of presentation is to provide an overview on the application of software safety practices to the NASA Constellation Program (CxP) Ground Operations Project (GOP) Command, Control, and Communications (CCC) Element Launch Control System (LCS) software development activities
- The LCS software safety program resulted in the successful implementation of the NASA Software Safety Standard NASA-STD-8719.13B and CxP software safety requirements

ICSQ
International Conference on Software Quality

Background

- **Constellation Program**:

  The purpose of the Constellation Program (CxP) is to develop flight and ground infrastructure and systems required to enable continued human access to space after the Space Shuttle retirement and provide future crewed missions to the Moon, Mars and beyond.

- **CCC Element**:

  The Command, Control and Communications Element will provide the Launch Control System (LCS) and associated communications infrastructure to process and launch the CxP launch vehicles and payloads.

ICSQ
International Conference on Software Quality

Background

- **Launch Control System**:

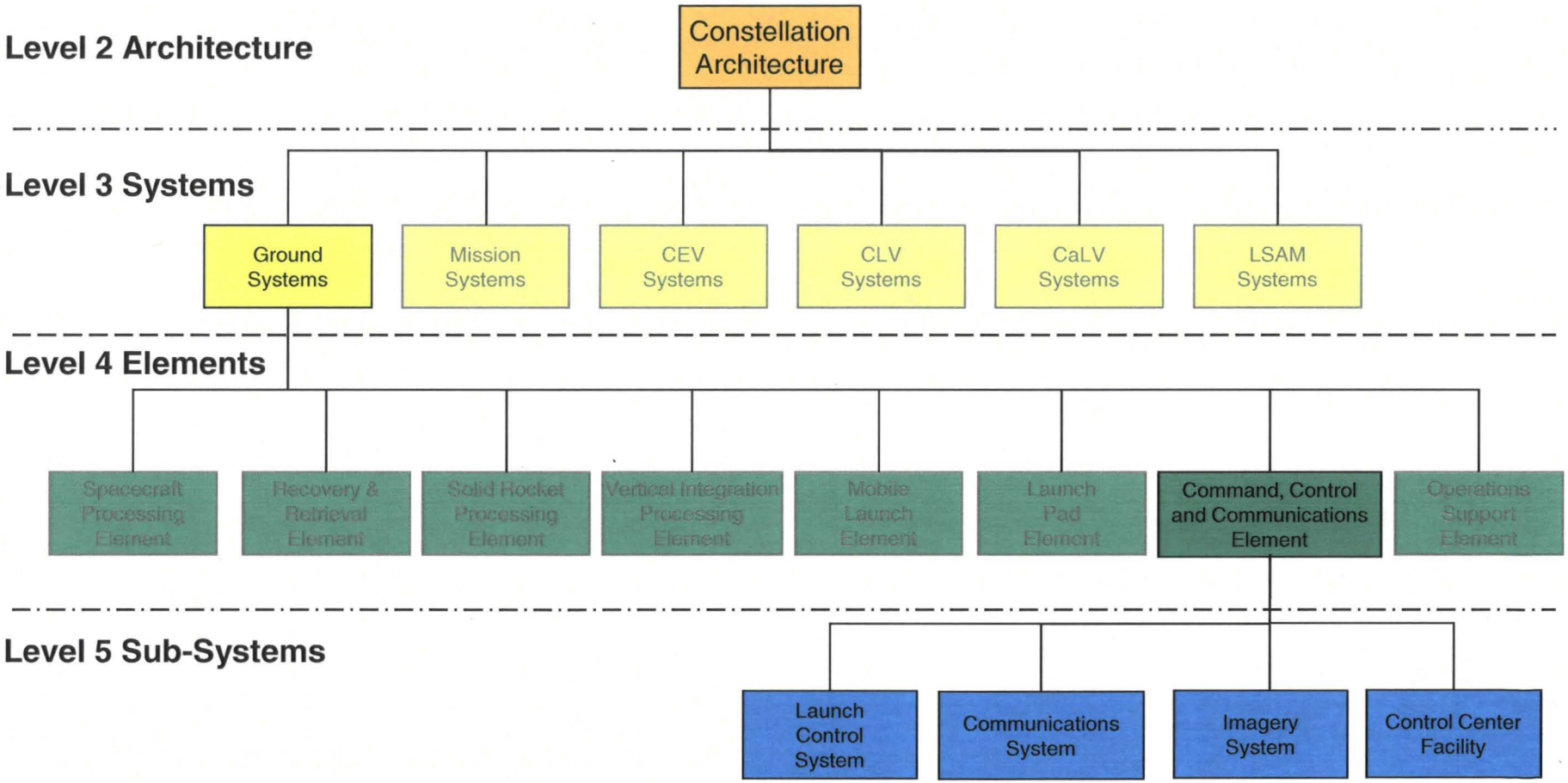
  The Launch Control System (LCS) provides testing, systems integration and launch site processing for Exploration vehicles and their associated ground support systems. This includes computer hardware and software and communications equipment integral to command and control.

- **Kennedy Ground Control System (KGCS)**:

  The Kennedy Ground Control System provides the hardware for control and monitoring of GSE and of vehicle analogs and discretes.

ICSQ
International Conference on Software Quality

Ground Systems Elements



Command, Control, and Communications Project

ICSQ International Conference on Software Quality

General Characteristics

Design maximizes the use of industrial based process control products and COTS to configure a software communication and data distribution architecture rather than build one from scratch

Launch Control System (LCS)

LCS – provides C&C functionality for vehicle processing.

LCS Hardware Architecture

Control Room Workstation – Windows/Linux platforms providing Thin-Client Displays, Light-Weight Displays, and Application Display Clients

Application/Gateway/Display Servers – Unix/Linux platforms, Mid-Range, multi-processor servers providing Integrated Control Applications, Subsystem Control applications, reactive control, emergency vehicle safing, command processing and telemetry data publication.

Industrial Controllers – embedded control systems to provide closed loop control.

LCS System Software Architecture

Isolation service layers providing common functionality, data logging services, networking services, recording services, commanding services, application framework, display framework and system monitoring and control.

LCS Application Software

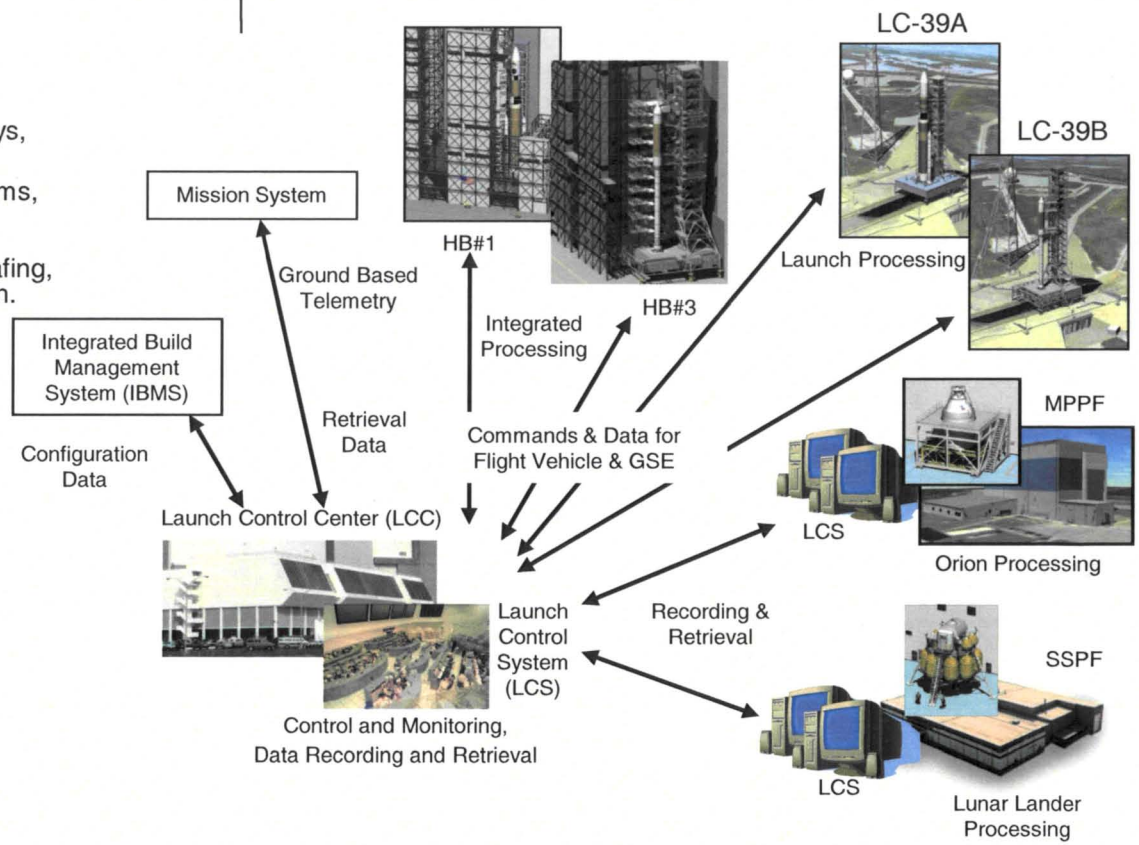
Processing Operations Applications for Orion/Ares I.
Processing Operations Applications for LSAM/Ares V.

LCC Control Rooms

Firing Room 1 for Ares I / Orion,
Firing Room 4 for Ares V / LSAM

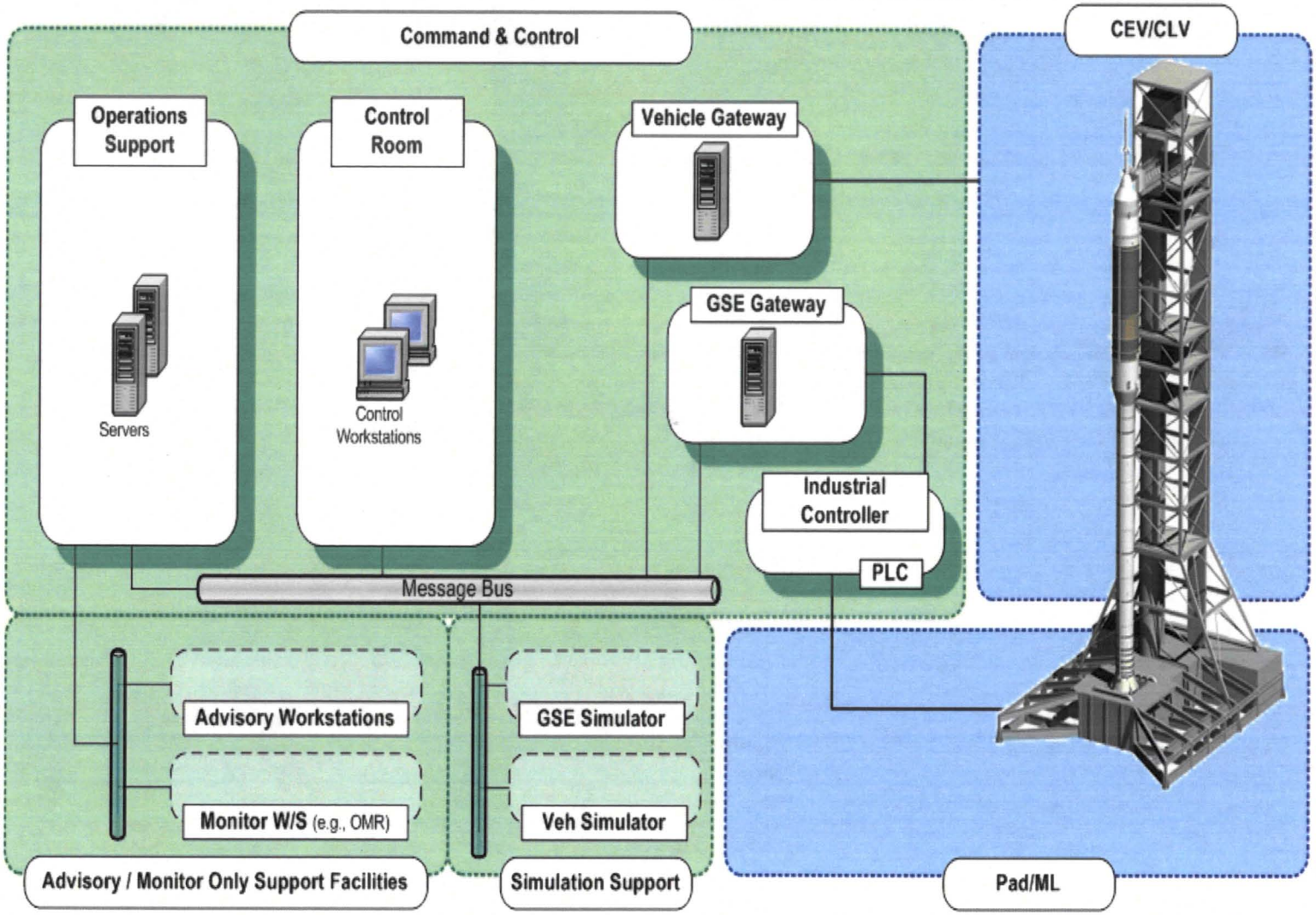
LCS Simulation System

Element simulation, training, and testing support



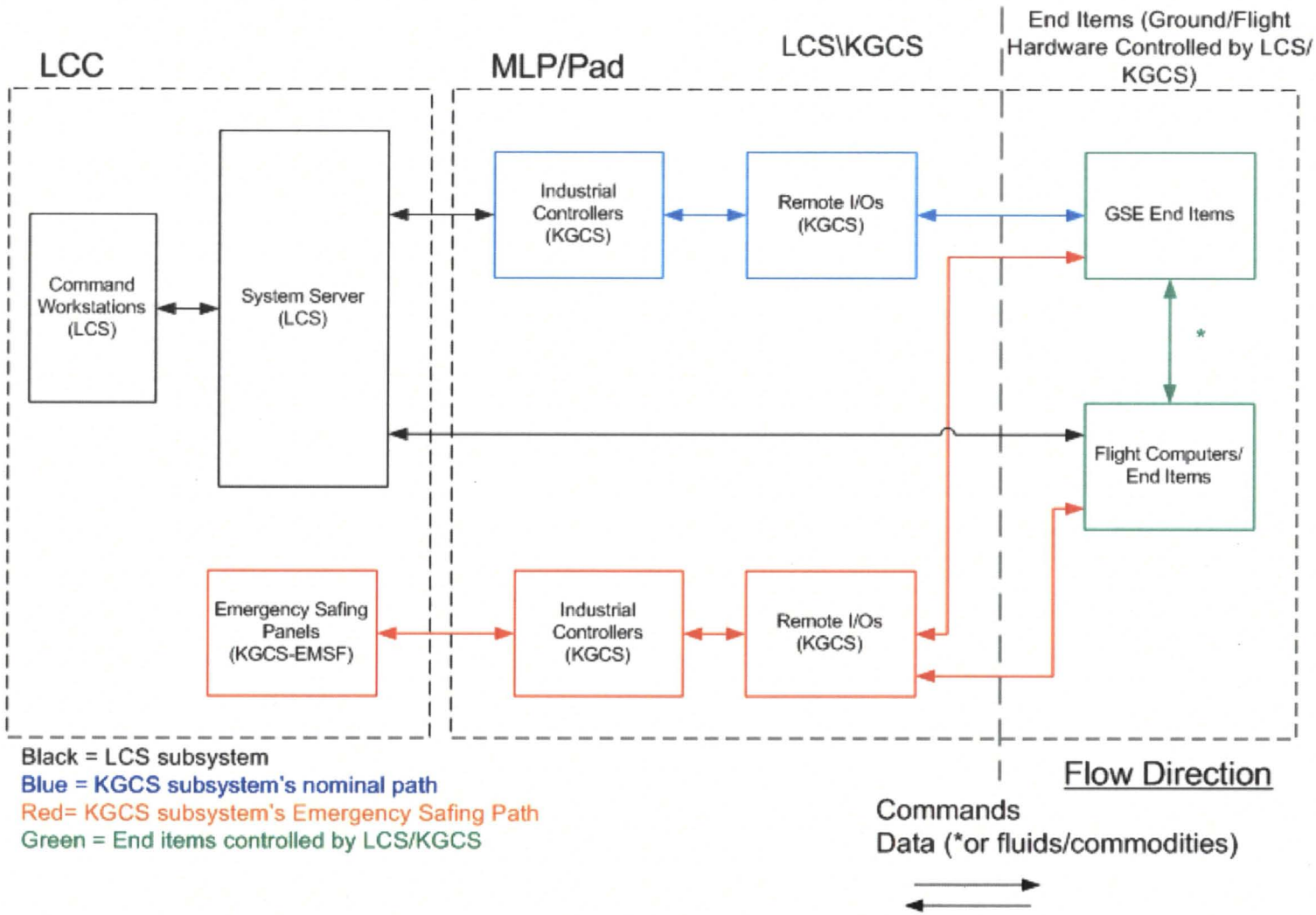
ICSQ
International Conference on Software Quality

LCS System Architecture Overview



ICSQ
International Conference on Software Quality

System Overview



System Overview Summary

- A failure of one or more of the following can cause a hazard to occur if the operation being performed is a hazardous operation:
  - Critical Hardware
  - Application Software
  - System Software
  - Operating Systems
  - Firmware
- A failure in Test Software that yields false positives in test results that test the above items can contribute towards a hazard.
- An error in the operational procedures can also cause a hazard to occur.

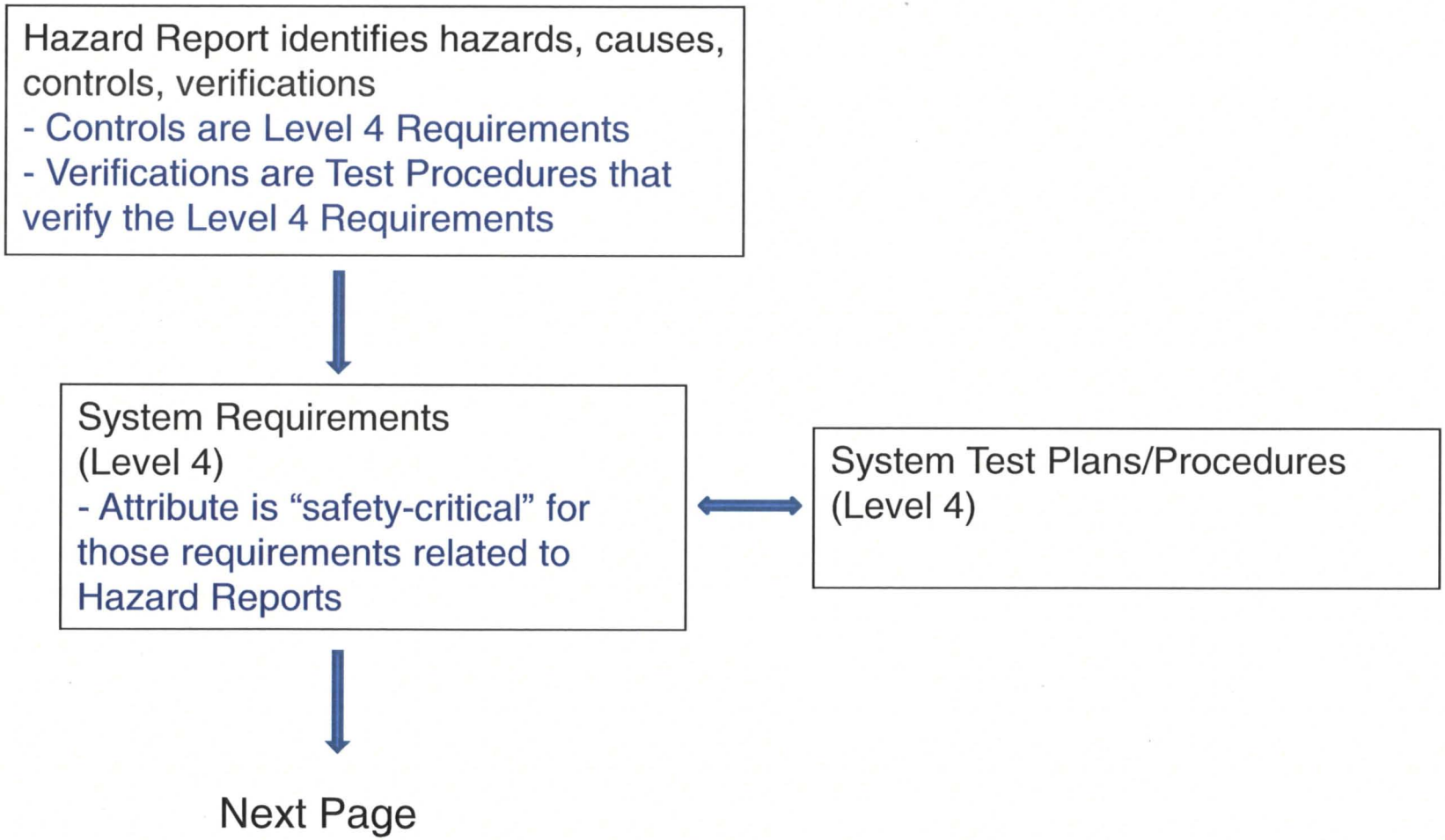
Overall Software Safety Approach

- Integrated approach: Software Safety is implemented jointly with project management, designers, and developers as part of the system design and software development processes from the start of the project
- All project members understand they have a responsibility for implementing safety and that Software Safety's role is to ensure everyone is taking responsibility for implementing safety in their area
- Designers/developers are educated about Software Safety requirements and processes
- Software Safety helps developers define plans/processes/procedures that require safety considerations and additional checks/rigor for safety-critical software (e.g., identification of software requirements as safety-critical, 100% segment coverage in unit test for safety-critical code)
- Software Safety assists developers in defining software coding standards that contain Software Safety related rules
- Software Safety assures the plans, processes, procedures, and coding standards pertaining to Software Safety are followed

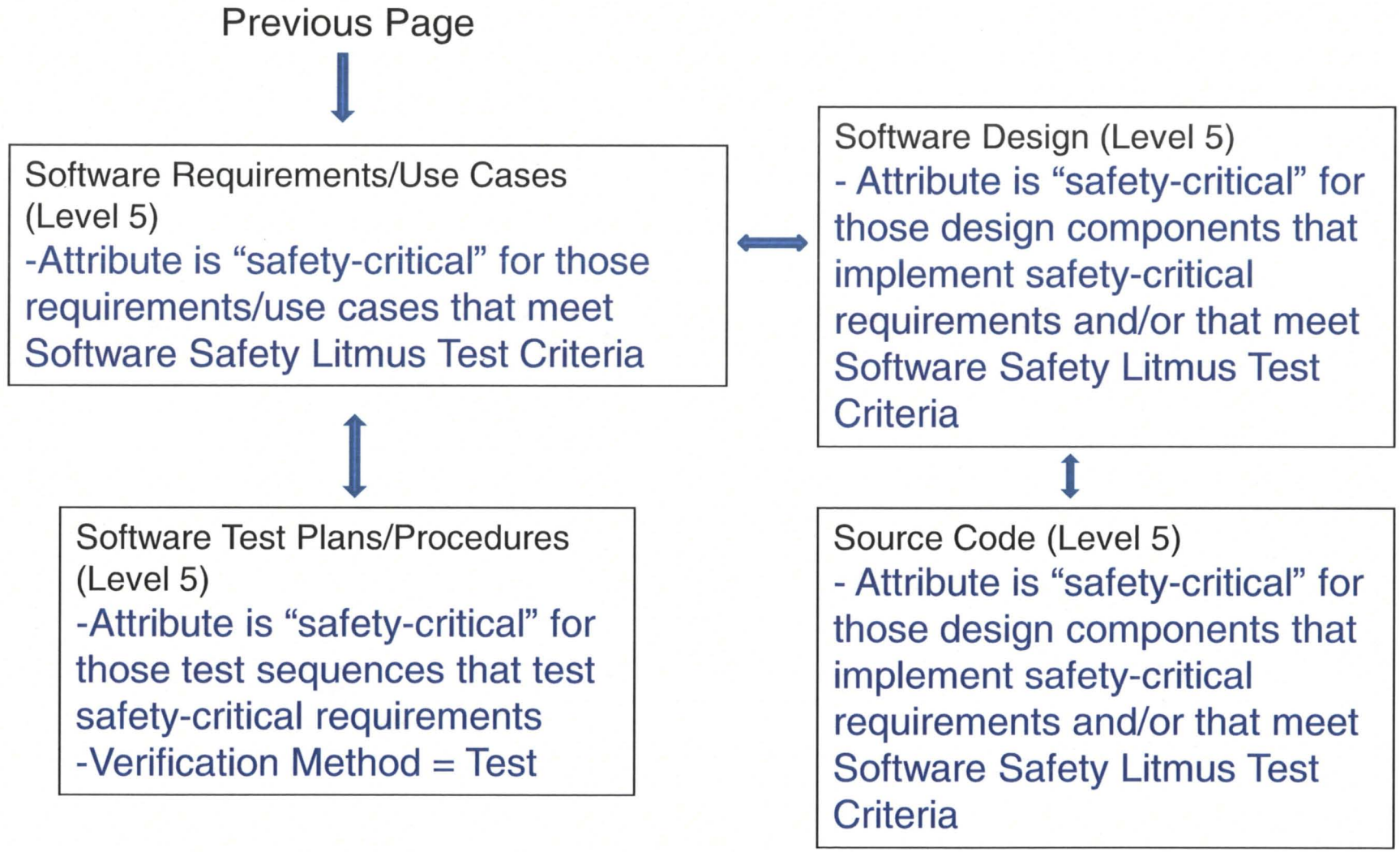
Implementing the Software Safety Program

- Identify potential hazards and hazard causes (Fault Tree Analysis)
- Identify computer-based control requirements used to control (e.g., eliminate, mitigate, reduce, respond to) the hazards/causes – flow down & make these into Level 4 requirements
- Identify other LCS/KGCS system-level safety requirements – also make these into Level 4 requirements
- Annotate the above Level 4 requirements as "controls" for the hazard causes and link controls to causes (in Hazard Reports)
- Use requirements decomposition, requirements traceability, and application of Software Safety Litmus Test to tag decomposed requirements (Level 5 requirements) as "safety-critical" -- *TRACEABILITY IS VERY IMPORTANT !!!*
- Perform software safety analyses/checks upon selected software products (requirements, design, code, tests) by independent software safety analysts
  - Use software risk methodology to decide which software products to sample
  - Perform software safety technical analyses

Software Safety Traceability



Software Safety Traceability



Development of ERD Safety Critical Requirements and Hazard Report

Ground Elements Command, Control, and Communications Project Element Requirements Document GOP407001 Safety Requirements were developed using:

- GOP Preliminary Hazard Analysis Report for EDR (GOP507025)
- System Assurance Analysis of LCS/KGCS (723CAA00001)

All three documents including the draft LCS HR were used as inputs into the GOP-GEN-GSW-011

Element Requirements Document (ERD) GOP 407001-01 Safety Requirements

- The purpose of the ERD is to define the technical requirements allocated from Ground Systems to the CCCE
- It defines the detailed system-level technical requirements and the verification methods (test, demonstration, inspection and analysis) for the CCCE.
- The ERD contains a total of 540 requirements
  - 304 are allocated to LCS
  - 160 are designated as safety-critical
- A subset of the safety requirements were identified as controls for the hazard causes listed in GOP-GEN-GSW-011

PHAR Preliminary Hazards List

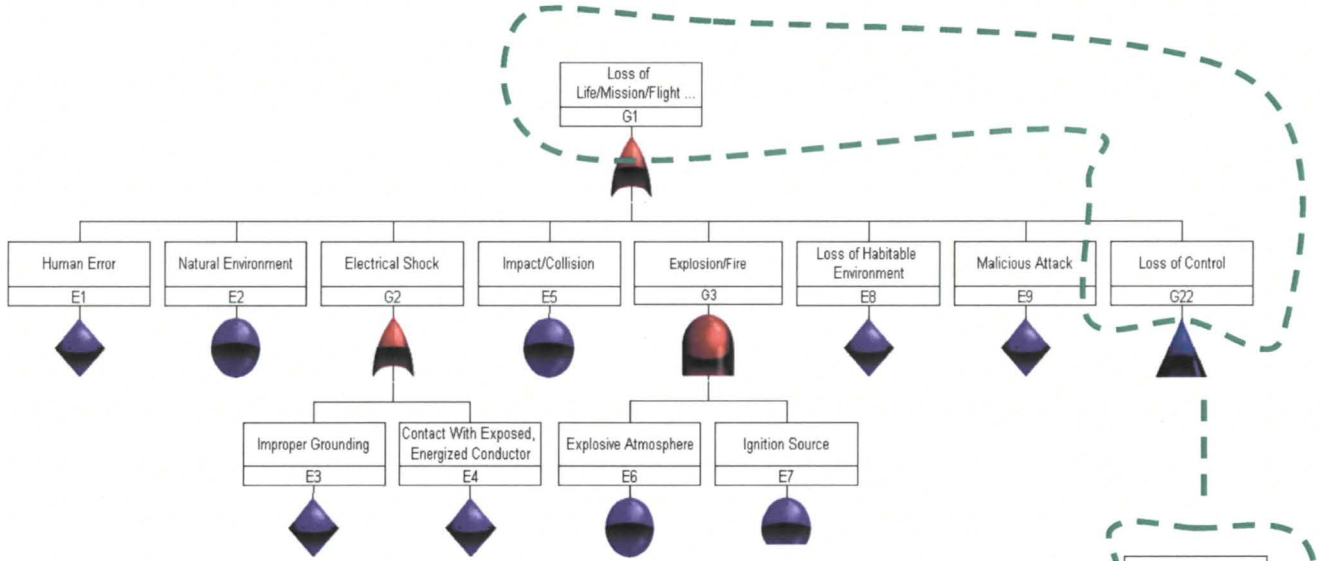
- **The GOP Preliminary Hazard Analysis Report for EDR GOP507025 contains the Preliminary Hazards List**
  - **identifies Loss of Control/Loss of Critical Function as a Hazardous Condition caused by**
    - **Loss of Command**
    - **Loss of Monitoring or Control Function**
    - **Loss of Critical Data**
    - **Unsolicited Command**
    - **Loss of Data (data used by control functions)**
    - **Loss of Monitoring**
    - **Failure to Operate**

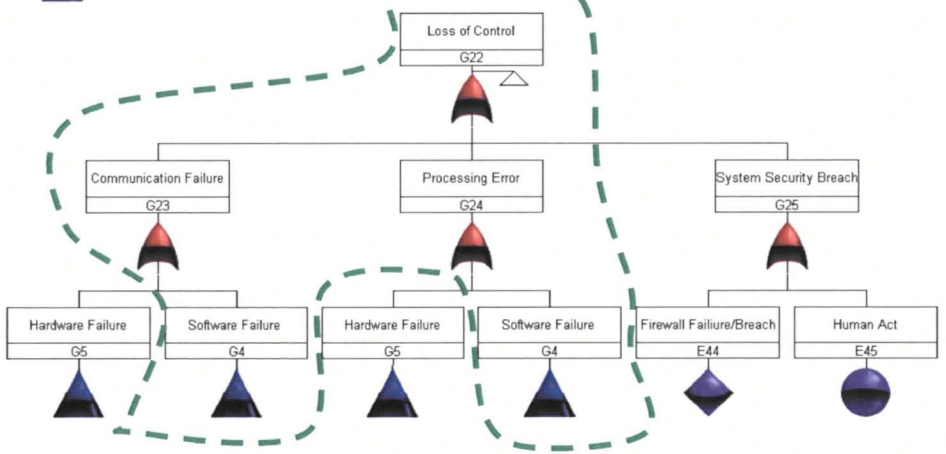
LCS/KGCS SAA FT and HA

- **The LCS/KGCS SAA Fault Tree and Hazard Analysis identified Loss of Control and Software Failure as a Hazardous Condition caused by:**
  - **Loss of Command**
  - **Latent Command**
  - **Latent Data**
  - **Corrupt Command**
  - **Corrupt Data**
  - **Unsolicited Command**
  - **Missed/Misinterpreted Requirement**
  - **Insufficient Testing**
  - **Configuration Error**
  - **Loss of Data**
  - **Sequencing Error**

ICSQ
International Conference on Software Quality

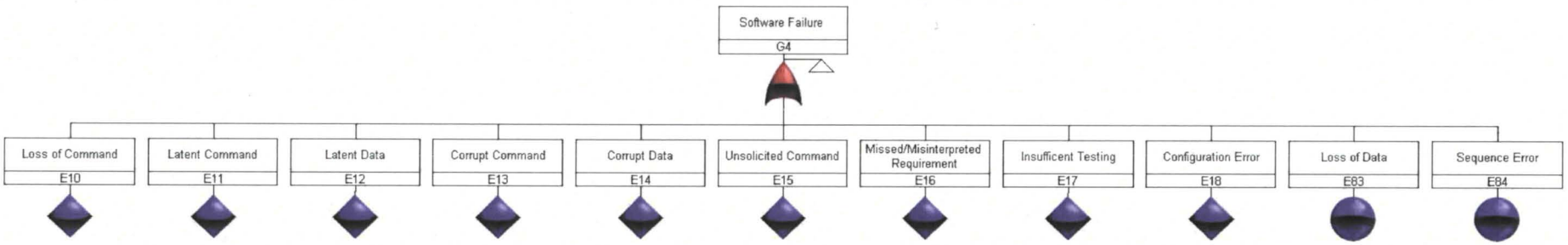
Fault Tree Analysis





System-level Fault Tree Analysis identifies: Loss of Life/Mission/Flight Hardware due to Loss of Control, which can be caused by Software Failure

SAA Software Failure Fault Tree



GO Hazard Analysis Methodology

- The CxP Level 3 GO hazard analyses are driven by CxP Hazard Analysis Methodology (CxP 70038) requirements

- These analyses are organized based on the GO processing flow
  - **CxP 72149, Volume 3, Ground Operations Planning Document (GOPD)**
  - **Logical ordering consistent with major facilities and significant operations within those facilities**

- Top-level fault tree structure shows how GO hazard reports are organized

- GO hazard reports are packaged as part of the System Safety Assessment Report (SSAR) and was processed through the CSERP in a series of Phase Safety Reviews
  - **Industrial Ground Processing Hazard Report (1 total)**
  - **General Ground Processing Hazard Reports (11 total)**
  - **Operation-Specific Ground Processing Hazard Reports (36 total)**

GO Hazard Analysis Structure (Continued)

- Top GO fault tree event is Loss of Life, Flight Hardware, Facilities, and/or GSE During Ground Processing (Loss of life includes injury; Loss of Flight Hardware, Facilities, and/or GSE includes damage)

- Industrial Ground Processing Hazard Report (GOP-IND-ALL-001) addresses standard industrial hazard concerns associated with ground processing

- General Ground Processing Hazard Reports (11 total) document typical ground processing hazards and their associated hazard causes. These hazard causes will occur numerous times in (and be pointed to from) Operation-Specific Ground Processing hazard reports

GO Hazard Analysis Structure (Continued)

- General Ground Processing Hazard Reports (11 total) document typical ground processing hazards and their associated hazard causes
  - **(GOP-GEN-BAT-001) Improper Handling/Charging of Flight Batteries**
  - **(GOP-GEN-CON-002) Introduction of Contamination into Flight Systems**
  - **(GOP-GEN-ESD-003) Failure to Protect ESD-Sensitive Equipment from the Effects of Static Discharge**
  - **(GOP-GEN-FOD-004) Failure to Control FOD**
  - **(GOP-GEN-TRN-005) Transport and Handling of Flight Hardware Between KSC Facilities**
  - **(GOP-GEN-HPS-006) Improper Handling/Configuration of Pressurized Systems**
  - **(GOP-GEN-LFT-007) Failure of Lifting Devices or Associated Equipment**
  - **(GOP-GEN-MAT-008) Flammable/Combustible Materials Could Ignite**
  - **(GOP-GEN-STR-009) Failure of Support Equipment and Handling Equipment Due to Corrosion/Induced Loads**
  - **(GOP-GEN-WEA-010) Exposure to Adverse Weather**
  - ***(GOP-GEN-GSW-011) Loss of Control due to Ground Software Failures***

GO Hazard Analysis Structure (Continued)

- Operation-Specific Ground Processing Hazard Reports (35 total) document unique ground processing hazards and their associated causes. These hazard reports are based on the detailed analysis of hazards associated with the Ares I ground processing flow

- A total of 11 of these Operation-Specific Ground Processing Hazard Reports have been identified as containing software-related hazards

General Hazard Report for Software

- Hazard Report
  - GOP-GEN-GSW-011, Loss of Control of Flight Hardware/Ground Subsystems Due to Ground Software (Launch Control System/Kennedy Ground Control System [LCS/ KGCS]) Failure Results in Loss of Life, Flight Hardware, Facilities, and/or GSE

- Hazardous Condition Description
  - The Launch Control System (LCS) and Kennedy Ground Control System (KGCS) provide testing, systems integration and launch site processing for Exploration vehicles and their associated ground support systems.
  - This includes computer hardware, software, and communications equipment integral to command the control
  - The LCS will be used to support activities such as: control of launch site GSE; monitoring vehicle health and status; recording and retrieval of data communications; and control of flight elements
  - LCS allows users to command, control, and monitor the flight vehicle during VAB and Pad operations

General Hazard Report for Software (Cont)

- Hazardous Condition Description (Continued)
  - LCS provides command, control, and monitoring capability during integration of the flight vehicle in the VAB. This includes integration between the flight vehicle/spacecraft and ground elements during the final assembly and checkout of launch vehicles in the VAB
  - LCS also provides command, control, and monitoring capabilities during element servicing, launch readiness, and terminal launch countdown operations at the Pad
  - LCS interfaces with Mobile Launcher (ML) GSE and is used to command, control, and monitor ML GSE, which in turn, has direct interfaces with the vehicle, including: umbilicals; propellants; hydraulics; pneumatics/purge/pressure; coolant; environmental control; access and handling; power; command/control/monitoring; communication and data; hazardous gas detection; propellant fire detection; launch vehicle ignition and separation; launch vehicle range safety; and lightning detection
  - LCS command and control software failures and ground software development process deficiencies can lead to loss of control of the launch vehicle and/or GSE subsystems, which can result in loss of life, flight hardware, facilities, and/or GSE

ICSQ
International Conference on Software Quality

GOP-GEN-GSW-011 Software Hazard Causes

- **(Cause 1) Loss of Command**
- **(Cause 2) Latent Command**
- **(Cause 3) Corrupt Command**
- **(Cause 4) Unsolicited Command**
- **(Cause 5) Sequencing Error**
- **(Cause 6) Loss of Data**
- **(Cause 7) Latent Data**
- **(Cause 8) Corrupt Data**

LCS/KGCS Software Failures

- **(Cause 9) Configuration Error**
- **(Cause 10) Inadequate Testing**
- **(Cause 11) Requirements Error**
- **(Cause 12) Design Error**
- **(Cause 13) Coding Error**
- **(Cause 14) Security Breach**

LCS/KGCS Software Development Process Deficiencies

Software Hazard Cause Definitions

- Loss of Command - Inability to Issue Commands
- Latent Command - Commands Delayed from Being Issued and/or Received
- Corrupt Command - Command Issued is Incorrect Due to Corruption
- Unsolicited Command - Command Issued Inadvertently or Without Cause
- Sequencing Error - Failure to Issue Commands in the Correct Sequence
- Loss of Data - Data Required to Maintain Control is Missing or Incomplete

Software Hazard Cause Definitions

- Latent Data - Data that is Delayed and not Provided Within the Time Required
- Invalid Data - Data is Incorrect or Incomplete
- Corrupt Data - Data Corrupted During Transmission
- Configuration Error - Software Load/Build Does not Contain Required Displays/Commands/Data)
- Requirements Error - Requirements not Fully Defined or Incorrectly Translated from Requirement to Design
- Design Error - Errors not Detected and/or Removed)
- Coding Error - Insufficient Coding Standards or Coding Reviews

Software Hazard Cause Definitions

- Security Breach - External Act that Bypasses or Contravenes System Security

ICSQ International Conference on Software Quality

Loss of Command Hazard Cause Summary

Hazard Cause	Severity	Likelihood	Hazard Controls
(1) Loss of Command – Inability to issue command(s) due to incompatible transmission protocols/handshakes between interfacing systems/ subsystems in the end-to-end-command the data paths. Inability to issue command(s) due to the transmission protocol/scheme selected during the design effort not being correctly designed for real-time applications such that transmission loss/failure goes undetected and/or uncorrected. Inability to issue command(s) due to loss of timing signal distribution during hazardous operations. Inability to issue command(s) due to failure to react to hazard control related measurements	Catastrophic (5)	Low (2)	•The following Command, Control, and Communications Element (CCCE) Element Requirements Document GOP 407001-01 requirements provide the controls for this hazard cause: [R.GE7018] Error Message Handling [R.GE7019] Continued Operations in Presence of Single Fault [R.GE7072] Hold Countdown: Discrete Signals [R.GE7074] Safety-Critical Loss of Communication Failure Detection [R.GE7078] Timing/Sequencing of Safety-Critical Commands [R.GE7079] Simulated Data Versus Real End Item Data [R.GE7099] Limit Monitoring and Event Exception [R.GE7110] Hazardous Conditions Monitoring [R.GE7117] Fault Tolerance Notification [R.GE7445] End-Item Event Notification [R.GE7458] Continued Operations in Presence of Single Fault [R.GE7468] No Disruption of Network Communication [R.GE7471] Propagation Failures in GSE and Flight Vehicle [R.GE7473] Safety Critical Communication Failure Notification [R.GE7474] Feedback for User-Initiated Safety Critical Commands [R.GE7505] Display Event Notification [R.GE7514] Command Response Specification

Hazard Cause – Loss of Command

- Loss of Command
  - Inability to issue command(s) due to incompatible transmission protocols/handshakes between interfacing systems/ subsystems in the end-to-end-command the data paths.
  - Inability to issue command(s) due to the transmission protocol/scheme selected during the design effort not being correctly designed for real-time applications such that transmission loss/failure goes undetected and/or uncorrected. Inability to issue command(s) due to loss of timing signal distribution during hazardous operations.
  - Inability to issue command(s) due to failure to react to hazard control related measurements

Hazard Controls – Loss of Command

- The following Command, Control, and Communications Element (CCCE) Element Requirements Document GOP 407001-01 requirements provide the controls for this hazard cause:

  - [R.GE7018] Error Message Handling
  - [R.GE7019] Continued Operations in Presence of Single Fault
  - [R.GE7074] Safety-Critical Loss of Communication Failure Detection
  - [R.GE7078] Timing/Sequencing of Safety-Critical Commands
  - [R.GE7099] Limit Monitoring and Event Exception
  - [R.GE7110] Hazardous Conditions Monitoring
  - [R.GE7117] Fault Tolerance Notification
  - [R.GE7445] End-Item Event Notification
  - [R.GE7458] Continued Operations in Presence of Single Fault
  - [R.GE7468] No Disruption of Network Communication
  - [R.GE7473] Safety Critical Communication Failure Notification
  - [R.GE7474] Feedback for User-Initiated Safety Critical Commands

Hazard Controls – Loss of Command

- [R.GE7018] Error and Message Handling
  - The CCCE LCS Subsystem shall provide error and message handling.
  - This includes logging messages and displays of messages. This will aid in trouble-shooting and recreating any anomalous conditions. Error messages displayed at the console provide information on for a future course of action requiring commanding to the end-items. It allows errors in commanding to be detected prior to operations start and for a fix or workaround to be developed. It allows the operator to identify, prior to issuing a command, if the command will not be executed due to a system anomaly. It raises the level of awareness if a command may be delayed, and if data provided to the system may be delayed, incorrect/incomplete, corrupt, or missing.

Hazard Controls – Loss of Command

- [R.GE7019] Data Acquisition Fault Tolerance
  - The CCCE subsystems data acquisition and processing functionality shall continue to operate in the presence of a single fault in any system component.
  - This functionality associated with essential end items will continue to operate in the presence of a single fault in any system component. This allows ability to send a command even in the presence of a fault. The reliability of the data acquired ensures the correct command is executed. It allows the system to continue processing data in the presence of a fault to prevent missing, invalid, delayed, or corrupt data.

Hazard Controls – Loss of Command

- [R.GE7074] Safety-Critical Loss of Communication Failure Detection
  - The CCCE subsystems shall detect loss of communication with end items within (TBDCCCERD-008) seconds beginning with the failure event and ending with system recognition of the failure when any communications path linking safety critical software and its end-item fails.
  - The Command and Control System needs to be aware of the health and status of communications links to the vehicle and GSE. During critical operations, a loss of communication with end items could result in critical or catastrophic events. Therefore, detection of communications loss is needed to allow users to safe the system.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-002
- **Title**: Ares 1 High Pressure Gas Servicing At LC-39 Pad B Results In Loss Of Life, Flight Hardware, Facility, And/Or GSE
- **Hazard Causes Involving Software**: Cause 5 – Overpressurization /Underpressurization
- **Hazard Cause Description**: During FS Roll Control System (RoCS), US Reaction Control System (ReCS), Ambient Fill Bottle, and Upper Stage Engine (USE) Spin Start Bottle fill operations, high pressure gas servicing GSE components fail to regulate pressure and/or human error can cause flight hardware system overpressure/underpressure. Software is used to command GSE valves open and closed to monitor pressure for the servicing GSE, and to monitor temperature measurements from the vehicle.

Overpressurization/Underpressurization Hazard Controls

- LCS/KGCS controls the Gaseous Helium (GHe) pneumatically-operated inlet valves by switching 28VDC power to solenoid valves, which apply Gaseous Nitrogen (GN2) to the actuators using primary and redundant Programmable Logic Controllers (PLCs), whose outputs are both issued simultaneously to energize solenoids from primary and redundant power sources (i.e., there are redundant signal paths [A and B] to each solenoid valve).
- Software (i.e., Integrated Launch and Operations Application [ILOA] Computer Software Configuration Items [CSCI] Main Propulsion System, Upper Stage Engine, and Roll/Reaction Control Systems) is used to command the helium servicing GSE fill isolation valves to close when pressure transducers on the helium servicing GSE read TBD psig pressure.

Overpressurization/Underpressurization Hazard Controls

- The MUST-WORK software functions are correct commanding (i.e., opening/closing) of the isolation valves, pneumatically-operated inlet valves, and the electronically-controlled dome regulators.
- The MUST-NOT-WORK software function is commanding the regulator high. (NOTE: Additional MUST-WORK and MUST-NOT-WORK software functions may be identified as the ILOA CSCI Main Propulsion System, Upper Stage Engine, and Roll/Reaction Control Systems development matures.)

Overpressurization/Underpressurization Hazard Controls

- Controls for hazard causes related to LCS/KGCS software failures and ground software development process deficiencies are addressed in the following general hazard report:
  - HR GOP-GEN-GSW-011 C01 (Loss of Command)
  - HR GOP-GEN-GSW-011 C02 (Latent Command)
  - HR GOP-GEN-GSW-011 C03 (Corrupt Command)
  - HR GOP-GEN-GSW-011 C04 (Unsolicited Command)
  - HR GOP-GEN-GSW-011 C05 (Sequencing Error)
  - HR GOP-GEN-GSW-011 C06 (Loss of Data)
  - HR GOP-GEN-GSW-011 C07 (Latent Data)
  - HR GOP-GEN-GSW-011 C08 (Invalid Data)
  - HR GOP-GEN-GSW-011 C09 (Corrupt Data)
  - HR GOP-GEN-GSW-011 C10 (Configuration Error)
  - HR GOP-GEN-GSW-011 C11 (Requirements Error)
  - HR GOP-GEN-GSW-011 C12 (Design Error)
  - HR GOP-GEN-GSW-011 C13 (Coding Error)
  - HR GOP-GEN-GSW-011 C14 (Security Breach)

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: GOP-OSS-TST-001
- **Title**: Orion Short Stack Portable Equipment, Payloads, And Cargo (PEPC) Testing And Fit Checks In The Multi-Purpose Processing Facility (MPPF) Results In Loss Of Life And/Or Damage To Flight Hardware
- **Hazard Causes Involving Software**: Cause 6 - Inadvertent Orion subsystem activation during OSS configuration for powered cargo/FCE/IVT
- **Hazard Cause Description**: During final configuration of the Orion Short Stack for powered cargo/Flight Crew Equipment/Integrated Vehicle Tests (IVTs), Launch Control System (LCS) software is used to issue a sequence of commands. Improper commanding (e.g., corrupt command, unsolicited command, sequencing error) may inadvertently activate specified Orion subsystems (e.g., solar arrays, separation pyrotechnics) that are not intended for activation during ground processing operations.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: OSS-SVC-002
- **Title**: Orion Short Stack High Pressure Gas Servicing (GHe, GN2, GO2) In The Multi-Purpose Processing Facility (MPPF) Results In Loss Of Life, Short Stack, Facility, And/Or GSE
- **Hazard Causes Involving Software**: Cause 3 - Overpressurization/Underpressurization
- **Hazard Cause Description**: During Orion ECLSS, Reaction Control System, and Main Propulsion System fill operations, high pressure gas servicing GSE components fail to regulate pressure and/or human error can cause flight hardware system overpressure/underpressure. Software is used to command GSE valves open and closed, to monitor pressure for the servicing GSE, and to monitor temperature measurements from the vehicle.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: OSS-SVC-003
- **Title**: Orion Short Stack Hypergolic Servicing (Fuel/Oxidizer) In The Multi-Purpose Processing Facility (MPPF) Results In Loss Of Life, Short Stack, Facility, And/Or GSE
- **Hazard Causes Involving Software**: Cause 3 - Overfill/Underfill (weight scale failure)
- **Hazard Cause Description**: Overfill/underfill of the hypergolic tanks due to electrical weight scale failure. Software is used to command hypergol servicing GSE valves open and closed, to monitor pressure/temperature on the hypergol servicing GSE, and to monitor temperature measurements from the vehicle.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: OSS-SVC-003
- **Title**: Orion Short Stack Hypergolic Servicing (Fuel/Oxidizer) In The Multi-Purpose Processing Facility (MPPF) Results In Loss Of Life, Short Stack, Facility, And/Or GSE
- **Hazard Causes Involving Software**: Cause 11 - Overpressurization
- **Hazard Cause Description**: Servicing GSE fails to regulate flight hardware tank ullage pressure, causing flight hardware system overpressure. Software is used to command GSE valves open and closed and to monitor pressure/temperature on the hypergol servicing GSE.

ICSQ
International Conference on Software Quality

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: ITC-TST-001
- **Title**: Configuration of Hardware to Support Orion/Ares I Integrated Test and Closeout Activities in the Vehicle Assembly Building (VAB) Results in Loss of Life, Flight Hardware, Facilities, and/or GSE.
- **Hazard Causes Involving Software**: Cause 6 - Composite Overwrapped Pressure Vessel (COPV) rupture (Main Propulsion System [MPS] and Roll Control System [RoCS]) during pressurization/repressurization operations
- **Hazard Cause Description**: During FS RoCS, and MPS Ambient Fill Bottle fill operations, high pressure gas servicing GSE components fail to regulate pressure and/or human error can cause flight hardware system overpressure/underpressure. Software is used to command GSE valves open and closed to monitor pressure for the servicing GSE, and to monitor temperature measurements from the vehicle.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-TST-001
- **Title**: Configuration of Hardware to Support Orion/Ares I Testing Activities at LC-39 Pad B Results in Loss of Life, Flight Hardware, Facilities, And/Or GSE
- **Hazard Causes Involving Software**: Cause 3 - Composite Overwrapped Pressure Vessel (COPV) Rupture (Main Propulsion System [MPS]) during pressure maintenance operations for the J-2X Engine Control Unit Confidence Check
- **Hazard Cause Description**: The GHe servicing GSE pressurizes the two Spin Start helium tanks to replenish the helium withdrawn for the J-2X Engine Confidence Check test. Failure of the helium servicing GSE to regulate pressure and/or human error can cause flight hardware system overpressure. Software is used to command GSE valves open and closed, and to monitor pressure/temperature for the helium servicing GSE.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-001
- **Title**: Ares 1 Hydrazine Servicing At LC-39 Pad B Results In Loss Of Life, Flight Hardware, Facility, And/Or GSE
- **Hazard Causes Involving Software**: Cause 5 - Overpressurization
- **Hazard Cause Description**: During FS RoCS and US ReCS fill operations, hydrazine servicing GSE fails to regulate flight hardware tank ullage pressure, causing flight hardware system overpressure.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-PYR-001
- **Title**: Inadvertent Ignition of Orion/Ares I Pyrotechnics During Final Ordnance Connections/Testing at LC-39 Pad B Results in Loss of Life, Flight Hardware, Facilities, and/or GSE
- **Hazard Causes Involving Software**: Cause 6 - Improper Pyrotechnic Initiator Controller (GO-PIC) resistance test
- **Hazard Cause Description**: Improper Pyrotechnic Initiator Controller (GO-PIC) resistance test at LC-39 Pad B due to overcurrent.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-003
- **Title**: Cryogenic Loading Operations At LC-39 Pad B Results In Loss of Life, Flight Hardware, Facilities, And/Or GSE
- **Hazard Causes Involving Software**: Cause 1 - Overpressurization/underpressurization of Cold GHe bottles and LH2/LO2 tanks
- **Hazard Cause Description**: The Cold GHe servicing GSE pressurizes the 10 helium bottles inside the hydrogen tank after the hydrogen tank is filled, and pressurizes the LH2 and LO2 tanks on the vehicle. Failure of the Cold GHe servicing GSE to regulate pressure and/or human error can cause flight hardware system overpressure/underpressure. Software is used to command GSE valves open and closed, to monitor pressure/temperature for the Cold GHe servicing GSE, and to monitor pressure/temperature measurements from the vehicle.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-003
- **Title**: Cryogenic Loading Operations At LC-39 Pad B Results In Loss of Life, Flight Hardware, Facilities, And/Or GSE
- **Hazard Causes Involving Software** Cause 4 - Premature Disconnect of Upper Stage (LH2,LO2, Instrument Unit [IU]) umbilicals
- **Hazard Cause Description**: Each US umbilical plate is held onto the vehicle by a single collet, and is commanded by the Launch Release System (LRS) to separate at T-0. Failure of the collet or an erroneous signal from the LRS can cause a premature disconnect. Premature disconnect during tanking may result in cryogenic leakage. Cryogenic contact with energized electrical connectors may result in fire/explosion.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-003
- **Title**: Cryogenic Loading Operations At LC-39 Pad B Results In Loss of Life, Flight Hardware, Facilities, And/Or GSE
- **Hazard Causes Involving Software**: Cause 6 - Overfill/Underfill of LO2 and LH2 tanks
- **Hazard Cause Description**: Overfill/underfill of cryogenics tanks due to the failure of the cryogenic servicing GSE fill valves. The cryogenic servicing GSE is remotely commanded by the LCS software to control valve positions and to monitor pressure and temperature transducers. The LCS will also receive pressure transducers and liquid sensor data from the vehicle during servicing operations.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-SVC-003
- **Title**: Cryogenic Loading Operations At LC-39 Pad B Results In Loss of Life, Flight Hardware, Facilities, And/Or GSE
- **Hazard Causes Involving Software**: Cause 8 - GH2 and GO2 overpressurization (Inability to vent GH2 and GO2)
- **Hazard Cause Description**: Failure to provide pneumatic pressure for the vehicle GH2/GO2 vent valves or the failure of the ground GH2 vent valve may result in the inability to vent GH2/GO2 from the vehicle, which may result in overpressurization of the vehicle hydrogen and/or oxygen tanks. Software is used to command GSE valves (which in turn open/close flight tank vent valves) and to monitor pressure transducers.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-CLO-001
- **Title**: Configuration of Integrated Vehicle During Closeout Activities Results in Loss of Life, Flight Hardware, Facilities and/or GSE.
- **Hazard Causes Involving Software**: Cause 7 - Impact/Collision (Crew Access Arm [CAA]) during retraction
- **Hazard Cause Description**: Retraction of the CAA/extendable platform will be performed remotely at around T-5 minutes using a sequence of Launch Control System (LCS) software commands. There exists the possibility of CAA/extendable platform impact/collision with the vehicle due to an erroneous software command (i.e., extend the CAA/extendable platform rather than retract the CAA/extendable platform) being issued. This includes the console operator manually issuing an improper command.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-LCH-001
- **Title**: Final Ares I/Orion Integrated Vehicle Launch Countdown Operations (Post-Cryogenic Servicing) Until the Vehicle Clears the LC-39 Pad B Mobile Launcher Tower Results in Loss of Life, Flight Hardware, Facilities, and/or GSE
- **Hazard Causes Involving Software**: Cause 2 - Premature separation (Service Module/First Stage Forward Skirt [SM/FSFS] Umbilicals, VSDS Arms)
- **Hazard Cause Description**: Premature separation due to collet failure or a non-commanded signal passing through the Launch Release Signal (LRS) Programmable Logic Controllers activating the release solenoids, causing a disconnection of the umbilicals (SM, FSFSU) and the Vehicle Stabilization and Damping Subsystem (VSDS) stabilizer and sway damper arms.

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-LCH-001
- **Title**: Final Ares I/Orion Integrated Vehicle Launch Countdown Operations (Post-Cryogenic Servicing) Until the Vehicle Clears the LC-39 Pad B Mobile Launcher Tower Results in Loss of Life, Flight Hardware, Facilities, and/or GSE
- **Hazard Causes Involving Software**: Cause 4 - Failure to provide ignition overpressure pulse protection
- **Hazard Cause Description**: Failure to provide ignition overpressure protection due to a failure in the IOP subsystem (software command failure to open the 48-inch butterfly valves, erroneous software command which prematurely closes the 48-inch butterfly valves, or a mechanical failure that occurs within the allotted time the 48-inch butterfly valves are to remain open).

Software Hazards in Operation Specific Hazard Reports

- **Report Number**: PAD-LCH-001
- **Title**: Final Ares I/Orion Integrated Vehicle Launch Countdown Operations (Post-Cryogenic Servicing) Until the Vehicle Clears the LC-39 Pad B Mobile Launcher Tower Results in Loss of Life, Flight Hardware, Facilities, and/or GSE
- **Hazard Causes Involving Software**: Cause 5 - Failure to separate (T-0 Umbilicals and Vehicle Stabilization and Damping Subsystem [VSDS] arms)
- **Hazard Cause Description**: During the First Stage (FS) ignition sequence a failure of the Launch Release System (LRS) to receive the T-0 umbilical release command from the vehicle (coupled with failure of the backup separation modes) would result in FS ignition without LRS T-0 umbilical release/retraction.

ICSQ
International Conference on Software Quality

Conclusion

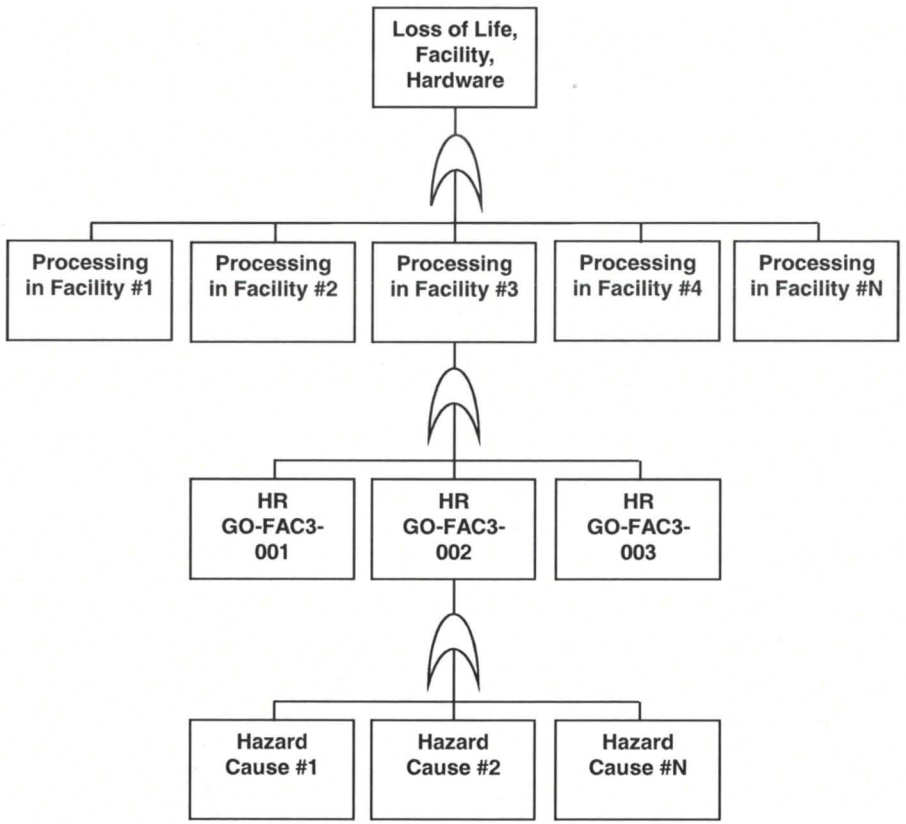
- The application of software safety practices on the LCS project resulted in the successful implementation of the NASA Software Safety Standard NASA-STD-8719.13B and CxP software safety requirements
- The GOP-GEN-GSW-011 Hazard Report was the first report developed at KSC to identify software hazard causes and their controls
- This approach can be applied to similar large software – intensive systems where loss of control can lead to a hazard

Backup

GO Hazard Analysis Structure

Generic Hazards (CxP 70038)
- Collision
- Loss of Control
- Contamination
- Corrosion
- Electrical Discharge/Shock
- Environmental/Weather
- Temperature Extremes
- Accelerations/Decelerations/ Gravitational Forces
- Electromagnetic Interference
- Radiation (Ionizing/Non-Ionizing)
- Explosion
- Fire/Overheat
- Flight Termination Systems
- Implosion/Loss of Pressure
- Pneumatic/Hydraulic Pressure Sources
- Impact from Debris
- Impact from Structural Failure
- Loss of Structural Integrity
- Mechanical
- Loss of Critical Function
- Loss of Safe Return Capability
- Loss of Habitable Environment (PPE/PVS and Breathable Air)
- Loss of Habitable Environment from Toxins/Contamination
- Pathological/Physiological/ Psychological
- Inadequate Human Factors
- Lasers
- Utility Outages
- Common Cause Failures

Operational Data Sources
- CxP 72119, GS Ops-Con Document
- CxP 72149, GO Planning Document
- Processing Facility Breakdown
- GSE/Facility System List (By Facility)



Ground Operations Top-Level Fault Tree Analysis

Processing Facility Breakdown
- RPSF (LAS – Pre-DD250)
- ARF (Aft Skirt – Pre-DD250)
- O&C (Orion – Pre-DD250)
- MPPF **(Orion)**
- RPSF (First Stage)
- VAB (Integration/Testing of Elements)
- Pad (Testing/Loading/Launch)
- Recovery Ships/Hangar AF (FS, CM)

SE&I/Element Hazard Analysis Data
- Element Hazard Causes (requiring GO hazard controls/verifications)
- Integrated Hazard Causes (requiring GO hazard controls/verifications)
- SE&I Functional Hazard Analysis (GO portion)
- Element Pre-DD250 Hazard Analyses (e.g., LAS [RPSF], Orion [O&C])

GO Hazard Analysis Data Sources
- SSP Hazard Reports/Critical Items
- SSP System Assurance Analyses
- SSP Ground Operational Risk Assessments
- Ares I-X Operating and Support Hazard Analyses
- Ares Level V SAAs (New/Modified)

ICSQ International Conference on Software Quality

Hazard Report Matrix

GOP-GEN-GSW-011	OSS-TST-001	OSS-SVC-002	OSS-SVC-003	ITC-TST-001	PAD-TST-001	PAD-SVC-001	PAD-SVC-002	PAD-PYR-001	PAD-SVC-003	PAD-CLO-001	PAD-LCH-001
C1		C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6, C8		C4, C5
C2		C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6, C8		C4
C3	C6	C3 (X3)	C3, C11	C6	C3	C5	C5	C6	C1, C4, C6, C8	C7	C2, C4, C5
C4	C6	C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C4, C6		C2
C5	C6	C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6	C7	
C6		C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6, C8		
C7		C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6, C8		C4, C5
C8		C3 (X3)	C3, C11	C6	C3	C5	C5		C1, C6, C8		C4
C9									C6, C8		C4
C10				C6							
C11	C6	C3 (X3)	C3, C11	C6	C3	C5	C5	C6	C1, C4, C6, C8	C7	C2, C4, C5
C12	C6	C3 (X3)	C3, C11	C6	C3	C5	C5	C6	C1, C4, C6, C8	C7	C2, C4, C5
C13	C6	C3 (X3)	C3, C11	C6	C3	C5	C5	C6	C1, C4, C6, C8	C7	C2, C4, C5
C14	C6	C3 (X3)	C3, C11	C6	C3	C5	C5	C6	C1, C4, C6, C8	C7	C2, C4, C5