National Aeronautics and Space Administration

NASA Hazard Analysis Process

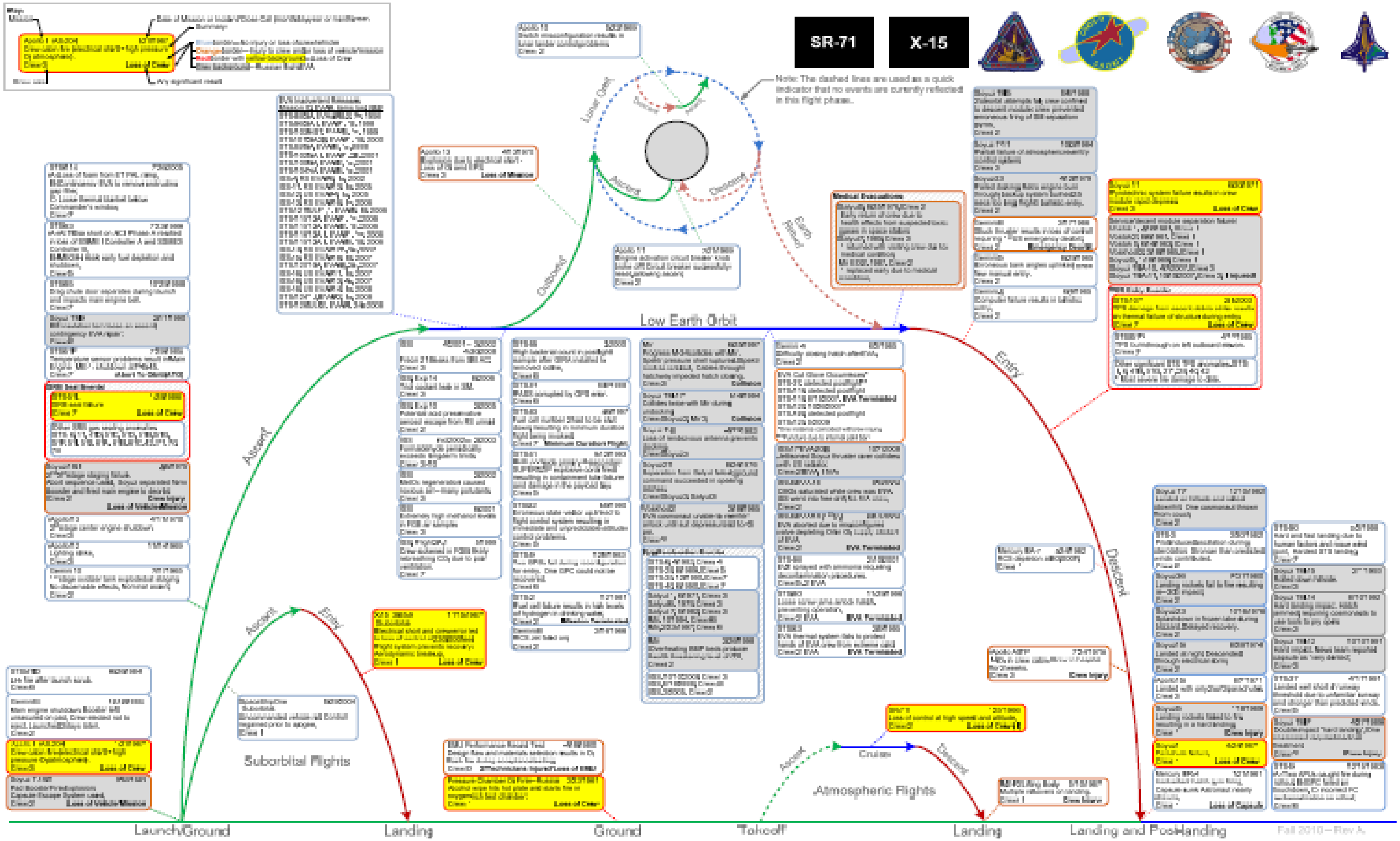
George Deckert

Johnson Space Center

Safety, Reliability and Mission Assurance Directorate

Significant Incidents and Close Calls in Human Spaceflight

A Product of the JSC S&MA Flight Safety Office



The *Significant Incidents and Close Calls in Human Spaceflight* graphic is primarily focused on human spaceflight incidents that have occurred while a crew was aboard a space vehicle. It includes suborbital, orbital, and lunar missions. The two ground facility events and two atmospheric flight events are included due to the significance of the events to spaceflight. The pressure chamber O_2 fire in Russia occurred prior to the loss of the Apollo 1 crew in an O_2 fire and could have served as a lesson learned had it been known in the US. The EMU fire resulted in the redesign of the EMU and heightened awareness of design and materials selection for man-rated systems using a pure O_2 environment. The M2-F2 lifting body accident occurred during the development of the space shuttle and yielded human engineering lessons learned. The SR-71 accident is the highest and fastest vehicle breakup on record that was survivable and it represents the demonstrated limit of crew survival with currently fielded technologies. *Note: This document is a work in progress. It is continually under review and frequently updated. Please direct comments and questions to the Flight Safety Office contacts at right.*

Acronyms

APU	Auxiliary Power Unit
ATO	Abort to Orbit
CDRA	Carbon Dioxide Removal System
CMG	Control Moment Gyroscope
CO	Carbon Monoxide
CO_2	Carbon Dioxide
DM	Descent Module
EMU	Extravehicular Mobility Unit
EPS	Electrical Power System
EV	Extravehicular
EVA	Extravehicular Activity
FC	Flight Control
FSO	Flight Safety Office
GIRA	Galley Iodine Removal Assembly
GPC	General Purpose Computer
GPS	Global Positioning System
H_2	Hydrogen
ISS	International Space Station
LH_2	Liquid Hydrogen
LOC	Loss of Crew
LOV	Loss of Vehicle
ME	Main Engine
MetOx	Metal Oxide
MMOD	Micro-Meteoroid Orbital Debris
N_2O_4	Nitrogen Tetroxide
O_2	Oxygen
OM	Orbital Module
OSMA	Office of Safety & Mission Assurance
PAL	Protuberance Air Load
PASS	Primary Avionics Software System
RCS	Reaction Control System/Subsystem
RIP	Rapid Information Page
S&MA	Safety & Mission Assurance
SM	Service Module
SRB	Solid Rocket Booster
SSME	Space Shuttle Main Engine
SSP	Space Shuttle Program
TPS	Thermal Protection System

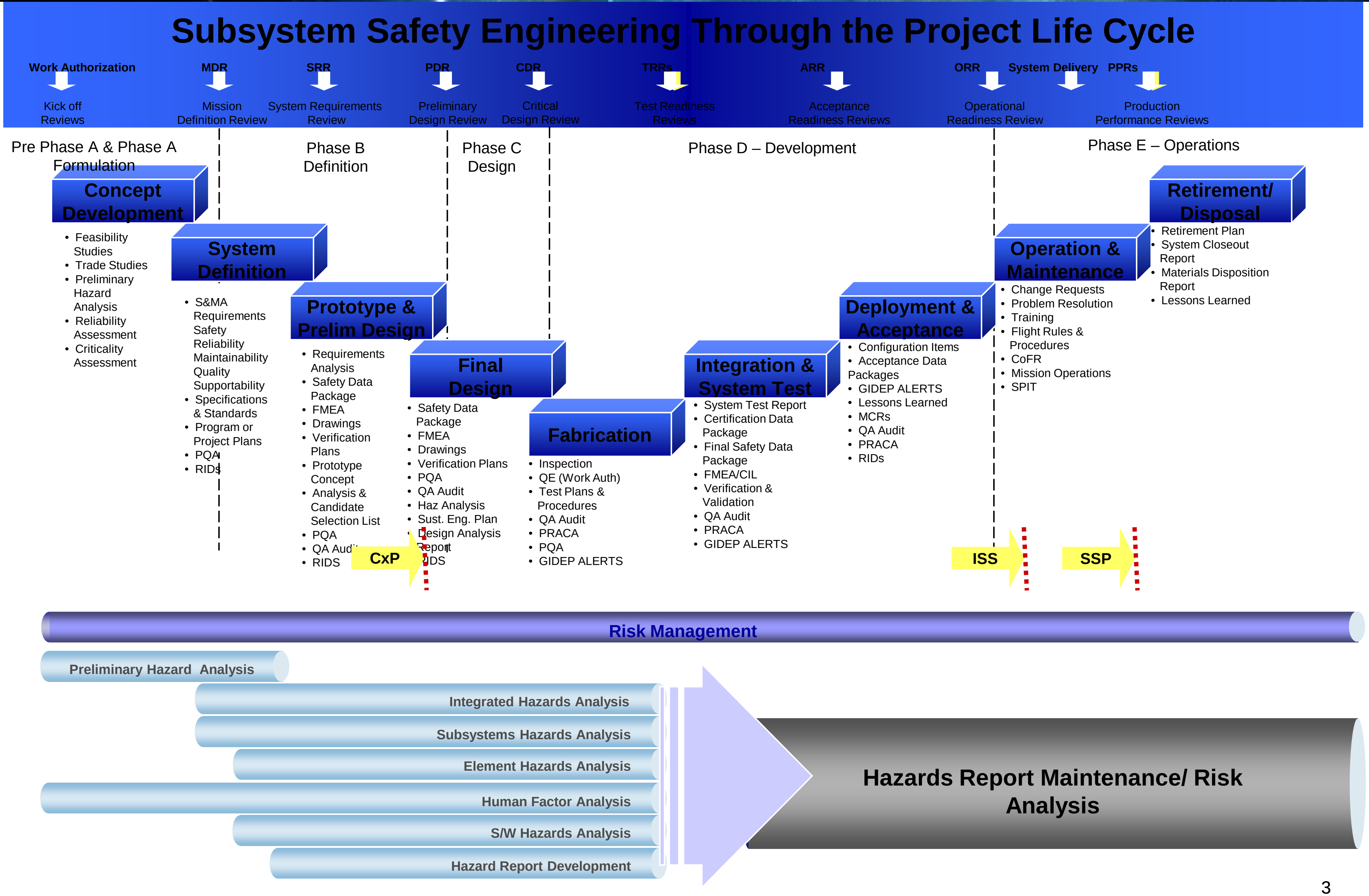
Contacts

David Thelen, NASA
Manager, JSC S&MA Flight Safety Office
[illegible]

Bill Wood, SAIC
Manager, Flight Safety/Integration Office
[illegible]

Dennis Pate, SAIC
Assessments Specialist, FSO Issue Resolution Team
[illegible]

Subsystem Safety Engineering Through the Project Life Cycle



Subsystem Safety Engineering Through the Project Life Cycle

Work Authorization – Kick off Reviews

MDR – Mission Definition Review

SRR – System Requirements Review

PDR – Preliminary Design Review

CDR – Critical Design Review

TRRs – Test Readiness Reviews

ARR – Acceptance Readiness Reviews

ORR – Operational Readiness Review

System Delivery

PPRs – Production Performance Reviews

Pre Phase A & Phase A Formulation

Phase B Definition

Phase C Design

Phase D – Development

Phase E – Operations

Concept Development

- Feasibility Studies
- Trade Studies
- Preliminary Hazard Analysis
- Reliability Assessment
- Criticality Assessment

System Definition

- S&MA Requirements Safety Reliability Maintainability Quality Supportability
- Specifications & Standards
- Program or Project Plans
- PQA
- RIDS

Prototype & Prelim Design

- Requirements Analysis
- Safety Data Package
- FMEA
- Drawings
- Verification Plans
- Prototype Concept
- Analysis & Candidate Selection List
- PQA
- QA Audit
- RIDS

Final Design

- Safety Data Package
- FMEA
- Drawings
- Verification Plans
- PQA
- QA Audit
- Haz Analysis
- Sust. Eng. Plan
- Design Analysis Report
- RIDS

Fabrication

- Inspection
- QE (Work Auth)
- Test Plans & Procedures
- QA Audit
- PRACA
- PQA
- GIDEP ALERTS

Integration & System Test

- System Test Report
- Certification Data Package
- Final Safety Data Package
- FMEA/CIL
- Verification & Validation
- QA Audit
- PRACA
- GIDEP ALERTS

Deployment & Acceptance

- Configuration Items
- Acceptance Data Packages
- GIDEP ALERTS
- Lessons Learned
- MCRs
- QA Audit
- PRACA
- RIDs

Operation & Maintenance

- Change Requests
- Problem Resolution
- Training
- Flight Rules & Procedures
- CoFR
- Mission Operations
- SPIT

Retirement/ Disposal

- Retirement Plan
- System Closeout Report
- Materials Disposition Report
- Lessons Learned

CxP

ISS

SSP

Risk Management

Preliminary Hazard Analysis

Integrated Hazards Analysis

Subsystems Hazards Analysis

Element Hazards Analysis

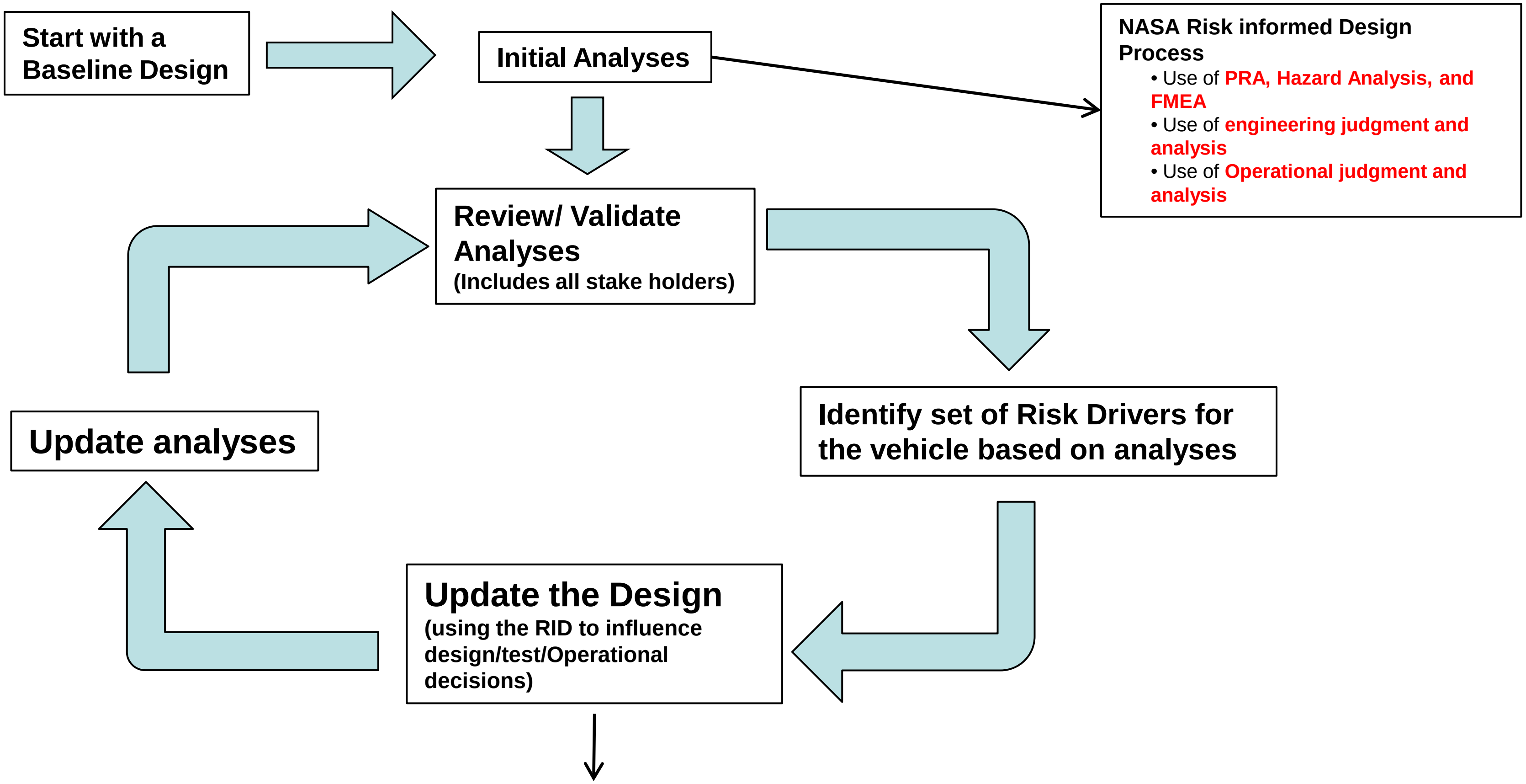
Human Factor Analysis

S/W Hazards Analysis

Hazard Report Development

Hazards Report Maintenance/ Risk Analysis

The Risk Informed Design Process



Start with a Baseline Design

Initial Analyses

NASA Risk informed Design Process

- Use of **PRA, Hazard Analysis, and FMEA**
- Use of **engineering judgment and analysis**
- Use of **Operational judgment and analysis**

Review/ Validate Analyses
(Includes all stake holders)

Identify set of Risk Drivers for the vehicle based on analyses

Update the Design
(using the RID to influence design/test/Operational decisions)

Update analyses

- The process is a continuous process throughout the lifecycle of the Project
- At each design and verification cycle, work to reduce the risk drivers
    - Focus on the Top Drivers to maximize impact
- When new drivers emerge (new cycles) as Top Drivers, work those drivers
- Key decision points emerge at various program milestones (e.g. Achievability)

Types of NASA Hazard Analysis

- Preliminary Hazard Analysis
- Subsystem Hazard Analysis
- Element Hazard Analysis
- Operating and Support Hazard Analysis
- Software Hazard Analysis
- Integrated Hazard Analysis
- Functional Hazard Analysis

Preliminary Hazard Analysis (PHA)

- The PHA is the initial effort in hazard analysis during the early design phases that identifies top level hazards and controls, provides a first look at the system risk, and provides the foundation for future analyses. It is based on the best available data. Sources for data include but are not limited to: system description documents, system diagrams, mission descriptions, operational concepts, functional analysis/architecture documents, Functional Flow Block Diagrams (FFBDs), mishap data from similar systems, and lessons learned from other projects. The PHA identifies and evaluates the hazards and hazardous events associated with the proposed design or functions for potential hazard severity, probability, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented.

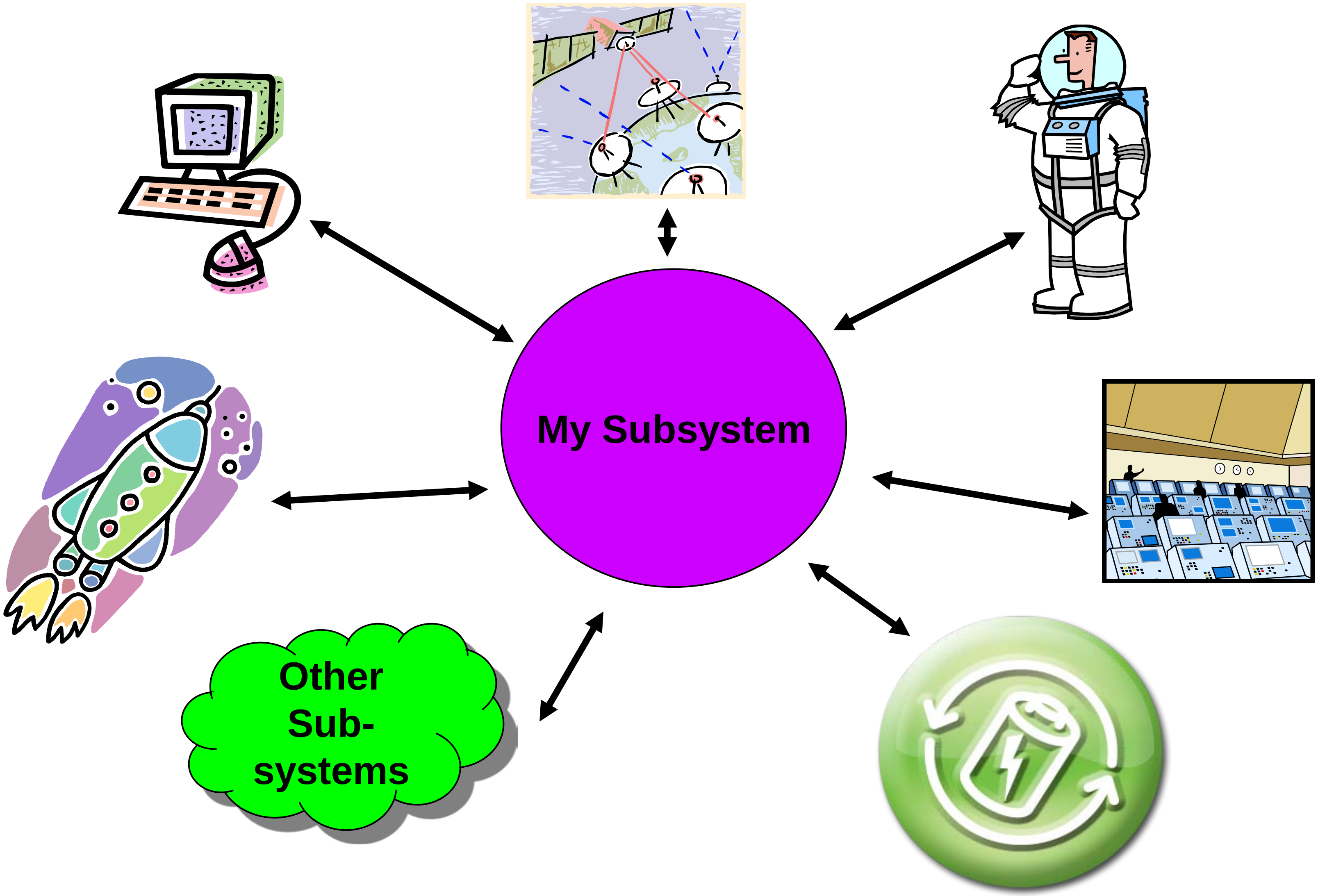
Hazard Analysis Process

- Identify hazardous conditions, events or states
- Identify the effect of the hazardous state
- Identify severity of the effect
- Identify all potential causes of the hazardous states
- Identify controls for each of the hazard causes
- Identify likelihood of each cause
- Identify verification strategies for the controls
- Track verification to closure

Identify Hazardous Conditions

- Basically this is a brainstorming exercise!
- What is inherently dangerous about the operation of your system?
  - Standard hazard lists
  - Historical experience/documentation from legacy systems
  - Your engineering training and experience

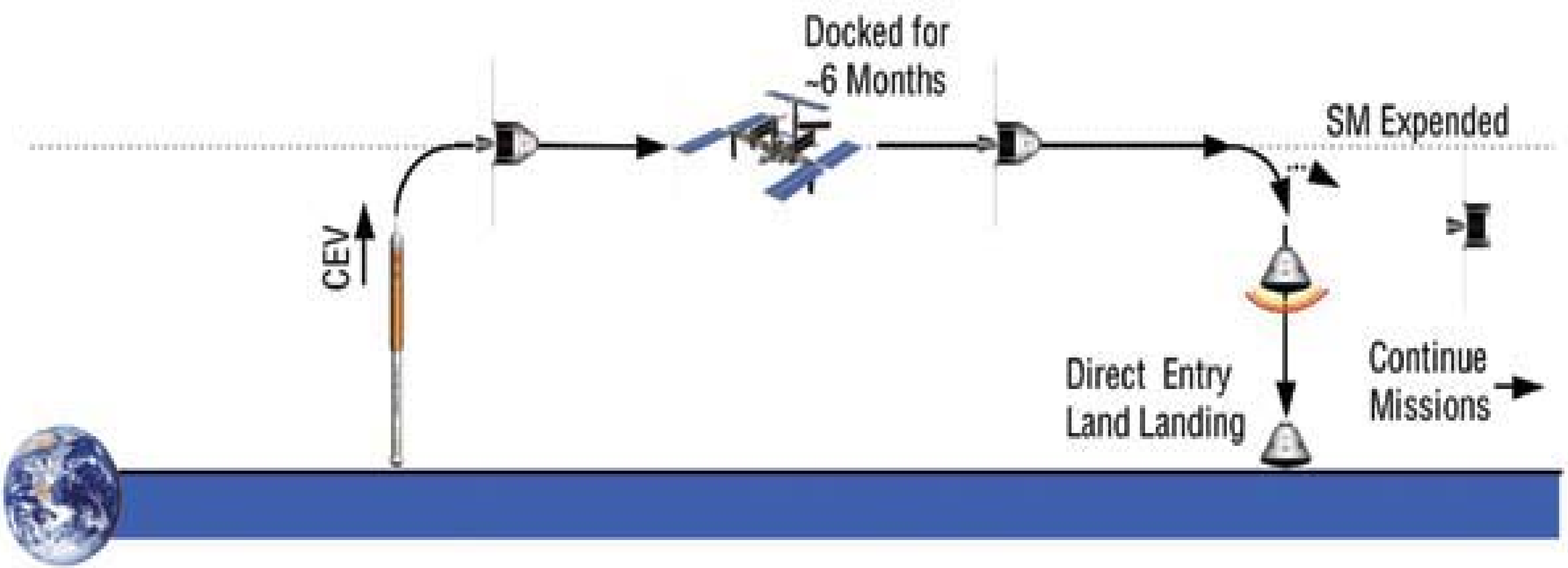
Consider all Interfaces



My Subsystem

Other Sub-systems

Example



- ISS Crew Transport Mission
  - Launch a crew to the International Space Station
  - Stay docked to the Space Station for 6 months
  - Return the crew to Earth and land in the water

Work a Preliminary Hazard List

- Identify the hazards for this mission.

NASA Generic Hazards List

- Collision or Impacts
- Loss of Control
- Contamination
- Corrosion
- Electrical Discharge/Shock
- Environmental/Weather
- Temperature Extremes
- Gravitational Forces
- Electromagnetic Interference
- Radiation
- Explosion
- Fire/Overheat
- Flight Termination Systems
- Implosion/Loss of Pressure
- High Pressure Sources
- Loss of Structural Integrity
- Mechanical
- Loss of Critical Function
- Loss of Safe Return Capability
- Loss of Habitable Environment
- Pathological/Physiological/ Psychological
- Inadequate HF Engineering
- Lasers
- Utility Outages
- Common Cause Failures

- Hazard analysis results in the identification of risks and the means of controlling or eliminating them. Hazard analysis also quantifies the risk for the Program/Project Manager.

Final Thoughts

- Hazard analysis is structured process to
  - Identify risk
  - Classify risk
  - Manage risk
- Hazard analysis is not an exact science
  - Relies on engineering expertise and engineering judgment
  - Requires rationale to justify hazard classification
- Hazard analysis is an important tool in
  - Design Process
  - Requirements Validation
  - Risk Management