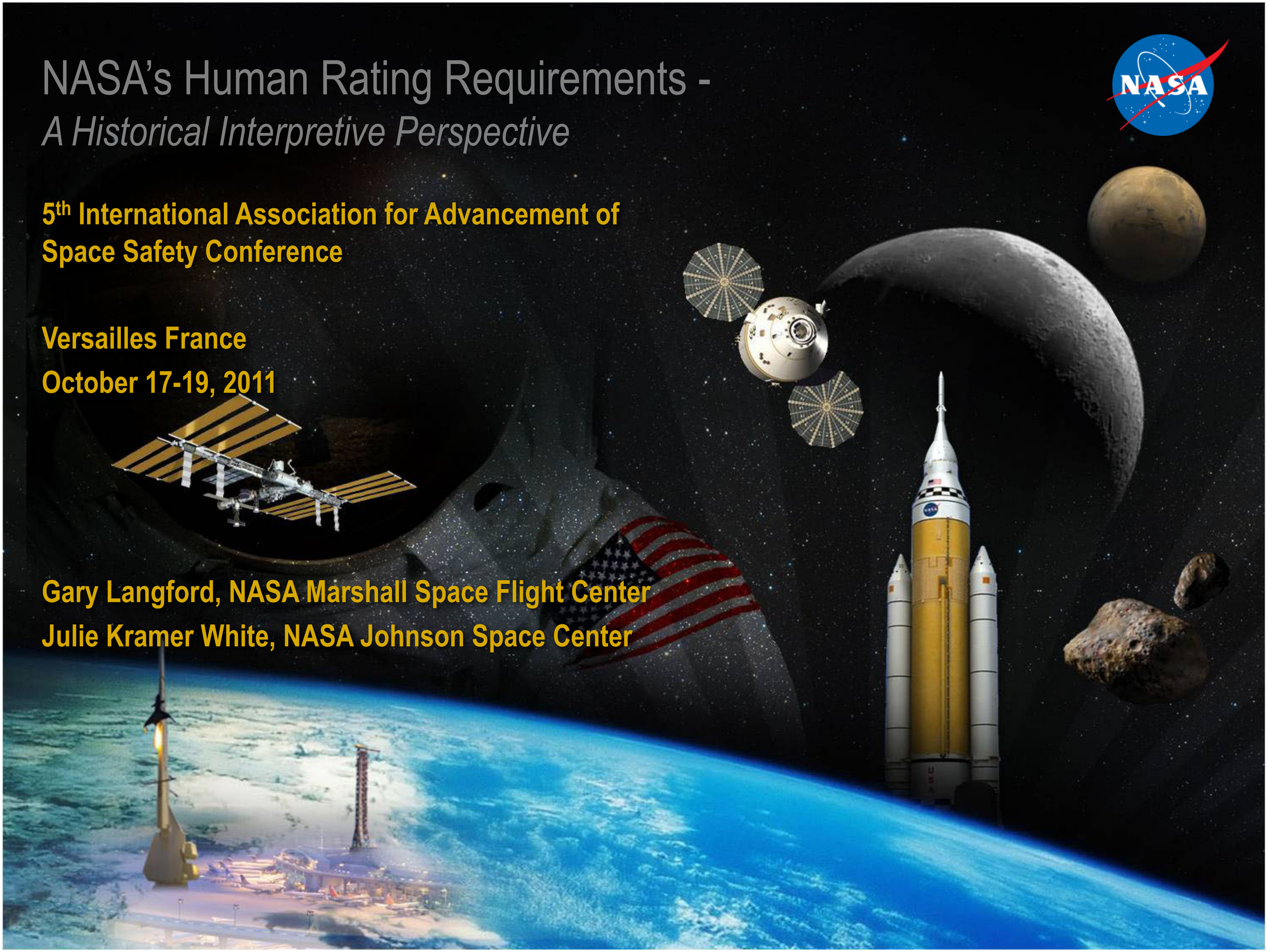
NASA's Human Rating Requirements A Historical Interpretive Perspective

Section 3.0 of NASA's Human Rating Requirements for Space Systems, NPR 8705.2, represents technical engineering requirements that the Agency requires of Human Space Systems. In many cases the requirements are not unlike requirements for any space system, crewed or uncrewed, they deal with successfully accomplishing the mission objectives. However, they go one step further and have requirements that go beyond successful completion of the mission and dictate functions or actions necessary to assure the survival of the crew. In that regard they are unique from other space system requirements. Even with their uniqueness the technical requirements of the NPR 8705.2 have been relatively unchanged in overall intent over the revisions. They all have provided for system redundancy, crew habitable environment, crew situational awareness, crew operation, system control, emergency egress and abort systems. In a few cases the intent of the requirement was changed intentionally, either to restrict certain types of systems or their functions, or to encompass lessons learned from previous programs. For the most part the requirements are non controversial and represent the current best practices for human space systems, however, a few requirements are always debated and have evolved over revisions of the NPR due to studies conducted with various programs like the Orbital Space Plane and the Constellation Programs. Those requirements will be discussed using results of trade studies conducted during past programs highlighting how these particular requirements have evolved through the revisions of the NPR. Comments will also be provided for requirements that although not debated, have provided challenges in interpretation.



NASA's Human Rating Requirements -

A Historical Interpretive Perspective

5th International Association for Advancement of Space Safety Conference

Versailles France

October 17-19, 2011

Gary Langford, NASA Marshall Space Flight Center

Julie Kramer White, NASA Johnson Space Center

What is a “Human Rated” System?

*“The concept of a man-rated space system entails the incorporation of those **design features and requirements necessary to accommodate human participants** within the system and thus provide the capability to safely conduct manned operations, including **safe recovery from any credible emergency situation**. Man-rating is the process of evaluating and assuring that the total system, both hardware and software, has the ability to meet prescribed**, safety oriented design and operational criteria and requirements**, and becomes involved in all program activities including design and development, test and verification, management and control and finally, certification for operational readiness”*

“A Review of Man-Rating in Past and Current Manned Space Flight Programs”, A. Bond, 1988

Tenants of Human Rating per NPR 8705.2B

The fundamental intent has not changed over the decades…

Human rating is the process of designing, evaluating and assuring that the total system can safely conduct the mission.

- Managing risk in a highly constrained situation
- Exploring risk and uncertainty
- Hazard identification and control.

A system design that accommodates and utilizes human capabilities and system interactions

- Providing for basic human needs
- Providing insight and control

A system that provides the capability to safely recover the crew

- Acknowledgement of inherent risk and unpredictability of hazards in human spaceflight

Evolution of Implementation

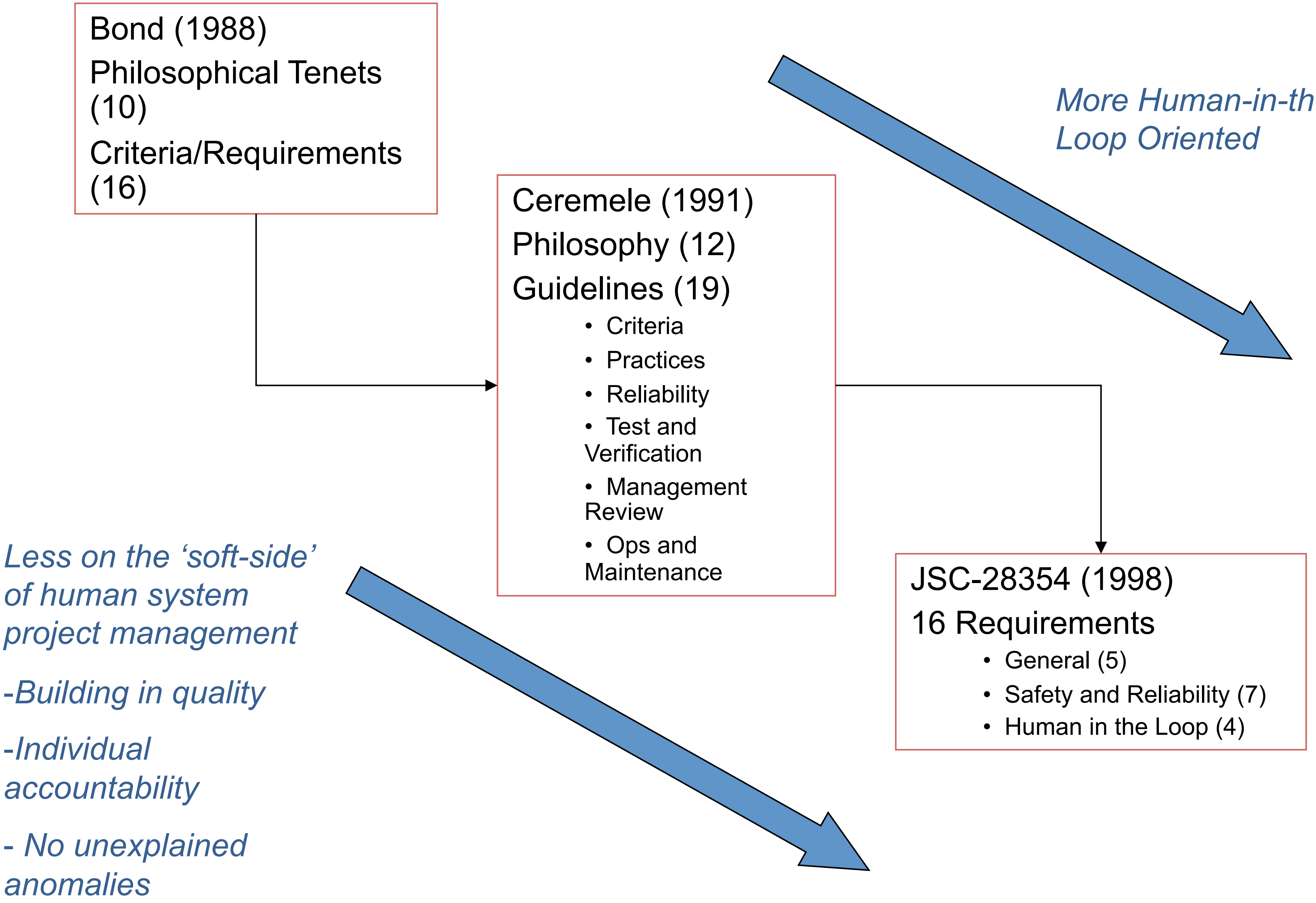
As the Agency has attempted to codify these Human Rating best practices, they have struggled with the limitations of the English language, consensus requirements development and artificial constraints of "Rules for Rules" of requirements writing, the latest revisions acknowledges this limitation explicitly…

"It is impossible to develop a set of Agency-level technical requirements that will definitively result in the development of safe systems for all human space missions…"

"These technical requirements should not be interpreted as all inclusive or absolute"

"The Project Manager is expected to evaluate the intent of these technical requirements and use the talents of the development and operation team to design the safest practical system that will accomplish the mission within the constraints" [mass, volume, cost and schedule]

Evolution of Requirements/Guidelines



Bond (1988)

Philosophical Tenets (10)

Criteria/Requirements (16)

Ceremele (1991)

Philosophy (12)

Guidelines (19)

- Criteria
- Practices
- Reliability
- Test and Verification
- Management Review
- Ops and Maintenance

JSC-28354 (1998)

16 Requirements

- General (5)
- Safety and Reliability (7)
- Human in the Loop (4)

More Human-in-the-Loop Oriented

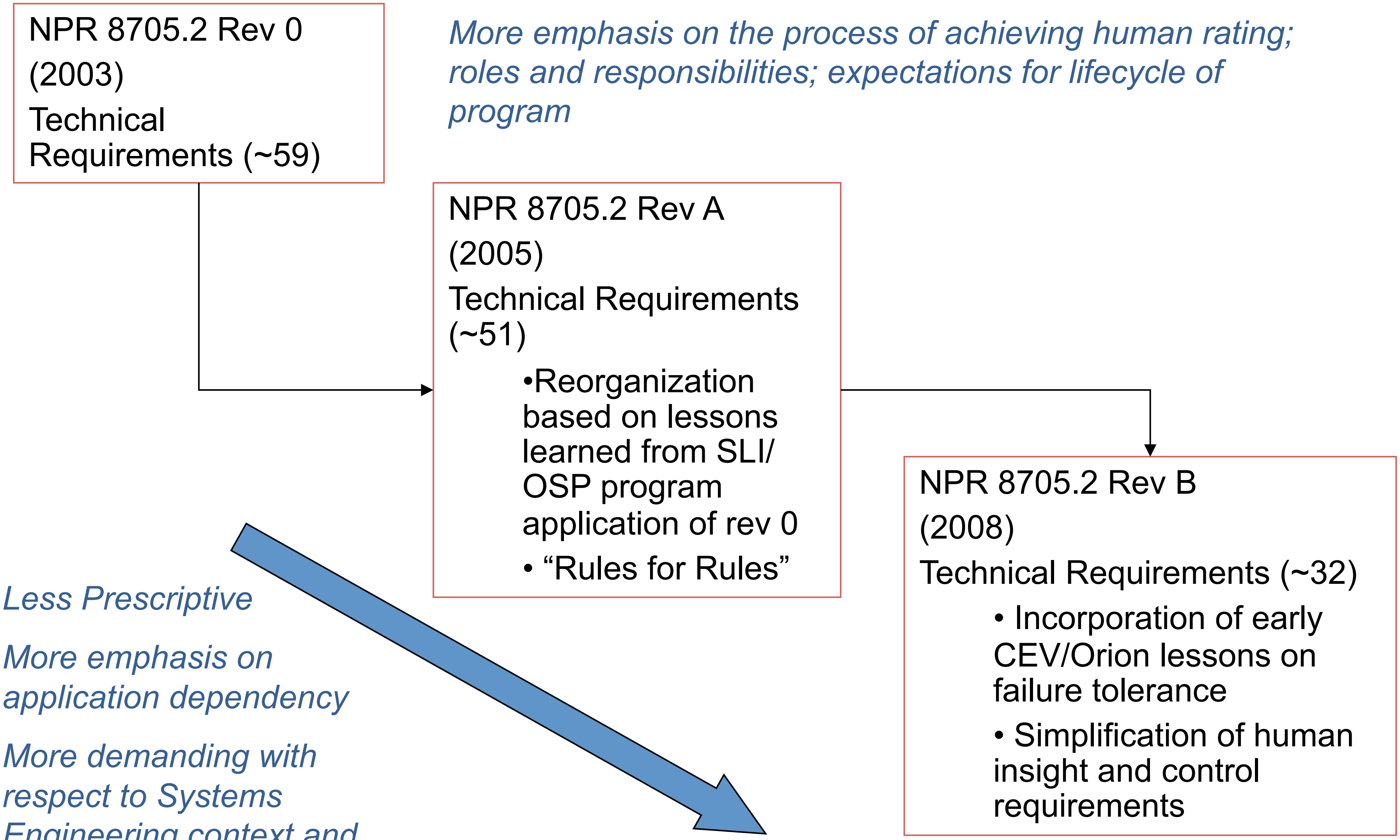
Less on the 'soft-side' of human system project management

-Building in quality

-Individual accountability

- No unexplained anomalies

Evolution of Requirements/Guidelines



NPR 8705.2 Rev 0 (2003)

Technical Requirements (~59)

More emphasis on the process of achieving human rating; roles and responsibilities; expectations for lifecycle of program

NPR 8705.2 Rev A (2005)

Technical Requirements (~51)

- Reorganization based on lessons learned from SLI/ OSP program application of rev 0
- "Rules for Rules"

NPR 8705.2 Rev B (2008)

Technical Requirements (~32)

- Incorporation of early CEV/Orion lessons on failure tolerance
- Simplification of human insight and control requirements

Less Prescriptive

More emphasis on application dependency

More demanding with respect to Systems Engineering context and analysis

The Pareto Principle or the 80/20 Rule

20 percent of the requirements will result in 80 percent of the debate with regard to implementation

- **There is always a fundamental debate about reliability driven design vs. prescriptive design features**
  - It remains NASA's position, for NASA Human Systems, that some level of prescription remains appropriate due to the inability to validate reliability driven analysis
- **Historically, and with Space Launch Initiative/Orbital Space Plane (SLI/OSP) and Constellation as most recent test cases, there are a small number requirements which always generate the most consternation**
  - Fault Tolerance Requirements (Hardware, Human Error and Software)
  - Crew Escape/Abort and Emergency Systems
  - Manual Control/Human-in-the-loop Requirements

Fault Tolerance (hardware, human error and software)

Requirement	JSC 28354 (1998)	Baseline NPR (2003)	REV A (2005)	REV B (2008)
Failure Tolerance	All critical systems essential for crew safety shall be designed to be two-fault tolerant. When this is not practical, systems shall be designed so that no single failure shall cause loss of the crew.	All human-rated space flight systems shall be designed so that no two failures shall result in permanent disability or loss of life.	Space systems shall be designed so that no two failures result in crew or passenger fatality or permanent disability	The space system shall provide failure tolerance to catastrophic events (minimum of one failure tolerant), with the specific level of failure tolerance (one, two or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis .
Requirement	**JSC 28354 (1998)**	**Baseline NPR (2003)**	**REV A (2005)**	**REV B (2008)**
Emergency Systems	-	Emergency systems (such as fire suppression and crew escape) shall not be considered to satisfy failure tolerance requirements; however, these systems may be utilized in evaluation of failure mitigation and in reducing probability of loss of life	The space system shall provide the failure tolerance capability in 3.2.2 without the use of emergency equipment and systems (Requirement).	The space system shall provide the failure tolerance capability in 3.2.2 without the use of emergency equipment and systems

Fault Tolerance

- **Requirement most debated. Debates range from:**
  - ‘Should be a reliability requirement’
  - ‘Fully two failure tolerant’ (Shuttle/International Space Station)
- **Orbital Space Plane Program began to change paradigm.**
  - Use of commercial Expendable Launch Vehicle (ELV) fleet (Delta IV/ Atlas V)
  - Precedent from Mercury/Gemini Program.
    - Some added redundancy
    - Manned Space Flight Awareness Program
  - Saturn V/Shuttle developed exclusively for human flights
- **Rev A tried to address Lessons Learned from SLI/OSP.**
  - Applied exceptions to two failure tolerance.
    - Failure tolerance not practical
    - Added FT no longer reduces risk
    - Design For Minimum Risk (DFMR)
  - Resultant Process was to start at two failure tolerance and provide rationale for exclusions to the requirement.

Failure Tolerance (FT)

- **Cx Identified Issues with Rev A**
  - Very strict 2 Fault Tolerance interpretation
  - Reliability. Historic data showed that in some cases adding failure tolerance beyond a certain level did little to improve reliability for launchers. 0 to 1 shows marked improvement, 1 to 2 very little.
  - Rev A did not exclude use of abort for failure tolerance.

Rev A implementation:

- *Ares had avionics architectures that were either 3 or 4 strings depending on whether Abort was counted as part of FT.*
- *Orion weight challenges exacerbated by stove-piped 3 and 4 string systems.*

- **Changes Were Made for Rev B**
  - Allowed a minimum of single FT. Requires levels of FT to be justified in a provided Integrated Safety Analysis.
  - Reliability becomes a commodity like mass or power
  - Explicitly excluded ascent abort as a method of meeting the failure tolerance. Allowed for mission termination (early end of mission) on orbit as a method of meeting failure tolerance.

Rev B implementation:

- *Ares avionics architecture fixed at three strings.*
- *Orion started a weight scrubbing exercise that started at single FT and had systems buy into more redundancy as required to meet mission objectives and reliability goals resulting in two FT in key, high risk systems, including avionics. In critical systems where single FT was allowed, cross strapping of strings was employed to retain degraded operation after the second failure.*

Conclusion: Although failure tolerance is an important requirement it should not be looked at solely alone but in combination with reliability predictions and overall mission objectives.

Human Error

Requirement	JSC 28354 (1998)	Baseline NPR (2003)	REV A (2005)	REV B (2008)
Human Error	-	All human-rated space flight systems shall be designed so that neither two human errors during operation or in-flight maintenance nor a combination of one human error and one failure shall result in permanent disability or loss of life.	The system shall be designed and operated so that neither two inadvertent actions during operation or in-flight maintenance nor a combination of one inadvertent action and one failure result in crew or passenger fatality or permanent disability.	The space system shall be designed to tolerate inadvertent operator action (minimum of one inadvertent action), as identified by the human error analysis (paragraph 2.3.11), without causing a catastrophic event

Human Error

- Baseline version of NASA Procedural Requirements (NPR) dictated two error tolerance for all types of human error, both omission and commission.
- During the Rev A rewrite the Crew Office noted that some of that implementation in the ISS program was ‘over-bearing’ and did little to enhance safety.
- Argued that inadvertent actions was more the culprit. Protecting against other errors lead to a more complicated system prone to other errors.
- Rev A was then changed to reflect a two inadvertent error requirement.
- Subsequently Rev B was changed to be similar to the fault tolerance requirement requiring a minimum of one error tolerance (inadvertent action).
- Levels of error tolerance must be justified as part of integrated safety analysis.

Conclusion: Just as in failure tolerance, levels of human error protection should be governed by analysis of potential errors and criticality of those errors.

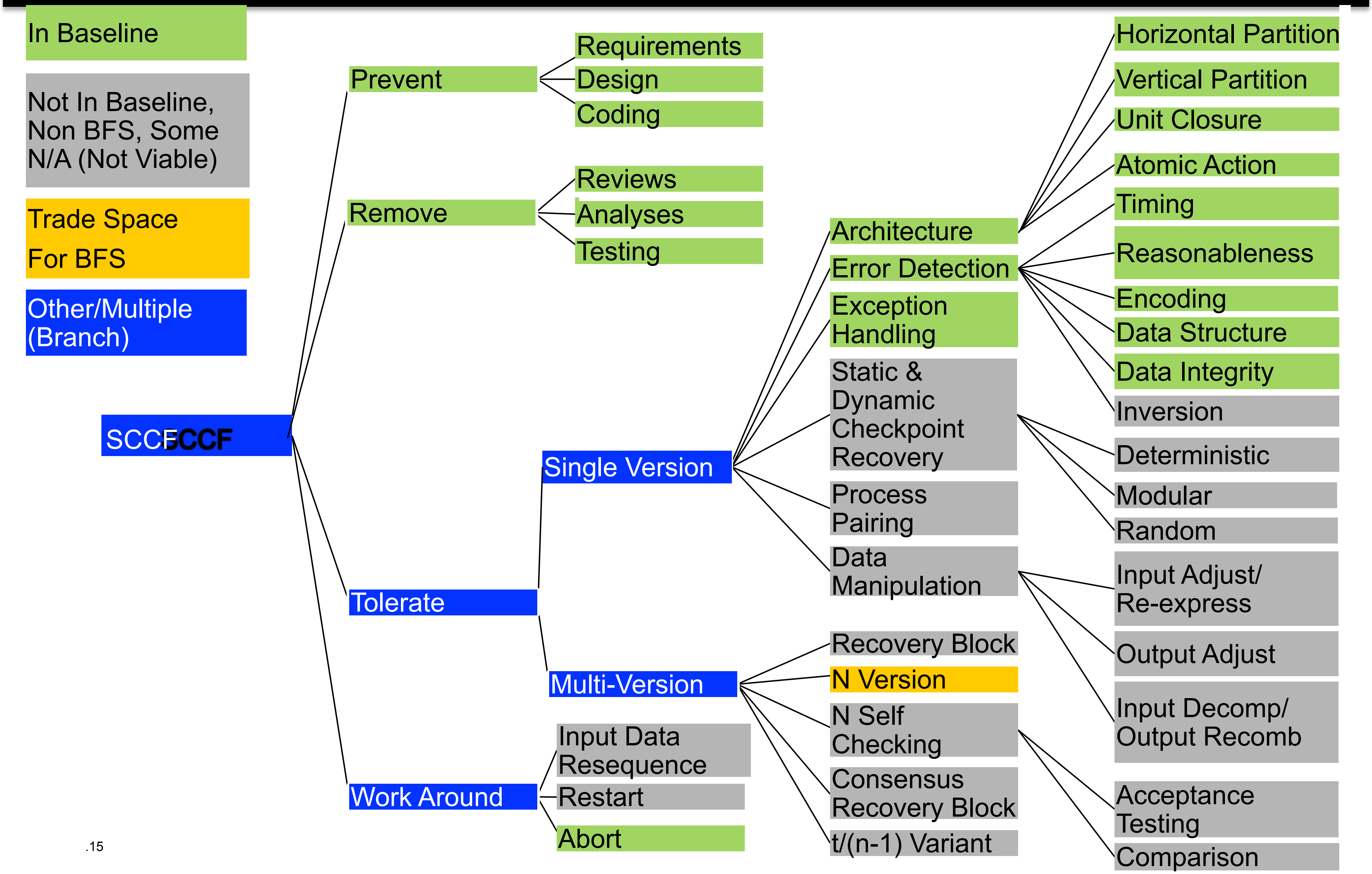
Fault Tolerance (hardware, human error and software)

Requirement	JSC 28354 (1998)	Baseline NPR (2003)	REV A (2005)	REV B (2008)
Software Failure	-	The control of vehicle flight path and attitude, during dynamic phases of flight such as ascent and entry, shall be provided by independently developed and redundant software systems.	The system design shall prevent or mitigate the effects of common cause failures in time-critical software (e.g., flight control software during dynamic phases of flight such as ascent. i. Redundant independent software running on a redundant identical flight computer ii. Use of an alternate guidance platform, computer and software iii. Use of nearly identical source code uniquely compiled for different dissimilar processors.	The space system shall provide the capability to mitigate the hazardous behavior of critical software where the hazardous behavior would result in a catastrophic event.

Software Failure Mitigation

- **First instantiation of independently developed and coded Backup Flight Control System (BFCS or BFS) shows up in the baseline version of the NPR (Rev 0).**
- **Historic first implementation is in the Space Shuttle Program**
  - Concerns with software error forcing all four computers to fail resulted in addition of a 5th computer with independently developed source code specifically for the dynamic phases of flight (ascent and reentry).
  - Crew could select between them.
- **EELVs for OSP did not have BFS.**
  - Program argued for alternate methods of achieving the same levels of reliability
    - Boeing 777 approach of "same" code on different compilers on dissimilar processors.
    - Use of spacecraft guidance and control for a backup of launch vehicle
- **Rev A of the NPR allowed for alternate methods.**
- **Constellation Program conducted agency wide trade study on BFS for ascent and came to the conclusion it was not required.**
  - Ares Project concluded BFS was not necessary for their brief duration mission
  - Orion Project concluded BFS was appropriate for crewed spacecraft
- **Rev B of NPR modified to current version eliminating redundancy as an absolute requirement for flight SW.**

Software Fault Tolerance Options
And Associated Trade Tree Analysis (Ares-like)



- 🟩 In Baseline
- ▨ Not In Baseline, Non BFS, Some N/A (Not Viable)
- 🟨 Trade Space For BFS
- 🟦 Other/Multiple (Branch)

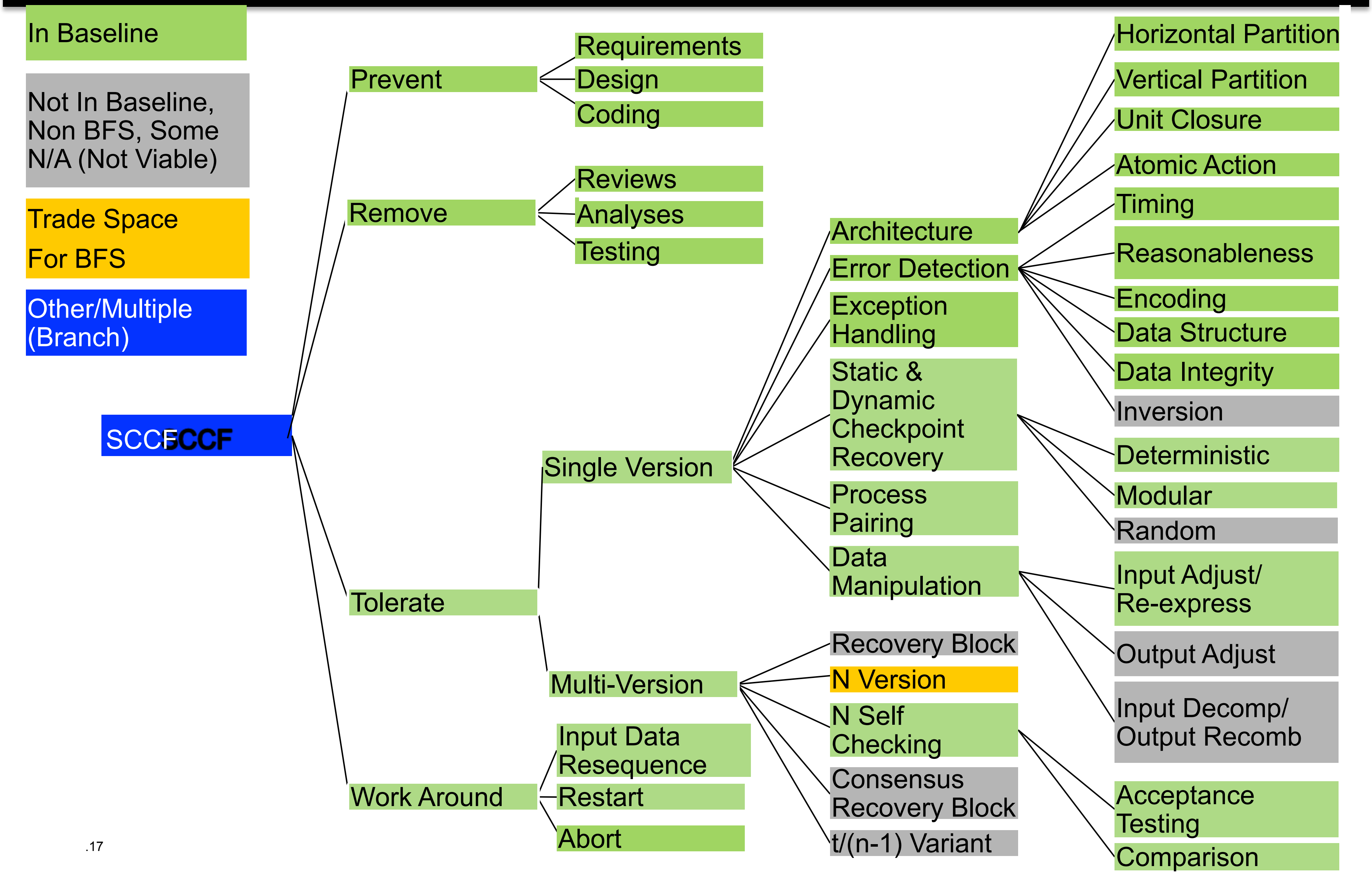
- 🟦 SCCF
  CCF
  - 🟩 Prevent
    - 🟩 Requirements
    - 🟩 Design
    - 🟩 Coding
  - 🟩 Remove
    - 🟩 Reviews
    - 🟩 Analyses
    - 🟩 Testing
  - 🟦 Tolerate
    - 🟦 Single Version
      - 🟩 Architecture
        - 🟩 Horizontal Partition
        - 🟩 Vertical Partition
        - 🟩 Unit Closure
        - 🟩 Atomic Action
        - 🟩 Timing
      - 🟩 Error Detection
        - 🟩 Timing
        - 🟩 Reasonableness
        - 🟩 Encoding
        - 🟩 Data Structure
        - 🟩 Data Integrity
        - ▨ Inversion
      - 🟩 Exception Handling
      - ▨ Static & Dynamic Checkpoint Recovery
        - ▨ Deterministic
        - ▨ Modular
        - ▨ Random
      - ▨ Process Pairing
      - ▨ Data Manipulation
        - ▨ Input Adjust/ Re-express
        - ▨ Output Adjust
        - ▨ Input Decomp/ Output Recomb
    - 🟦 Multi-Version
      - ▨ Recovery Block
      - 🟨 N Version
      - ▨ N Self Checking
        - ▨ Acceptance Testing
        - ▨ Comparison
      - ▨ Consensus Recovery Block
      - ▨ t/(n-1) Variant
  - 🟦 Work Around
    - ▨ Input Data Resequence
    - ▨ Restart
    - 🟩 Abort

.15

SW Failure

- **Results of Trade Study (Ares)**
  - BFS not required in response to primary flight software common cause failure.
  - Risk based on time of flight, code complexity (and size), and coding techniques employed deemed low enough to not justify the added expenditure. (20-40% of primary load).
  - Baseline coding techniques shown in trade tree deemed sufficient to meet the intent of NPR 8705.2b.
  - Trade study left the SW architecture in baseline form.

Software Fault Tolerance Options
And Associated Trade Tree Analysis (Orion-like)



- 🟩 In Baseline
- ▨ Not In Baseline, Non BFS, Some N/A (Not Viable)
- 🟨 Trade Space For BFS
- 🟦 Other/Multiple (Branch)

- 🟦 SCCFCCF
  - 🟩 Prevent
    - 🟩 Requirements
    - 🟩 Design
    - 🟩 Coding
  - 🟩 Remove
    - 🟩 Reviews
    - 🟩 Analyses
    - 🟩 Testing
  - 🟩 Tolerate
    - 🟩 Single Version
      - 🟩 Architecture
        - 🟩 Horizontal Partition
        - 🟩 Vertical Partition
        - 🟩 Unit Closure
        - 🟩 Atomic Action
      - 🟩 Error Detection
        - 🟩 Timing
        - 🟩 Reasonableness
        - 🟩 Encoding
        - 🟩 Data Structure
        - 🟩 Data Integrity
        - ▨ Inversion
      - 🟩 Exception Handling
      - 🟩 Static & Dynamic Checkpoint Recovery
        - 🟩 Deterministic
        - 🟩 Modular
        - ▨ Random
      - 🟩 Process Pairing
      - 🟩 Data Manipulation
        - 🟩 Input Adjust/ Re-express
        - ▨ Output Adjust
        - ▨ Input Decomp/ Output Recomb
    - 🟩 Multi-Version
      - ▨ Recovery Block
      - 🟨 N Version
      - 🟩 N Self Checking
        - 🟩 Acceptance Testing
        - 🟩 Comparison
      - ▨ Consensus Recovery Block
      - ▨ t/(n-1) Variant
  - 🟩 Work Around
    - 🟩 Input Data Resequence
    - 🟩 Restart
    - 🟩 Abort

SW Failure

- **Results of Trade Study (Orion)**
  - BFCS capability required in response to primary flight software common cause failure by using dissimilar hardware and software
  - BFCS coverage targeted to survive the crisis – not to duplicate all primary software capabilities. Assumes primary software can be recovered.
  - Covers dynamic flight phases where recovery of primary flight control functions are not immediately achievable
    - Ascent (launch thru orbit insertion & solar array deploy)
    - De-orbit/Entry (through landing)
    - On orbit flight phases considered ‘dynamic’ (eg TEI 3 burn, RPOD backout)
  - Manual survival mode capabilities are provided to breathe, communicate, and control critical power loads without computer control (or network). Likewise, manual emergency entry capabilities are planned for manual roll control and pyro event initiation

Crew Escape, Abort and Emergency Systems

Requirement	JSC 28354 (1998)	Baseline NPR (2003)	REV A (2005)	REV B (2008)
Abort	The program shall be designed such that the cumulative probability of safe crew return over the life of the program exceeds 0.99. This shall be accomplished through the use of all available mechanisms including mission success, abort, safe haven, and crew escape. A crew escape system shall be provided on ETO vehicles for safe crew extraction and recovery from in-flight failures across the flight envelope from prelaunch to landing. The escape system shall have a probability of successful crew return of 0.99	The capability for crew and occupant survival and recovery shall be provided on ascent using a combination of abort and escape. The capability for crew and occupant survival and recovery shall be provided during all other phases of flight (including on-orbit, reentry, and landing) using a combination of abort and escape, unless comprehensive safety and reliability analyses indicate that abort and escape capability is not required to meet crew survival requirements.	The space system shall provide crew and passenger survival modes throughout the ascent and on-orbit profile (from hatch closure until atmosphere entry interface) in the following order of precedence: a. Abort. b. Escape by retaining the crew and passengers encapsulated in a portion of the vehicle that can reenter without crew or passenger fatality or permanent disability. c. Escape by removing the crew and passengers from the vehicle. The program shall ensure that ascent survival modes can be successfully accomplished during any ascent failure mode including, but not limited to, complete loss of thrust, complete loss of control, and catastrophic booster failure at any point during ascent. The space system shall provide crew and passenger survival modes throughout the descent profile (from entry interface through landing) in the following order of precedence : a. Design features that increase tolerance to loss of critical functions such that landing can still be accomplished. b. Escape. The program shall ensure that the descent survival modes can be successfully accomplished for loss of critical functions including, but not limited to, loss of active attitude control and loss of primary power	The space system shall provide abort capability from the launch pad until Earth-orbit insertion to protect for the following ascent failure scenarios (minimum list): a. Complete loss of ascent thrust/ propulsion (Requirement). b. Loss of attitude or flight path control (Requirement)

Abort

- **The pre-baseline version of NPR 8705.2 called for a probability of safe crew return using escape, abort, and safe haven capabilities.**
  - Difficult to quantify ascent abort environments.
  - Studies conducted during the OSP program indicated that 99% was probably not achievable.
- **Baseline version removed quantified part of the requirement.**
  - Still no preference on use of either abort or escape.
  - Total coverage unspecified.
- **Rev A dealt with establishing an order of precedence for crew survival options.**
  - Carefully defined abort as the return of the crew in the spacecraft normally used for reentry – acknowledging value of keeping crew in vehicle
  - Allowed for an escape mechanism in a partial portion of the spacecraft, or as a last resort, classical crew escape (ejection).
  - Specified total coverage on ascent abort as 100% (no black zones).

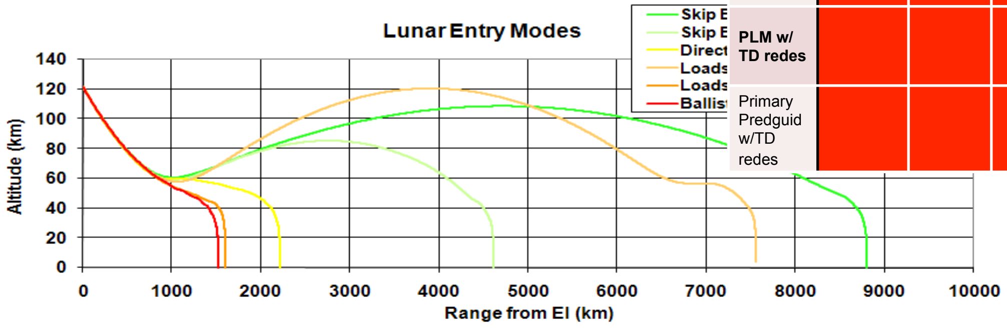
Abort

- **Rev A also led to the requirement that abort be accomplished without use of main propulsion and during loss of control scenarios.**
  - This requirement was driven by perceived shortfalls in previous implementation
    - The Space Shuttle had near 100% abort coverage, but required a minimum number of main engines to still be operation at various times during the trajectory.
    - Requires a solution that allows for the crew to be removed from the launch vehicle.
  - NPR users mistakenly believed that this was the ENTIRE requirement for monitoring for failures that could trigger an abort.
  - Other failures are just as likely, and need to be monitored, but Rev A Specifies that you must be able to accomplish an abort without the functions of propulsion and attitude control which are the end result of many failures.
- **Rev B removed all references to escape and prescriptive failures on entry**
  - All architectures studied and then implemented during Constellation used a capsule based solution that was separable from the launch vehicle – Escape wasn't meaningful
  - Entry success and failure tolerance down modes embedded in other requirements
    - Critical HW and SW failure, degraded modes, and redundancy requirement
    - Mission abort (declaring the mission over and returning with adequate redundancy for reentry).
    - Robust entry is still required.

Orion Implementation of Entry Abort Modes

GNC Mode	Method	Guidance	Control	Navigation	Drogue Accuray
PredGuid	Auto	Precision Landing	Auto 3-axis	PV, Att, Rate, Accel	3 nm
PredGuid	Manual	Precision Landing	Manual Bank - RHC Target Redesignate - Keyb	PV, Att, Rate, Accel	NA*
PLM	Auto	Precision Loads Managed	Auto 3-axis		
PLM	Manual	Precision Loads Managed	Manual Bank - RHC Target Redesignate - Keyb		
Ballistic	Auto	None	Auto 3-axis Constant Banl		
Ballistic	Manual	None	Adjustable Bank Rate - Ke		

Options	Common Cause Gyro failure	Common Cause Accel failure	ODN Failure	RCS Loss of Control Authority	Loss of Nav State	Deorbit over-burn	Deorbit under-burn	½ Prop Failure	Ascent Abort Support	Down-mode issues	Recovery time
Entry Survival Man Ballistic	🟩	🟩	🟩	🟨	🟩	🟨	🟥	🟩	🟨	🟩	🟨
Ballistic	🟥	🟩	🟥	🟨	🟩	🟨	🟥	🟩	🟨	🟩	🟨
Manual Bank	🟥	🟥	🟥	🟥	🟨	🟩	🟩	🟨	🟩	🟩	▨
PLM	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟨	🟥	🟩	▨
PLM w/ TD redes	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟨	🟥	🟩	🟩
Primary Predguid w/TD redes	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟩	🟩	🟩



Primary Entry Down Modes provide a graceful degradation of Entry performance as system failures occur

Manual Control and Human-in-the-Loop

Requirement	JSC 28354 (1998)	Baseline NPR (2003)	REV A (2005)	REV B (2008)
Manual Control	The flight crew shall be capable of taking manual control of the vehicle during all phases of flight. The vehicle shall exhibit Level I handling qualities as defined by the Cooper-Harper Rating Scale	On ascent, manual control of the vehicle flight path and attitude shall be provided where vehicle structural, thermal, and performance margins allow.	During all phases of flight, the system shall provide the capability for manual control of flight path and attitude, when the human can operate the system within the structural, thermal, and performance margins without causing crew or passenger fatality or permanent disability	The crewed space system shall provide the capability for the crew to manually control the flight path and attitude of their spacecraft, with the following exception: during the atmospheric portion of Earth ascent when structural and thermal margins have been determined to negate the benefits of manual control

Manual Control

- **Another hotly debated requirement for the ascent portion of the flight.**
- **All US launch vehicles developed for manned flight (Saturn I/V and the Space Shuttle allowed for the crew to manually steer the vehicle.**
  - Has never been used during flight.
  - Shuttle inhibited by flight rule from manual control during the first 90 seconds.
  - Limited utility especially during regions around max Q.
  - Requirement allows for limits based on vehicle structural and thermal margins.
- **NPR has remained relatively unchanged in this regard.**

Take Away – The Art of Human Rating

- Human rating is really just about system functionality required for the accommodation, utilization and protection of the human in the system in order to maximize mission success
- Requirement intent is directly traceable to and has remained intact from the beginning of human space flight programs
- These requirements define an intent which is not a single implementation for all designs or all missions
- The requirements can not be implemented without the acknowledgement of real programmatic constraints to success
- Pay more attention to the necessity of demonstrating the details of the design and how systems interact, particularly in failure scenarios, versus the exact verbiage of the requirement
- Do not underestimate the contribution of personal responsibility and accountability as an important enabler to establishing the best, most robust design within programs constraints