Safety & Mission Assurance Directorate -
Mission Assurance and Quality at NASA Goddard Spaceflight Center

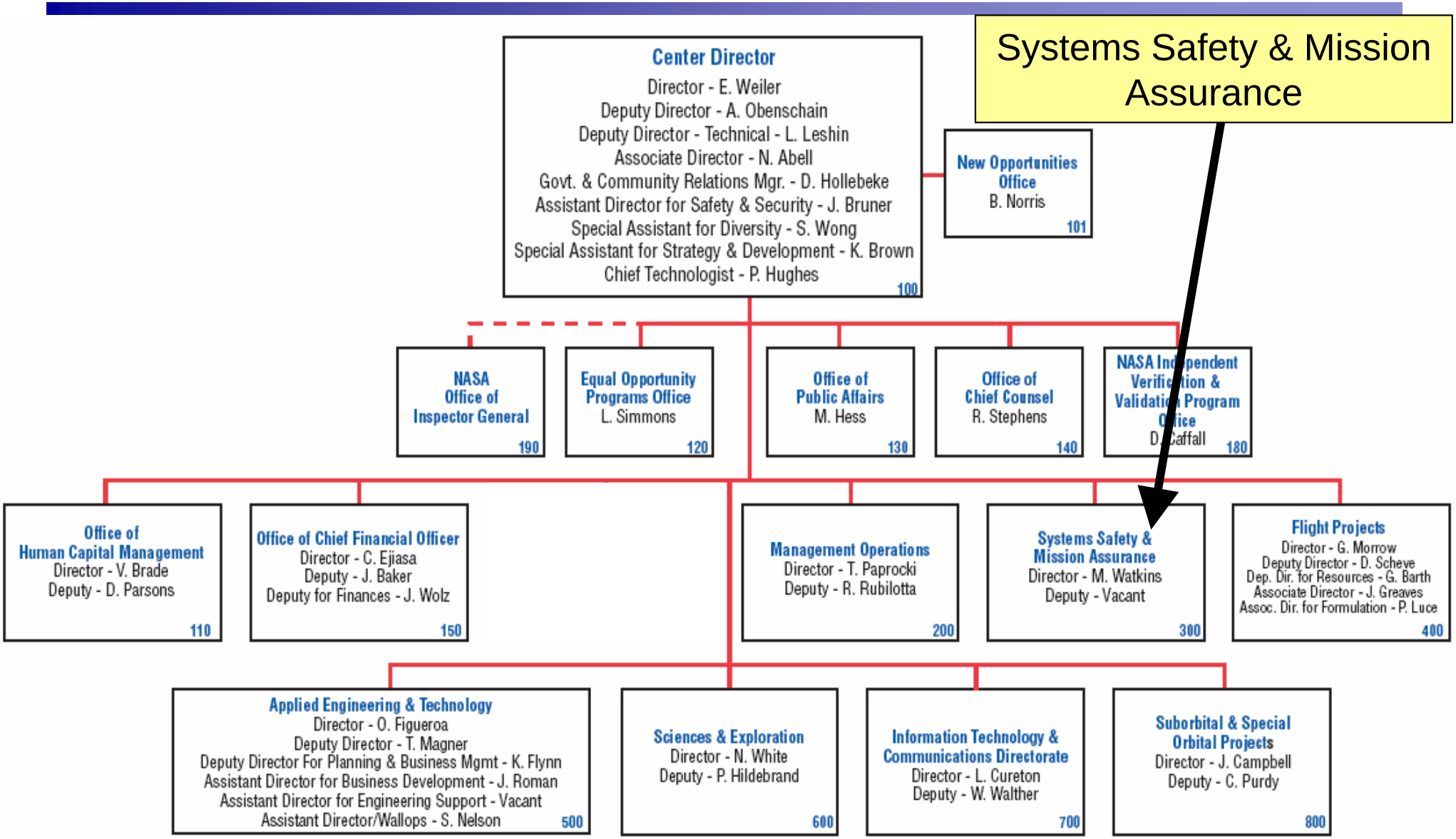
March 11, 2008

Presented by Mike Kelly, Institutional Support Office, Chief

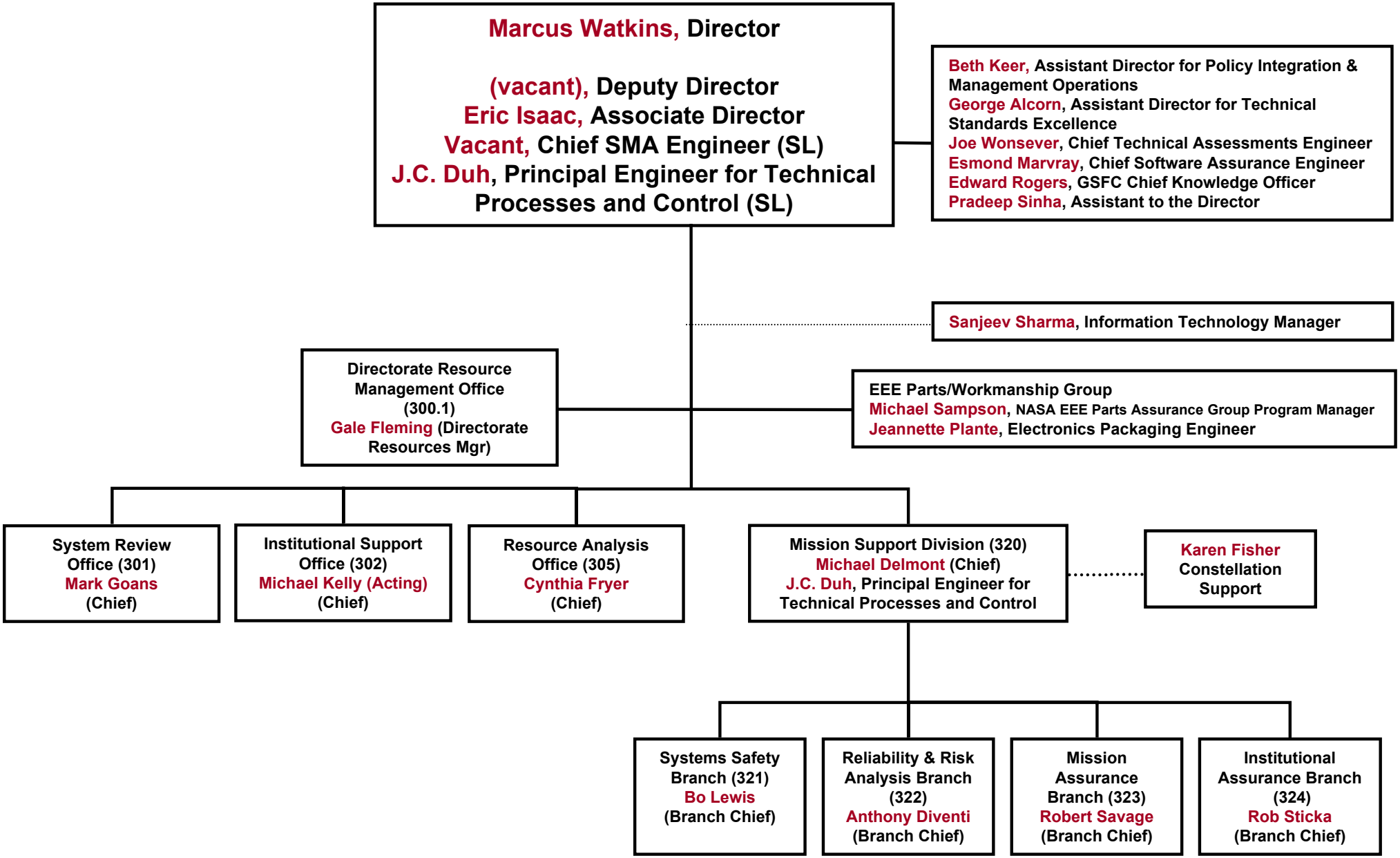
AGENDA

- Safety and Mission Assurance Directorate Organization Charts
- How Code 300 Organization Interacts with a GSFC Projects
- NASA/GSFC Mission Assurance Approach
- Chief Safety and Mission Assurance Officers (CSO, Code 320)
  - MAG and MAR
  - Control of Contractors and Subcontractors
  - Software Assurance
- Code 301, System Review Office
- Code 302, Institutional Support Office
  - Risk Management
  - Supply Chain Management
- Code 321, System Safety Branch – Safety Program
- Typical Safety Deliverables
- Code 322, Reliability and Risk Analysis Branch - Reliability Program
- Typical Reliability Deliverables
- Presenter's Lessons Learned

GSFC Organization Chart



Safety and Mission Assurance Directorate (Code 300) (DRAFT)

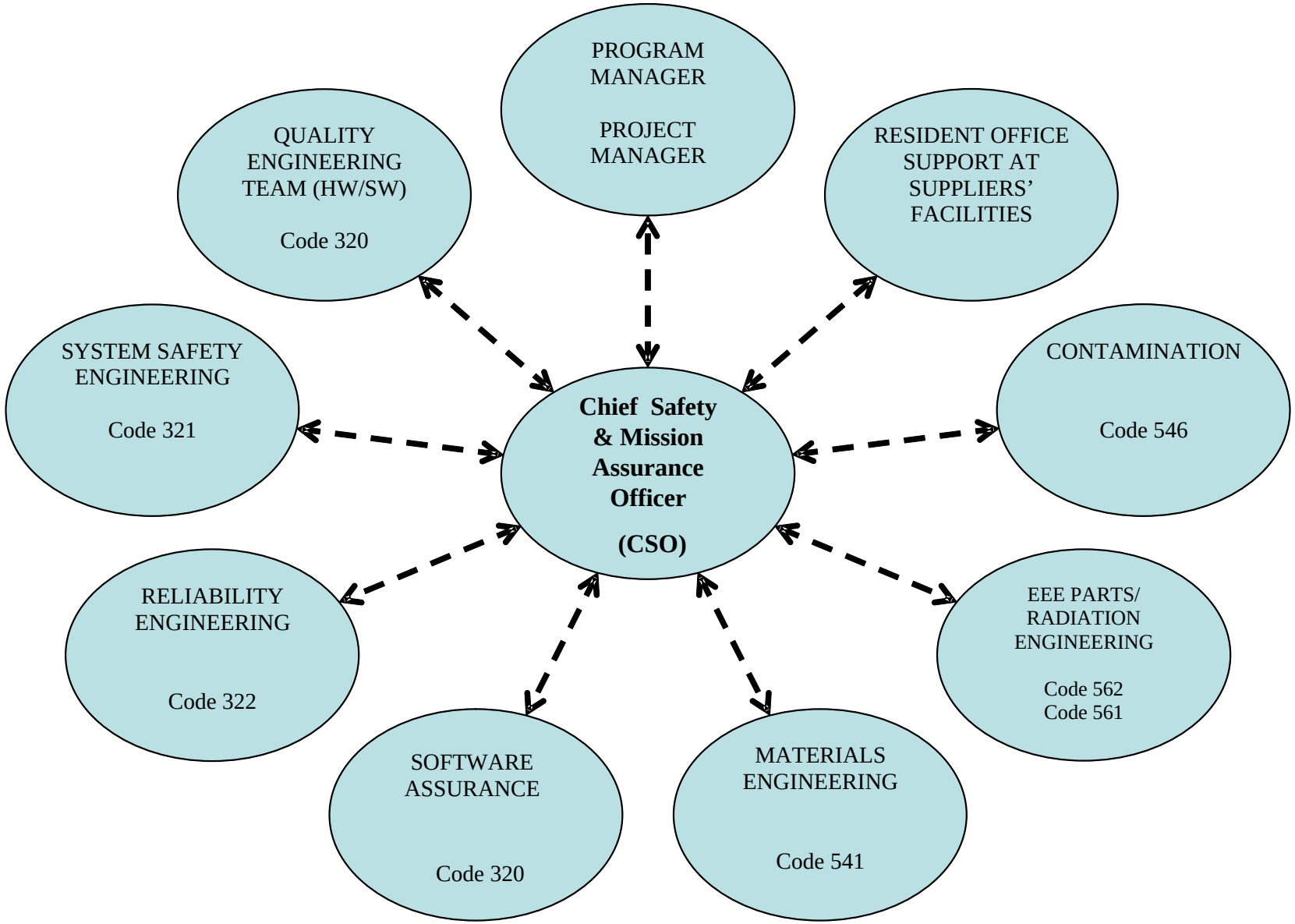


Actual Manpower Numbers for Safety & Mission Assurance Directorate

GSFC Code 300 manpower; 207 total distributed as follows:

- 107 Civil Servants
  - 87 permanent
  - 18 term
  - 2 co-op
- Approximately 100 contractors total from Mantech/SRS and Honeywell

How Code 300 Organization Interacts With GSFC Projects



NASA/GSFC Mission Assurance Approach

- NASA Chief Safety and Mission Assurance Officer (CSO) is the program/project focal point and is responsible for supporting the Goddard missions from an End-to-End Perspective which includes Procurement Activities through On-Orbit Operations.

- CSO coordinates a team of Code 300 Managers and Engineers (Safety, Reliability, Quality Assurance, S/W Assurance) and Code 500 Engineers (Parts, Materials) to implement NASA & GSFC safety & mission assurance requirements

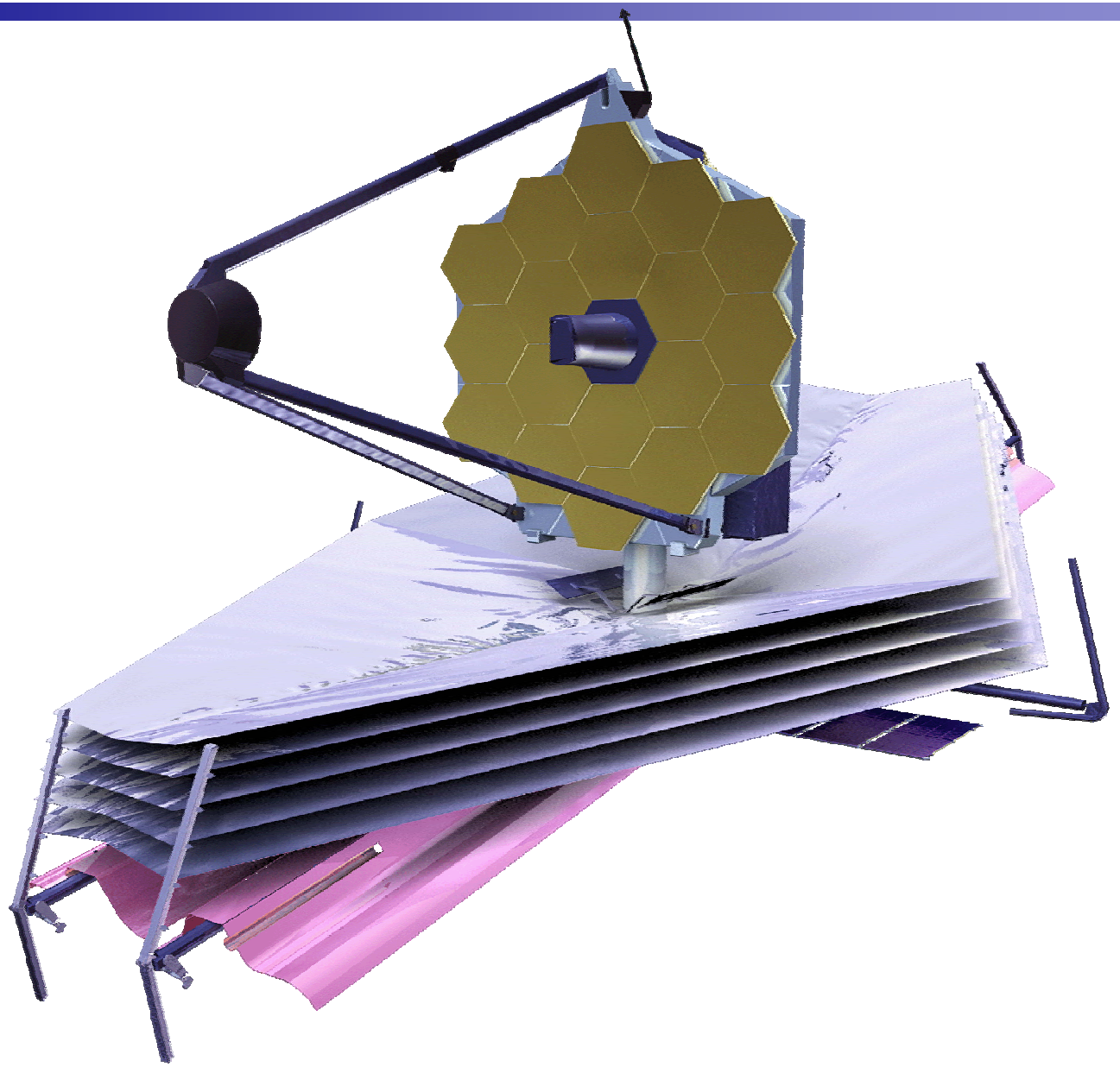
- CSO leads a team of QA and NACS/DCMA personnel based at GSFC and at supplier facilities.

(CONTINUED)

NASA/GSFC Mission Assurance Approach (continued)

- The Mission Assurance Organization at NASA (which includes the CSO and his QE staff) are totally independent of Program, Project, and Systems Engineering Offices.
  - This is a typical Mission Assurance Concept at NASA/GSFC and at most aerospace companies.
- CSO has an independent reporting chain to the GSFC Center Director.
- The Mission Assurance Team supports the Program and Project Offices in their daily operations. However, if there are conflicting opinions it is the CSO's responsibility to report those disagreements to NASA management.

Assurance Management



Chief Safety and Mission Assurance Officers (CSO, Code 320)

- Generally the CSO is co-located with the project office, to provide the most efficient access to the project manager and his staff. It is desirable to have safety and reliability personnel co-located there as well.

- CSO must be a good communicator and understand where support is needed and keep the Project in the loop.

- CSO walks a fine line between supporting the Project and remaining an independent entity.

(CONTINUED)

Chief Safety and Mission Assurance Officers (CSO, Code 320)

- **CSO duties in support of the Project are as follows:**
  - Voting member of CCB and risk management board
  - Conduct audits/assessments at hardware developers (and provide follow-up). Responsible for determining mandatory inspection points
  - Support in resolution of hardware/software problems
  - Member of Source Evaluation Boards
  - Member of Senior Staff
  - Interface for all Printed Wiring Board (PWB) coupons
  - Point of contact for all manpower in Code 300
  - Ensure LOD and LOA (task order) are written and followed to support the project. All task orders are in the Task Order Management System (TOMS).
  - Attendance and participation at all major reviews
  - Provide monthly presentations to Code 300 Management
  - Provide presentations to Project/Program Management as required
  - Development of Mission Assurance Requirements
  - Present Safety and Mission Assurance System Review to Headquarters

MAG and MAR

Mission Assurance Requirements (MAR) Preparation and Development

- The CSO uses as a guide the Mission Assurance Guidelines (MAG) Procedure (300-PG-7120.2.2) and consultation with functional disciplines in Codes 301, 302, 320 and other GSFC organizations to develop the MAR for the Instrument, Spacecraft, and Ground System
  - The purpose of the MAG is to serve as a resource to the CSO and Project Manager in supporting the development of a realistic set of mission assurance requirements tailored to specific needs of an individual project. CSO, with Project support, will select, tailor and then place the appropriate mission assurance requirements either directly into the contract SOW, and/or within a stand-alone contractual document entitled a Mission Assurance Requirements (MAR) document.
  - CSO discusses draft MAR requirements with the Project and vendors and then tries to finalize.
  - The CSO prepares a Summary Report that includes the concurrence of the team member for each section and any deviations from the standard MAG guidelines with a detailed explanation of each deviation.
    - This Summary Report and MAG vs. MAR comparison is discussed at the Code 300 Roundtable with management.
  - The Director of Code 300 and Project Manager approves all MARs.

Control of Contractors and Subcontractors

- The work activities performed by the developer and/or his suppliers are subject to evaluation and audit by government-designated representatives.
- There is a database of assessment reports performed by NASA for many suppliers. It is a good resource for information for GSFC engineers.
- The on-site supplier representative's may be a DCMA person via a letter of delegation, or an independent assurance contractor (IAC) via a contract such as the NASA Assurance Supplier Contract (NASC) or the Code 300 Mission Assurance Support Contract (MASC).
- DCMA and NASC/SAC are funded by NASA HQ, not by the GSFC Program/Project budget.
- MASC contract persons provide support at contractor facilities via the MASC contract.

- Advantage - Usually works exclusively on your project
- Disadvantage - Costs are directly to the GSFC Program/Project budget

(CONTINUED)

Control of Contractors and Subcontractors (con't)

- The SAM also ensures that the supplier has an acceptable system for controlling non-conforming product, reporting failures and flowing down requirements to suppliers.
- The SAM (and program management professionals) may use the NASA Supplier Assessment System. The SAS mission is to provide a consolidated and comprehensive on-line repository of supplier quality data, performance indicators, metrics, and assessment tools.
  - The database and system are located at http://sas.nasa.gov
- The SAM coordinates review and disposition of Government and Industry Data Exchange Program (GIDEP) Alerts and ensures that the supplier participates in the program.
- SAM coordinates review of supplier's workmanship standards for conformance to the NASA standards.
  (The current status and/or any application notes for these standards can be obtained at the following URL: http://workmanship.nasa.gov)
  - Soldering (NASA-STD-8739.3)
  - Conformal Coating (NASA-STD-8739.1)
  - Cable, Crimp, Harness (NASA-STD-8739.4)
  - ESD Protection (ANSI/ESD S20.20)

Software Assurance

Our primary objective is to assess program / project products and processes to assure that programmatic capabilities are achieved.

Software Assurance shall apply to flight and ground system software developed by or for GSFC.

- Government off-the-shelf (GOTS) software
- Modified off-the-shelf (MOTS) software
- Commercial off-the-shelf (COTS) software

Overview

Software assurance comprises a set of disciplines that strive to improve the overall quality of the product/software while employing risk mitigation techniques.

Software Quality Software Safety Software Reliability
Verification and Verification (V&V)
Independent Verification and Validation (IV&V).

SW Quality Assurance Functions:

- assures that the standards, processes, and procedures are appropriate for the project and correctly implemented,
- assures adherence to those software requirements, plans, procedures and standards,
- shall plan and conduct process and product assurance activities throughout the project development life cycle.

Goddard Review Process
System Review Office, Code 301

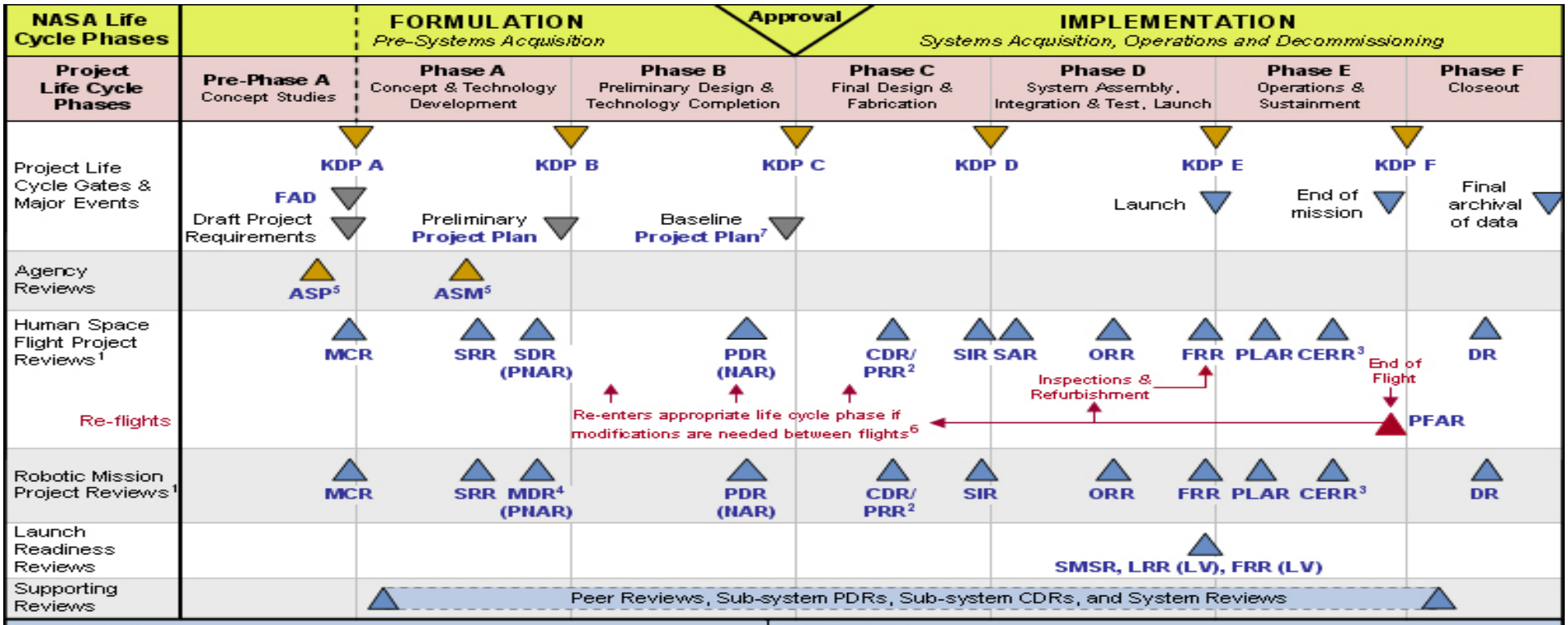
Mark Goans

Chief

Independent Review Process

- The Systems Review Office (SRO) is the implementation arm of the GSFC independent review process.
- Types of Independent Reviews
  - Mission Life-Cycle Reviews conducted Standing Review Board (SRB)
    - Reference: NPR 7120.5D NASA Space Flight Program and Project Management Requirements
  - Center Level Independent Reviews conducted by a SRO chartered Review Team
    - Reference: GPR 8700.4F Integrated Independent Reviews
  - Engineering Peer Reviews conducted by an independent peer review team
    - Reference: GPR 8700.6A Engineering Peer Reviews

Project Life-Cycle and Reviews



FOOTNOTES

1. Flexibility is allowed in the timing, number and content of reviews as long as the equivalent information is provided at each KDP and the approach is fully documented in the Project Plan. These reviews are conducted by the project for the independent SRB. See Section 2.5 and Table 2-6.
2. PRR needed for multiple (≥4) system copies. Timing is notional.
3. CERRs are established at the discretion of Program Offices.
4. For robotic missions the SRR and the MDR may be combined.
5. The ASP and ASM are Agency reviews, not life-cycle review.
6. Includes recertification, as required.
7. Project Plans are baselined at KDP C and are reviewed and updated as required, to ensure project content, cost, and budget remain consistent.

ACRONYMS

ASP	Acquisition Strategy Planning Meeting
ASM	Acquisition Strategy Meeting
CDR	Critical Design Review
CERR	Critical Events Readiness Review
DR	Decommissioning Review
FAD	Formulation Authorization Document
FRR	Flight Readiness Review
KDP	Key Decision Point
LRR	Launch Readiness Review
LV	Launch Vehicle
MCR	Mission Concept Review
MDR	Mission Definition Review
NAR	Non-Advocate Review
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PFAR	Post Flight Assessment Review
PLAR	Post Launch Assessment Review
PNAR	Preliminary Non-Advocate Review
PRR	Production Readiness Review
SAR	System Acceptance Review
SDR	System Definition Review
SIR	System Integration Review
SMSR	Safety and Mission Success Review
SRR	System Requirements Review

Mission Life-Cycle Reviews

- The agency convenes a Standing Review Board (SRB) to conduct Mission Life-Cycle Reviews
- The SRB comprises a chairperson, review manager and independent board members chosen based on their management, technical, safety or mission assurance expertise.
- Mission Life-Cycle reviews are conducted using approved agency and center review processes
- Requirements for each review are defined in a Terms of Reference (ToR) Document
- The SRO assigns a Systems Review Manager (SRM) to serve as a member of the SRB
- The SRM assists in development of the ToR, recommends additional GSFC SRB members, assists in the conduct of the review to ensure GSFC processes are followed, assists in writing the review report and presentation of review team findings to the Goddard Center Management Council

Center Level Independent Reviews (1 of 2)

- Center Level Independent Reviews comprise life cycle reviews for the Spacecraft(s), Instrument(s), Ground System(s) and Operations.
  - For larger projects dozens of reviews may be conducted
- The SRO convenes review teams to conduct Center Level Independent Reviews
- For each project, the SRO assigns a SRM to serve as the review team chair.
- The SRM develops a Systems Review Plan in conjunction with the Project that appropriately tailors the GSFC process to the mission needs.
- For each element the SRM establishes an appropriate independent review team with members chosen for their management and technical expertise
- The SRM presides at each review and ensures compliance with center-level processes.

Center Level Independent Reviews (2 of 2)

- The review team evaluates the project based on compliance with the review objectives and adherence to Key Project Management Practices
  - Formal Requests for Action or additional information are generated as needed
  - The review team caucuses and out briefs the project at the conclusion of the review
- The SRM provides a report to the Project documenting the review results and makes appropriate recommendations to the GSFC Center Management Council
- The SRM provides feedback the to mission SRB regarding key results from Center Level Reviews

Engineering Peer Reviews

- Each GSFC flight project is required to develop an Engineering Peer Review Plan
- Engineering Peer Reviews (EPRs) are conducted for spacecraft subsystem, instrument component, software and crosscutting functional elements.
- The project manager (PM) appoints an independent EPR chairperson for the various elements.
- For each element, the EPR chairperson recruits independent review team members based on their technical knowledge and practical experience.
- For each review the EPR chairperson provides a report with findings to the PM and the assigned SRM
- Engineering Peer Review Results are summarized at the next schedule Center Level Independent Review and/or Mission Life-cycle Review

Institutional Support Office, Code 302

Mike Kelly

Chief

GSFC Risk Management
GSFC Supply Chain Management

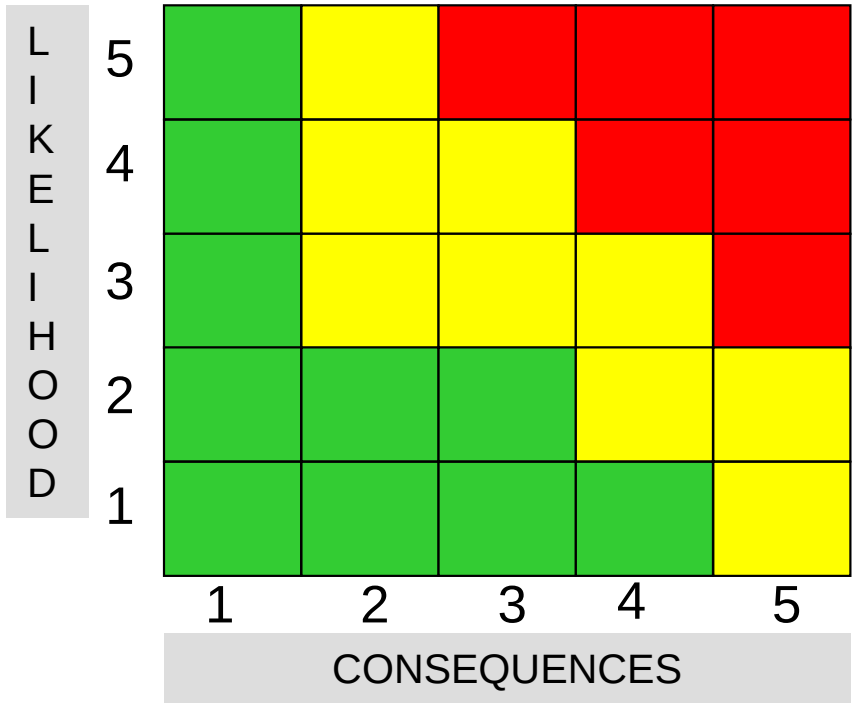
CRM Process

- **Continuous Risk Management** is a structured management practice with processes, methods, and tools for managing project risks

- CRM provides a disciplined environment for proactive decision making:
  - ***Identify*: Continuously search for risks**
  - ***Analyze*: Evaluate impact, probability, timeframe; prioritize**
  - ***Plan*: Implement strategies; accept, watch, or mitigate risks**
  - ***Track*: Monitor watched and mitigated risks**
  - ***Control*: Correct for deviations from mitigation plan**
  - ***Communicate and Document*: Provide feedback (both internal and external)**

See http://CRM.nasa.gov

Standard 5x5 Risk Matrix



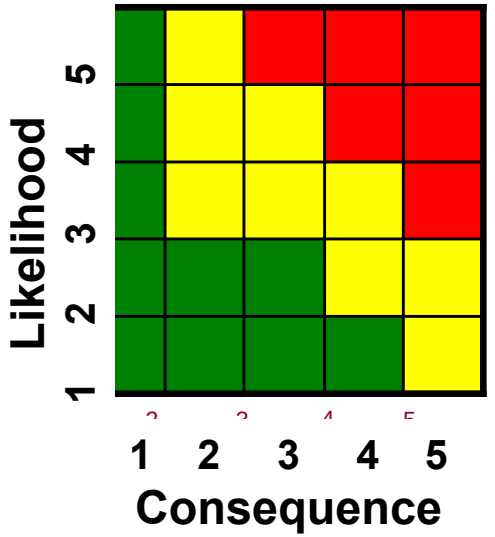
High

Med

Low

GSFC Risk Matrix Standard Scale

Likelihood	Safety (Estimated likelihood of safety event occurrence)	Technical (Estimated likelihood of not meeting performance requirements)	Cost/Schedule (Estimated likelihood of not meeting cost or schedule commitment)
5 Very High	($P_{SE} > 10^{-1}$)	($P_T > 50\%$)	($P_{CS} > 75\%$)
4 High	($10^{-2} < P_{SE} \leq 10^{-1}$)	($25\% < P_T \leq 50\%$)	($50\% < P_{CS} \leq 75\%$)
3 Moderate	($10^{-3} < P_{SE} \leq 10^{-2}$)	($15\% < P_T \leq 25\%$)	($25\% < P_{CS} \leq 50\%$)
2 Low	($10^{-6} < P_{SE} \leq 10^{-3}$)	($2\% < P_T \leq 15\%$)	($10\% < P_{CS} \leq 25\%$)
1 Very Low	($P_{SE} \leq 10^{-6}$)	($0.1\% < P_T \leq 2\%$)	($P_{CS} \leq 10\%$)



Consequence Categories					
Risk	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Safety	Negligible or No impact.	Could cause the need for only minor first aid treatment .	May cause minor injury or occupational illness or minor property damage.	May cause severe injury or occupational illness or major property damage.	May cause death or permanently disabling injury or destruction of property.
Technical	No impact to full mission success criteria	Minor impact to full mission success criteria	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin	Major impact to full mission success criteria. Minimum mission success criteria is achievable	Minimum mission success criteria is not achievable
Schedule	Negligible or no schedule impact	Minor impact to schedule milestones; accommodates within reserves; no impact to critical path	Impact to schedule milestones; accommodates within reserves; moderate impact to critical path	Major impact to schedule milestones; major impact to critical path	Cannot meet schedule and program milestones
Cost	<2% increase over allocated and negligible impact on reserve	Between 2% and 5% increase over allocated and can handle with reserve	Between 5% and 7% increase over allocated and can not handle with reserve	Between 7% and 10% increase over allocated, and/or exceeds proper reserves	>10% increase over allocated, and/or can't handle with reserves

HIGH RISK

MODERATE RISK

LOW RISK

Code 300
Rev. 021307

Supply Chain Management Overview

- Organization Charter
- Organization Functions
- Assessment Approach/Process
- Assessment Objectives
- Assessment Reporting
- Sample Assessment Plan “items to be reviewed”
- Sample assessment “One-Pager”
- AS9100 Class at GSFC
- Supplier Conference at GSFC
- Impact on Mission Success

Organization Charter

- The Supply Chain Manager is a key member of the Goddard Management System team and provides integrated technical leadership, across the entire portfolio of Goddard managed projects, for safety and mission assurance issues related to mission contractors and suppliers.

- The Supply Chain Manager works with all of the Chief Safety and Mission Assurance Officers (CSOs) to develop and manage a comprehensive process to track contractor-related safety and mission assurance issues across all Goddard projects, identify and analyze trends, and develop corrective action plans to improve the quality of procured systems, spacecraft, instruments, components, parts and materials. He provides an integrated approach to defining and managing all of our supplier audit activities.

Organization Functions

- Conducts Supplier assessments
- Maintains Records of assessments in GSFC audit database
- Sponsors Quality training (e.g. AS9100 quality system, ISO Lead Auditor)
- Sponsors suppliers conferences
- Is Technical Liaison for NASA Contractor Assurance Services (NCAS)
- Is Focal Point for Defense Command Management Agency (DCMA)
- Working with NASA Assurance Management Team (NAMT)
- Working with Joint Audit Planning Committee (JAPC)

The Assessment Approach/Process

NASA Goddard Supply Chain Manager has a large role in the planning of the assessment in order to work issues/concerns upfront

- He is calling supplier's to set up the assessments (not NCAS)
- He is conducting the in-brief when possible to set the proper tone for both the assessment team and the supplier
- He is attending each out-brief (sometimes remotely)

Draft copy of the Supplier's Assessment Plan is forwarded to the Supplier for their comments and feedback to ensure agreements are reached prior to the assessment

No scoring is used during the assessment process

- Only non-compliances, observations, & commendations and
- A final out-brief package is left with the supplier at the end of the assessment

(CONTINUED)

The Assessment Approach/Process

- A final report is written and forwarded to the supplier Point of Contact for comment
  - This report will be a few pages long and will contain the assessment cards and the final out-brief package
- NASA/GSFC provides a “Supplier Assessment Team Evaluation Survey Form” to solicit both positive and negative comments about the assessment process and the participation of each assessor
- NASA/GSFC does care about the Corrective Actions and wants to work with each supplier to support Closure of each one.
  - Plan to conduct follow-up assessments if necessary and/or if requested by the supplier

(CONTINUED)

The Assessment Approach/Process

CONCLUSION

- NASA/GSFC cares about all space suppliers.

- Let Louis Thomas (LT) (louis.a.thomas@nasa.gov) or Mike Kelly (Michael.P.Kelly@nasa.gov) know if they can help. Their contact information is as follows:

  LT (301) 286-4320 WORK or (301)-789-8590 CELL

  MK(301) 286-0662 WORK or (301) 980-4384 CELL

Assessment Objectives

- Assess the supplier's processes for compliance to:
  - the requirements of ISO9001:2000 or AS9100, (if supplier is third party certified, we will assess the supplier to it.)
  - to the applicable NASA Contractual Requirements, and
  - to the requirements of the internal Quality Management System.
  - Follow up on previous NASA assessments
- The goal of each assessment is to identify strengths and areas for improvement.

Assessment Reporting

- Assessment Team Members will document closed and outstanding non-compliances & observations during the course of the assessment as well as note any observed commendations

Critical Noncompliance:	Failure to follow requirements that could lead to loss of life, serious injury to personnel, or damage to high-value equipment.
Noncompliance:	Failure to comply with Federal, State, local, Agency, or Center requirements that would not have the impact of a Critical Noncompliance
Observation:	A condition that is not contrary to documented requirements, but, in the judgment of the assessor warrants improvement or clarification.
Commendation:	A process that is considered an industry benchmark by the assessor.

- Daily debrief will entail informal discussions of the day's activities.
- Draft copies of Corrective Action Reviews will be provided at the Out-briefing.
- A formal report will be provided within 20 working days after the assessment.

Sample Assessment Plan "items to be reviewed"

The following list provides an outline of some of the topics the assessment team will review:

- **Flowdown of contractual requirements**
- **Receiving inspection**
- **Configuration Management / Change Control**
- **Packaging**
- **Handling**
- **Parts sampling, selection, and traceability**
- **Training and Certification of operators/inspectors/disposition authorities/testers**
- **Process documentation adequacy (work orders, shop aids, drawings, etc.)**
- **Document control**
- **Workmanship and inspection**
- **Travelers, routers and configuration recording**
- **Nonconforming product control**
- **Scrap control**
- **Rework and repair processes**
- **Acceptance Data Packages**
- **Problem Reporting System**
- **Internal Audit**
- **Calibration**
- **GFE**

Management One-Pager

The following chart is a sample assessment "One-Pager" that is presented to Code 300 management after each assessment.

Goddard Contractor Excellence Award (GCEA)
George M. Low (GML) Award Overview

GCEA:

- Awarded annually since 1988 to current GSFC prime contractors, subcontractors, and suppliers who have met the eligibility requirements.
- They are companies that contribute significantly to the mission of the GSFC, regardless of the product or service provided, and that have achieved measurable results over a three-year period are encouraged to apply.

GML Award:

- NASA's premier quality and performance award for NASA's prime and sub contractors.
- Recognizes large and small businesses that demonstrate excellence and outstanding technical and managerial achievements in quality and performance on NASA-related contracts or subcontracts.

AS9100 Class at GSFC

- Civil servants and contractors are invited to attend a class presenting the requirements of Aerospace Standard AS9100 and ISO 9001/2000.
- The class is sponsored by Mike Kelly, Supply Chain Manager for the Office of Safety and Mission Assurance.
- Presented by DCMA Headquarters Representatives, Gil Kimbrough and James Rodden
- The course is an in-depth overview of requirements, organization, structure, and use of the Quality Management Standard (agenda is available per request). Contact (301) 286-4320 L**ouis.A.Thomas@nasa.gov** **or** (301) 286-0662 Michael.P.Kelly@nasa.gov
- The objective is to give the student a working knowledge and auditing skills of the International Organization for Standardization (ISO) Quality Management Standard (QMS) for the year 2000 and AS9100 Aerospace requirements.
- The room can accommodate 25 to 30 persons and spaces will be reserved on a first-come, first-served basis.
- Where: Goddard Spaceflight Center or vicinity.
- When: As scheduled. Typically Tuesday through Thursday. Class starts at 8am.

Suppliers Conference at GSFC

- **OSSMA Supply Chain Management hosted a Suppliers Conference at GSFC Nov 2007).**
  - **Partial list of subjects:**
    - "We're in this together, how to make the most of an assessment by NASA"
    - "Role of NCAS Assessment"
    - "Counterfeit Parts"
    - "Proper Storage of Integrated Circuits"
    - "Quality Leading Indicator (QLI) eTool and findings to date"
    - "NASA Gold Rules"
    - "50 Years of Mission Operations and Lessons Learned"
  - **Approximately 120 people representing 50 different aerospace suppliers attended the conference.**

- **A second conference is tentatively planned for October 28 & 29, 2008. On the morning of October 30, there will be a tour of Goddard buildings 7, 10, 15, 29 complex (the spacecraft I&T area).**
  - *If there are any suppliers who want to help support the conference, please contact us.*

Impact on Mission Success

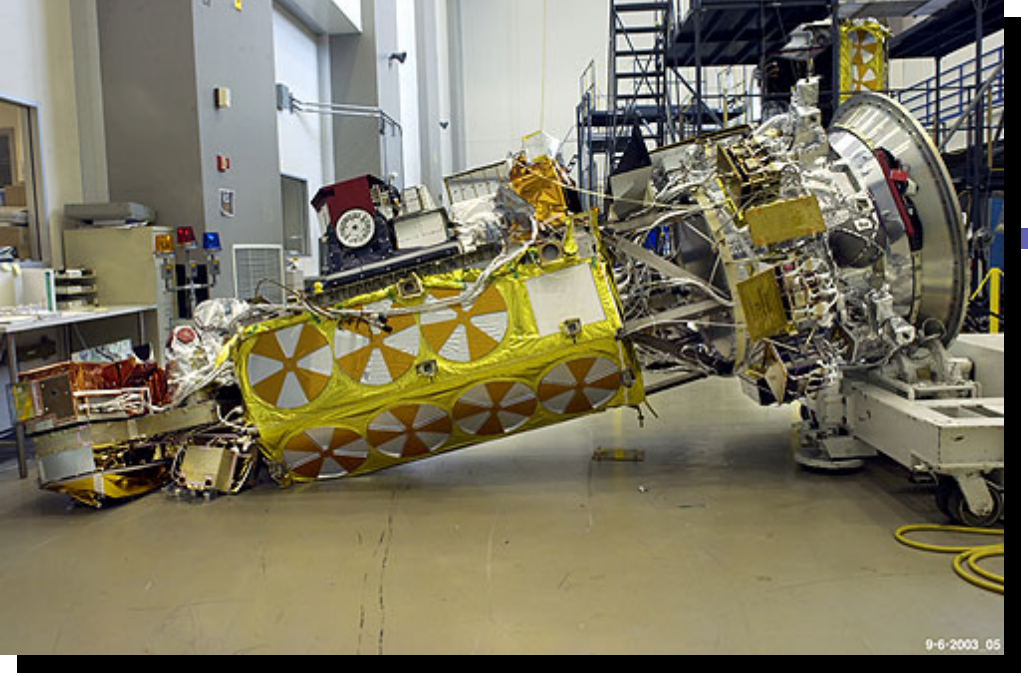
The Office Of Supply Chain Management:

- Mitigates risk through continuous assessment of project implementation by early identification of suppliers' flaws.
- Strives to provide Center management, CSOs, and PMs with focused, actionable information detailing identified non-conformances and risks to contractual requirements and also follows up with the suppliers on their mitigation strategies.
- Positively impacts the suppliers' community Quality Management System through assessments and site visits.
- NASA assessments provide leverage to Supplier's Mission Assurance and Safety Organizations to impact and make positive changes within their organizations.

System Safety Branch, Code 321

Bo Lewis

Chief

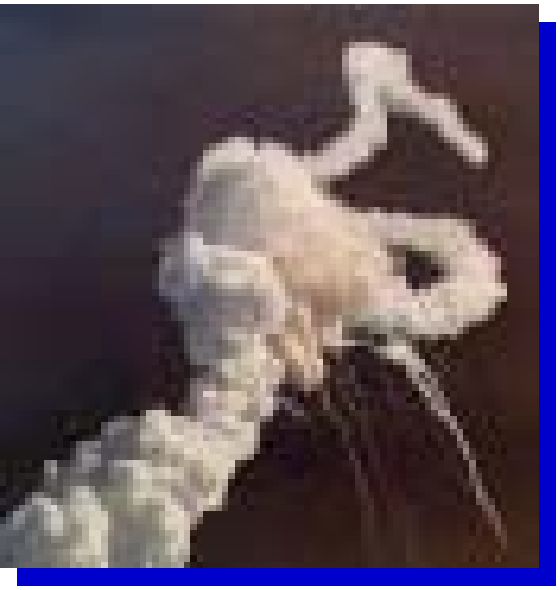


NOAA N Prime

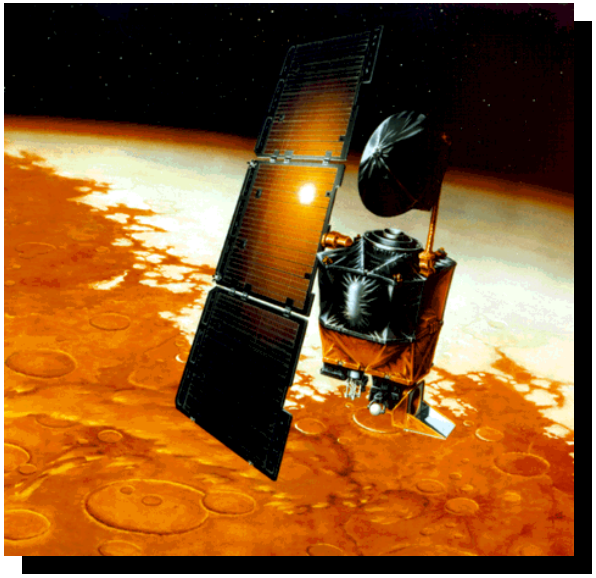
Helios

System Safety

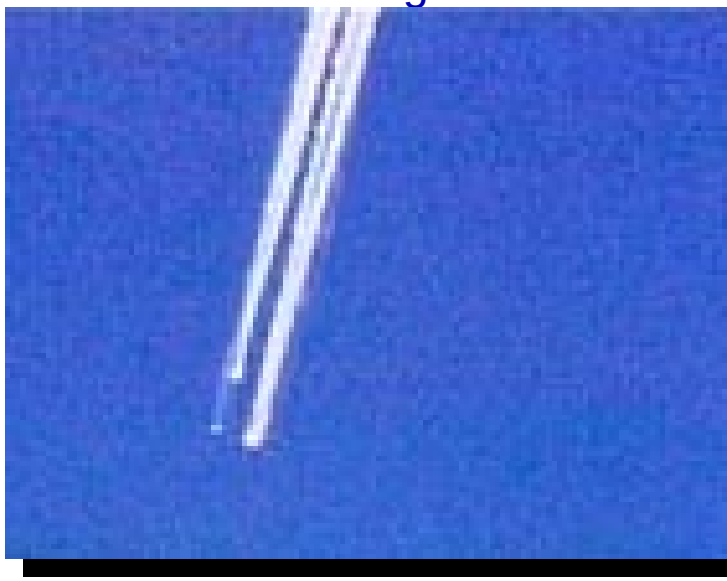
Columbia



Mars Climate Orbiter

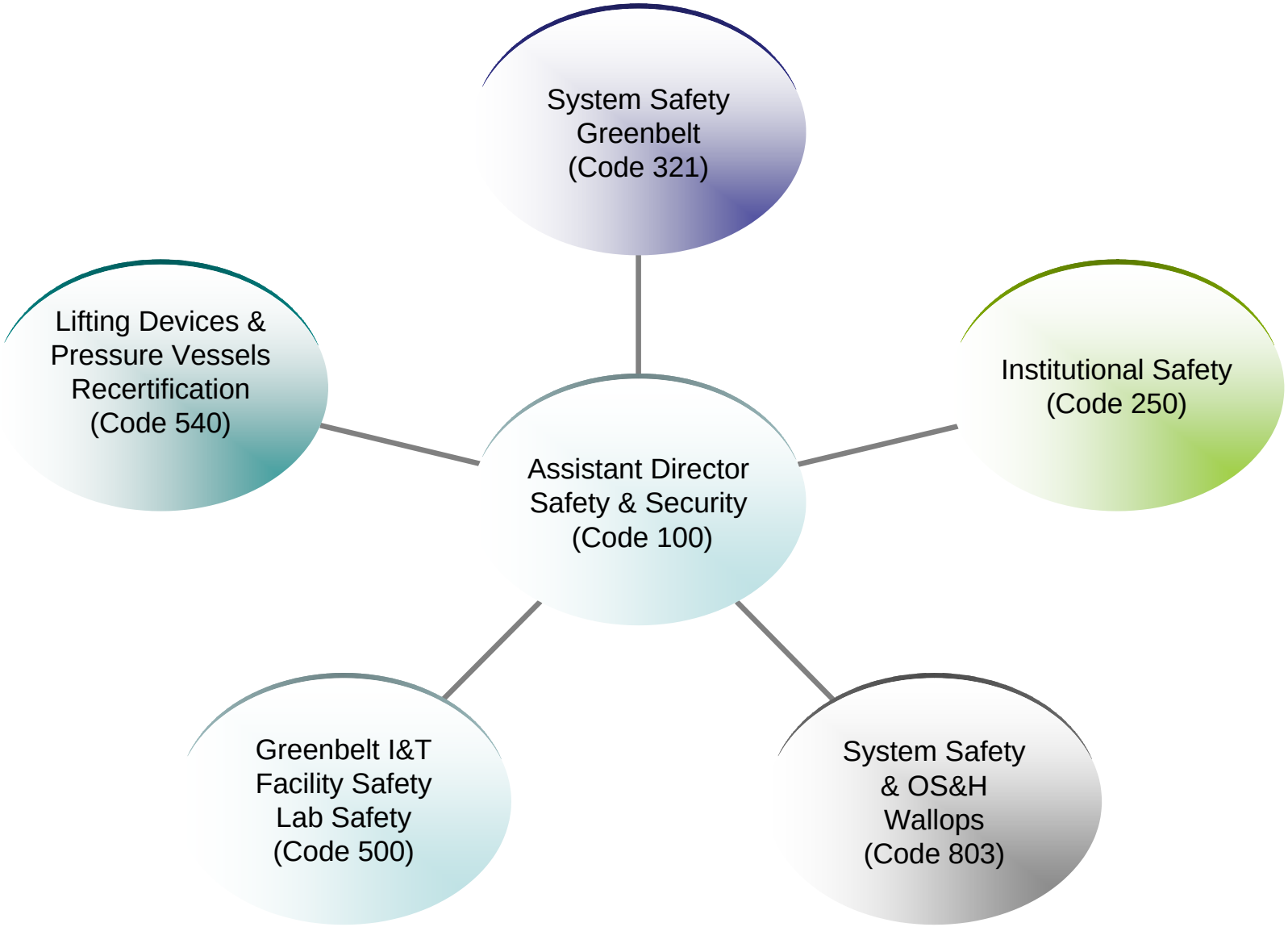


Challenger



GSFC Safety Organizations

(as documented in new GPR 8710.5 “GSFC Safety Program Management”)



Safety Roles at GSFC

- Assistant Director for Safety and Security (Code 100)
  - Overall integration of GSFC safety program
- Institutional Safety (Code 250)
  - Occupational Safety & Health
  - Environmental Management
- Safety in I&T Complex (B7, 10, 15, & 29) (Code 500)
  - Recertification Program
    - Lifting devices and equipment (LDE), and ground-based pressure vessels and pressurized systems (PV/S) at Greenbelt and Wallops.
    - Certification and recertification of LDE Operators and Critical Lift Coordinators is also included.
  - Lab Safety
  - Facility Safety
- Safety at Wallops (Code 803)
  - Occupational Safety & Health
  - Project Safety for Wallops payloads and sounding rockets
- **System Safety at Greenbelt (Code 321)**
  - **Organized, disciplined approach to early identification and resolution of system hazards impacting personnel, hardware, software, operations, GSE, and facilities.**
  - **Support all GSFC Greenbelt managed programs & projects**
  - **ELV, Shuttle, ISS, etc**

Code 321, Systems Safety Branch
System Safety Program

- The system safety program begins in the concept phase of design and continues up through launch.
- The system safety program will incorporate safety considerations into planning and operations and will provide for early identification and control of hazards during concept, design, development, fabrication, test, and transportation and ground activities.
- System Safety Requirements are levied by GSFC, the launch range, and the launch vehicle provider, and these requirements are mandatory for all space flight hardware developers. The Project Safety Manager in Code 321 provides assistance to the Flight Projects in interpreting and meeting those requirements.
- Specifically GSFC ELV Missions must meet the following requirements
  - AFSPCMAN 91-710, “Range Safety User Requirements”.
  - KNPR 8715.3, “Kennedy Space Center Safety Practices Procedural Requirements.”
  - NPR 8715.3, “NASA Safety Manual”

(CONTINUED)

Code 321, Systems Safety Branch
System Safety Program (continued)

- In-house GSFC missions must also meet facility-specific Safety Requirements, as applicable.
- Specific GSFC, Mechanical Systems Division Safety Manual
- 540-PG-8715.1.1 “Mechanical Systems Safety Manual Volume I and II”

GSFC System Safety Effort Throughout Project Lifecycle

- Proposal Support
- Requirements Definition
- Design Assessment
- Identification of Hazards
- Recommended Hazard Controls
- Assessment of Risk
- Verification of Hazard Controls
- Development of Safety Data Packages
- Interface with KSC & Range Safety
- Safety Support during I&T Activities
- Track Closure of Verification Items
- Safety Certification
- Prelaunch Safety Support

Typical Safety Deliverables (1 of 3)

SAFETY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Operations Hazard Analysis (OHA)	OHA addresses the implementation of safety requirements for personnel, all procedures, and equipment used during, testing, transportation, storage, and integration operations.	45 days prior to PER
Ground Operations Procedures	GOP documents all ground operations procedures to be used at GSFC facilities, other integration facilities, or the launch site for submittal to GSFC OSSMA for review and approval. Includes launch site ground operations procedures to be submitted to applicable Range Safety prior to use.	– Launch Range Procedures - Provide 45 days after PSR and submit to applicable Range Safety 45 days prior to first use. – GSFC Procedures - 7 days prior to first operational use.
Missile System Pre-Launch Safety Package (MSPSP)	Provides a detailed description of the payload design sufficient to support hazard analysis results, hazard analysis method, and other applicable safety related information. The developer shall take measures to control and/or minimize each significant identified hazard.	– Preliminary MSPSP, Mission PDR + 30 days – Intermediate MSPSP, Mission CDR – 30 days
Verification Tracking Log (VTL)	The VTL provides documentation that demonstrates the process of verifying the control of all hazards by test, analysis, inspection, similarity to previously qualified hardware, or any combination of these activities.	with final MSPSP, with regular updates until all hazards control verifications have been closed

Typical Safety Deliverables (2 of 3)

SAFETY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Preliminary Hazard Analysis (PHA)	***PHA identifies safety provisions and alternatives needed to eliminate instrument design or function hazards or reduce their associated risk.***	***– instruments or subsystems with the SAR at PDR + 30 days – spacecraft with the MSPSP at PDR + 30 days (S/C or Mission).***
Operating and Support Hazard Analysis (O&SHA)	***The O&SHA evaluates procedurally controlled activities for hazards or risks introduced into the system during pre-launch processing and to evaluate adequacy of procedures used to control identified hazards or risks.***	***with final MSPSP***
Safety Assessment Report (SAR)	***SAR shall identify all safety features of the hardware, software, and system design, as well as operational related hazards present in the system.***	***– Deliver the Preliminary SAR, PDR + 30 days (instrument / subsystem) – Deliver the Intermediate SAR, CDR - 30 days (instrument / subsystem). – Deliver the Final SAR, PSR - 30 days (instrument / subsystem)***
Safety requirements compliance checklist	***The checklist indicates for each requirement if the proposed design is compliant, non-compliant but meets intent, non-compliant (waiver required) or non-applicable.***	***– instrument/subsystems with the SAR at PDR + 30 days – spacecraft with the Missile System Pre-Launch Safety Package (MSPSP) at PDR + 30 days (S/C or Mission)***

Typical Safety Deliverables (3 of 3)

SAFETY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Safety Variances	***When a specific safety requirement cannot be met, the developer shall submit an associated safety variance, per NPR 8715.3; to GSFC OSSMA that identifies the hazard and shows the rationale for approval.***	***Deliver to GSFC OSSMA as early as known.***
Orbital Debris Assessment (ODA)	***ODA identifies any stored energy sources in instruments (pressure vessel, dewar, etc.) as well as any energy sources that can be passivated at end of life.***	***- PDR*** ***- CDR***

Reliability & Risk Analysis Branch, Code 322

Tony Diventi

Chief

Code 322, Reliability and Risk Analysis Reliability Program

- The Reliability section of Code 322 performs a wide range of reliability engineering analyses for both in-house and out-of-house missions:
  - Probabilistic Risk Assessment
  - Fault Tree Analyses
  - Failure Mode and Effects Analyses
  - Reliability Block Diagrams and Numerical Assessments,
  - Worst Case Analyses (facilitate/review),
  - Parts Stress Analysis (facilitate/review),
  - Mission Success Criteria (facilitate/review)
  - Limited-Life Items
  - Trend Analyses
  - Numerous other statistical analyses that support design engineering and decision making functions

Typical Reliability Deliverables

RELIABILITY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Reliability Program Plan	***Describes the planned approach for the reliability activities and scheduling of those activities relative to project milestones.***	***•Preliminary to be included with proposal for GSFC review and evaluation. •Draft 30 days after contract award for GSFC review. •Final 30 days before developer PDR for GSFC review and approval. •Updates as required including changes for GSFC review and approval.***
Probabilistic Risk Assessment (PRA)	***A comprehensive, systematic and integrated approach to identifying undesirable events, the scenarios leading to those events, the frequency or likelihood of those events and the event consequences.***	***•Plan with proposal for GSFC review. •Preliminary 30 days before PDR for GSFC review. •Final 30 days before CDR for GSFC approval. •Updates as required for GSFC approval.***
Failure Mode and Effects Analysis (FMEA) and Critical Items List	***Used to identify all modes of failure within a system design, its first purpose is the early identification of all catastrophic and critical failure possibilities so they can be eliminated or minimized through design correction at the earliest possible time.***	***•Preliminary 30 days before PDR for GSFC review. •Final 30 days before CDR for GSFC review •Revisions as required for GSFC review***

Typical Reliability Deliverables

RELIABILITY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Fault Tree Analysis	***•Used to assess mission failure from the top level. Undesired (top-level) states are identified; all possible combinations of basic (lower-level) events are considered to derive credible failure scenarios. The technique provides a methodical approach to identify events or environments that can adversely affect mission success providing an informed basis for assessing system risks.*** ***•The developer shall consider hardware, software and human factors in the analysis.***	***•Preliminary 30 days before PDR for GSFC review.*** ***•Revisions 30 days before CDR for GSFC review*** ***•Final 30 days before Mission Operations Review***
Worst Case Analyses (WCA)	***•Demonstrate design margins in electronic circuits, optics, electromechanical and mechanical items by analyses, test or both to ensure they meet design requirements.*** ***•The developer shall consider all parameters set at worst case limits and worst case environmental stresses.***	***•Available 30 days prior to CDR*** ***•Updates with design changes***

Typical Reliability Deliverables

RELIABILITY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Reliability Assessments and Predictions	***Comparative numerical reliability assessments and reliability predictions in order to evaluate alternative design concepts, redundancy, and part selections.***	***•Available at PDR and CDR for information •Available upon request***
Software Reliability (addressed in Software Assurance section of MAG)	***•Activities to be undertaken to achieve the software reliability requirements, as well as the activities to be undertaken to demonstrate that the software reliability requirements have been verified.*** ***•The developer shall collect, analyze, and track measures that are consistent with IEEE Standard 982.1-1988, IEEE Standard Dictionary of Measures to Produce Reliable Software. Measurements for evaluating reliability (e.g., defect density, mean-time-to-failure, and code complexity) shall be documented.***	***•The developer shall document their Software Reliability program in the Software Management Plan. •Initial draft due upon project inception. •Updated periodically throughout the lifecycle, as necessary. •Final due no later than requirements phase.***
Trend Analyses	***•Monitoring of selected parameters for trends.*** ***•The developer shall maintain and submit a list of subsystem and components to be assessed, and parameters to be monitored.***	***•The developer shall provide a list of parameters to be monitored at the CDR. •The developer shall provide trend analysis reports at the PER, PSR, and FRR.***

Typical Reliability Deliverables

RELIABILITY DELIVERABLE	*OBJECTIVE*	*TIME OF DELIVERY*
Limited-Life Items	***•Defines and tracks the selection, use and wear of limited-life items, and the impact on mission operations.*** ***•The developer shall obtain a program waiver approval by GSFC when the use of an item whose expected life is less than its mission design life.***	***•Preliminary 30 days before PDR for review.*** ***•Final 30 days before CDR for approval.*** ***•Updates as changes are made; between CDR and delivery, for approval.***

Presenter's Lessons Learned

Mike Kelly

Presenter's Lessons Learned

- Develop Mission Assurance Requirements and verify these requirements at the end of the procurement. Never approve supplier's Performance Assurance Implementation Plans (PAIPs). The project can "review" but not "approve" the PAIPs.
- CSOs should develop a professional relationship with all Mission Assurance Director's of Aerospace Companies they deal with
- CSO should develop a professional relationship with all levels within the project (this includes GSFC contracts reps., on-floor personnel, and mgmt.)
- CSO should use non-project (DCMA and NACS/SAC) funded manpower to support the project in the field at all supplier's including (their supplier's-subs)

(CONTINUED)

Presenter's Lessons Learned (continued)

- CSO is on the same team as Project Manager's. Project should understand exactly what the CSO is doing in support of their hardware/software. There must be open communication between the CSO and the Project members at all times.

- It is important that the CSO and Project communicate frequently to maintain a common understanding of intentions/expectations for resolving individual issues for monitoring of the contractor, and for communicating with the contractor. Frequent communication precludes "surprises" and "disconnects" from arising at inopportune times (such as formal reviews or contractor meetings).

- If CSO is working an out-of-house mission, the CSO should develop Letter of Delegation or Task Order for inspections and should visit the supplier regularly. If the CSO does not do this, then in my opinion, he/she is ineffective.

(CONTINUED)

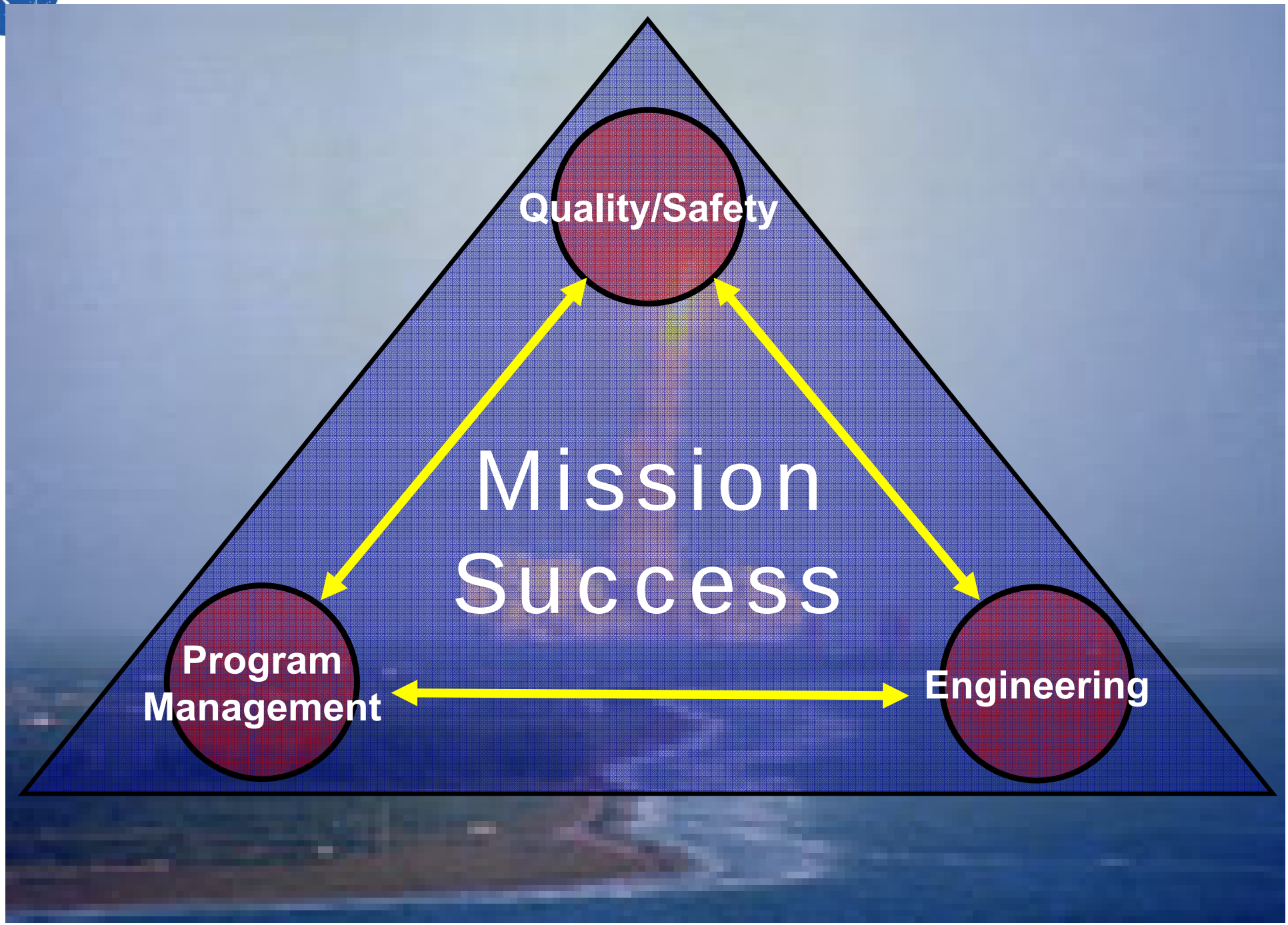
Presenter's Lessons Learned (continued)

- Involve QA, Safety, and Reliability early in the project.
- Ensure that supplier or in-house GIDEP resolutions continue as a launch approaches, including searches of their subcontractor's data.
- The frequency of GIDEP searches and status updates may need to be increased from the "normal" rate as launch date approaches.
- GIDEPs need to be dispositioned in near real-time in the days just prior to launch.
- Ensure that supplier supports post-launch anomaly resolutions.
- Ensure that supplier uses "test as you fly" methods.
- Ensure that supplier documents/tracks "unknown cause" anomalies since they will be scrutinized by Independent Review team.
- Ensure that supplier documents history of any engineering models in the event that they may become flight models.

(CONTINUED)

Presenter's Lessons Learned (continued)

- Institute a weekly telecon with all spacecraft/instrument supplier's to obtain status and track action items.
- Instruments developed by universities typically have been less rigorous in complying with quality requirements.
- University developers require extra scrutiny from Goddard.
- Visit the university to become familiar with the personnel, procedures, and standards.
- Institute periodic hardware inspections and facility audits.
- Compare the university standards to GSFC standards and identify differences.
- Determine workmanship certification status of personnel and their experience levels.
- During PWB development, some projects jump from the Engineering Model to flight development (did not have a protoflight model). Don't do this!!!
- Requirements Flow down and Supplier Control are key areas which must be addressed and performed successfully in order to reduce future spacecraft/instrument problems.


Quality/Safety
Mission Success
Program Management
Engineering