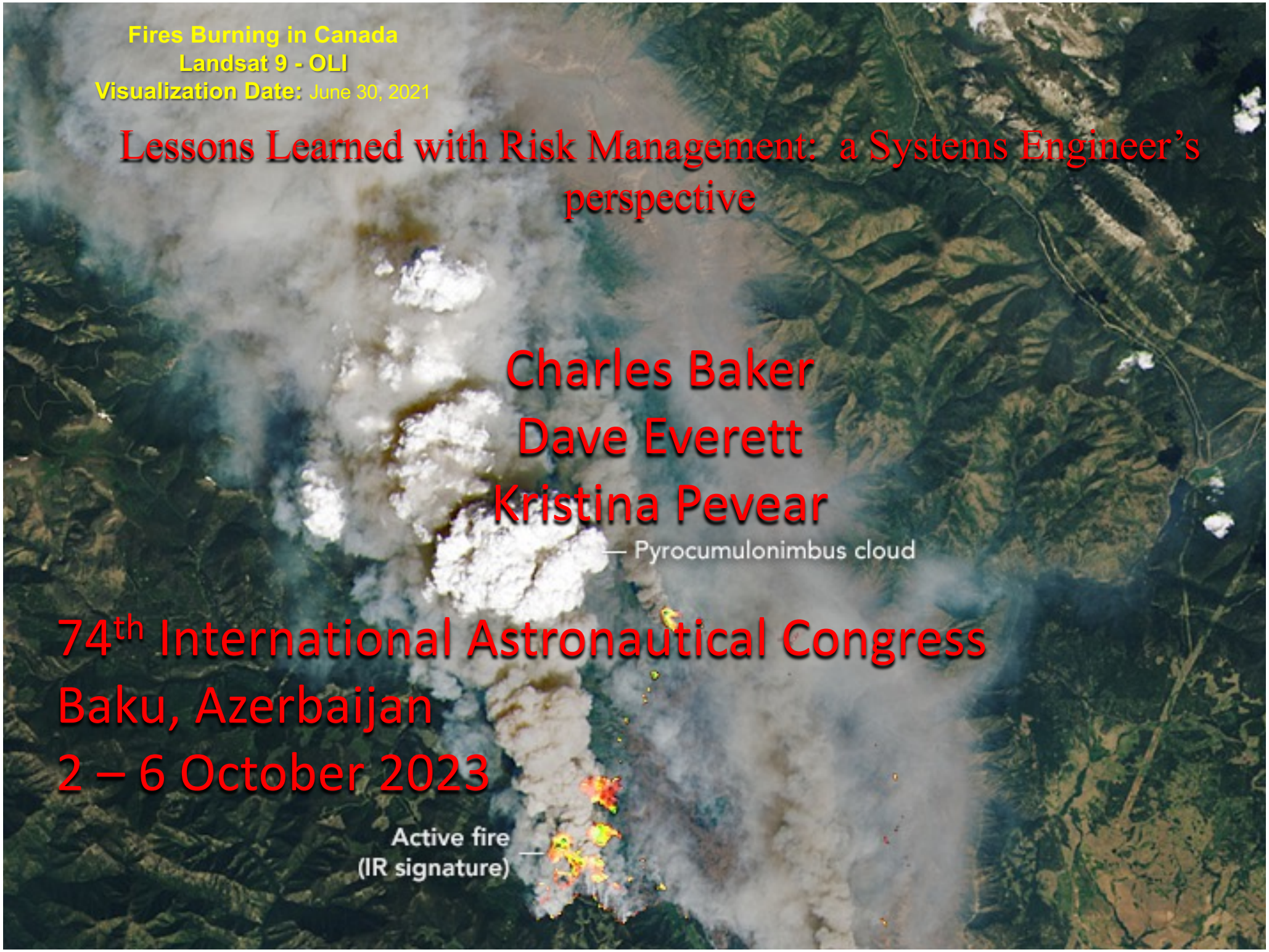


Lessons Learned with Risk Management: a Systems Engineer's perspective

Charles Baker
Dave Everett
Kristina Pevear

74th International Astronautical Congress
Baku, Azerbaijan
2 – 6 October 2023

What is Effective Risk Management?

- **Risk management is a communications device that enables systems engineering to effectively balance risk across the project.**
- **Risk management is most effective (to avoid the consequences of a risk) when mitigation steps start early enough.**
  - This requires a good risk identification process.
- **A well-managed risk identification process rapidly brings serious concerns into the risk management system.**
  - The risks are then communicated directly to management who can allocate resources or exert influence to mitigate them.
- **Risk management must be frequent enough to be useful and in depth enough to bring out emerging issues.**
  - It also requires a trusting relationship between the lead systems engineer and element and/or subsystem leads.
- **Not all concerns or worries are risks; it requires systems engineering expertise to help make the distinction.**
- **Often, the most valuable part of risk management are the conversations regarding concerns and worries, ensuring all teams have their needs heard and met.**

Risk Management Nuts and Bolts

- **Success is highly dependent on the commitment of the lead SE and Project Management team to use this communication device to mitigate risk.**
- **No project proceeds without risk. Well-run projects focus on discovering risks and balancing them with other risks and available resources, thereby avoiding significant consequences.**
- **Even the process of writing a risk can free a flight element to decide to proceed in a certain direction.**
  - Generally, few technical direction decisions can be made without incurring some level of risk.
  - Documenting dissenting opinions in risk form can be a way of enabling the team to move forward, building in a monthly check on whether the technical decision was the right one.
- **The product of the risk management process is a set of written concerns that can be 1) presented, 2) assessed for likelihood and consequence, and 3) assigned a trigger/watch date or mitigation steps.**
  - Quanitified risks can then be addressed or accepted by the project.
- **Most risks have a multitude of likelihoods and consequences that could be attributed to them.**
  - There is generally a subjective sweet spot of likelihood and consequence that bounds every risk.
  - We use the word ‘subjective’, as it is often a bigger discussion with project management and the risk owner that yields a mutually acceptable assessment.
- **Risks whose mitigation plans are continually delayed may be indicative of a project that is in trouble, or of a risk that has fallen to the baseline risk level.**

Types of Risks and Risk Status

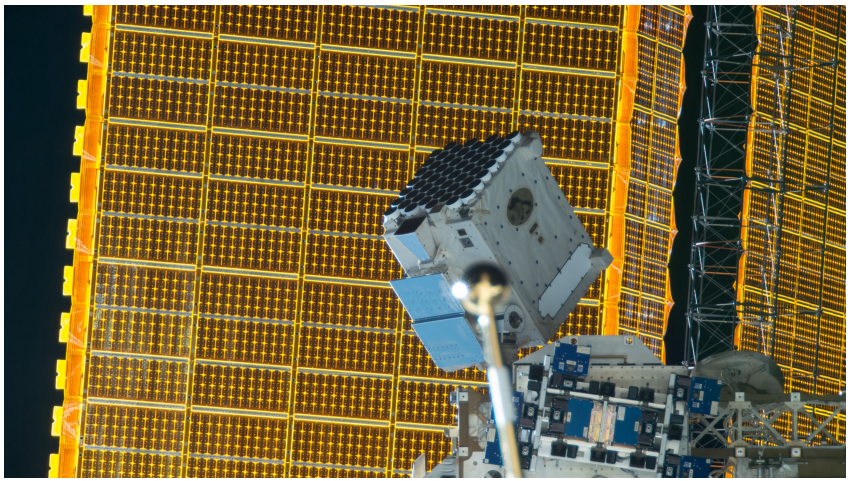
- **The Risk Management philosophy addresses three distinct types of risks: safety, mission performance, and project execution risks.**
  - Safety risks include the potential for personnel injury; this type of risk addresses hazards and other safety related risks.
  - A Mission Performance risk (Technical Risk) has the potential to impact Flight/Ground segments during operations (i.e., preventing "end products" from performing their desired functions in their operational environments). This type addresses inability to meet mission requirements, degraded science, loss of technical margin or system redundancy, or total loss of mission.
  - A Project Execution risk (Programmatic Risk) has the potential to impact development activities or the ability to deliver the required product within the allocated budget, schedule and technical resources.
- **Risks can also be in various states**
  - Composed but Unopened Risks have the potential to become active risks, but not enough is known about them to objectively assess criticality, or to determine if they are above the baseline risk threshold. Capturing these risks drives the team to re-consider monthly whether the risk has reached a state where enough is know to justify it being opened.
  - Watch Risks are risks it isn't possible or worthwhile to Mitigate at this time, but might require action later (often because it is some external threat the project does not have control of).
  - Mitigation Risks are the most common. The risk has been identified and resources are made available to mitigate the likelihood or consequence.
  - Accepted risks are risks for which all possible mitigation steps have been completed, but there is still is above baseline risk that the risk will be realized. These become important in later stages of the mission, but a risk can be accepted at any time in the project lifecycle. An accepted technical risk that can manifest after launch is a residual risk.

Examples from Neutron Interior Star Composition Explorer (NICER) – Example Risks (1 of 2)

➢ Mission Overview

- ISS ESPA Payload, Class D
- Launched on Dragon Transport Vehicle in 2017

Objective	Measurements
Structure — Reveal the nature of matter in the interiors of neutron stars	Neutron star radii to ±5%. Cooling timescales
Dynamics — Uncover the physics of dynamic phenomena associated with neutron stars	Stability of pulsars as clocks. Properties of outbursts, oscillations, and precession
Energetics — Determine how energy is extracted from neutron stars.	Intrinsic radiation patterns, spectra, and luminosities



➢ Example Mitigated Risk from 2015

- Given that Coupled Loads Analysis (CLA) is not required to be performed until 10 months before launch; There is a possibility that: analysis may reveal that some loads are higher than the Design Limit Loads (DLLs) to which NICER is designed, requiring redesign/rebuild and Resulting in: an increase in cost and schedule.

➢ How we used the written risk to mitigate the concern:

- By identifying the specific cost and schedule impacts of the risk, NICER was able to pressure the ISS Program to fund an early CLA with the launch vehicle provider so that the Payload Mechanical Qualification implemented sufficiently high mechanical loads.
- Without this well-defined, quantitatively evaluated risk, it would have been difficult to get the ISS to change their process.
- This also benefited NICER when the originally planned companion payload was de-manifested, and an additional representative CLA was needed to define accurate load cases.
- Communication of this risk supported successful coordination and information exchange with the launch vehicle provider to quantify reduced load sets outside of the standard CLA development process, defining random vibe loads compatible with the NICER X-Ray Timing Instrument (XTI).

Examples from Neutron Interior Star Composition Explorer (NICER) – Example Risks (2 of 2)

➢ Example Mitigated Risk from 2015

- ❑ Given that NICER Detector System or Star Tracker Flight Software (FSW) could fail to be updated on-orbit and be corrupted; There is a possibility that: the NICER Payload functionality would be inhibited Resulting in: Science degradation.

➢ How we used the written risk to mitigate the concern:

- ❑ We wanted to ensure that if the FSW in the Detector System and Star Tracker were corrupted due to a memory or radiation event we could upload a new version to fix the errors.
- ❑ This ultimately led to a boot up code review for each of these components.
- ❑ During Payload level testing, we also demonstrated the ability to update FSW through our ground system prior to launch.

➢ Example Residual Risk from 2016

- ❑ Given that: NICER will be in its stowed orientation on the ground for almost a year; There is a possibility that: the required torque margins could be lower on-orbit initially as the actuator lubricant creeps in a 1-g gravity field; Resulting in NICER failing to deploy on-orbit.

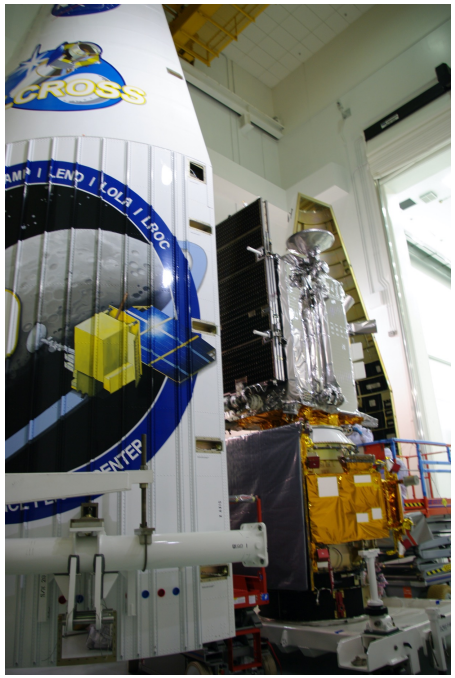
➢ How we used the written risk to mitigate the concern:

- ❑ After delivery to the Kennedy Space Center, NICER needed to remain in its stowed configuration for a year prior to launch
- ❑ We had a risk-risk trade in this case:
  without movement for a year, there was a risk that the lubricant in the stepper motor actuators would pool and make the first movements of the actuators more difficult or seize
  OR
  a workmanship risk if the project elected to perform significant structural mechanical disassembly to move the complicated 3-axis pointing system after mechanical qualification post-delivery;
- ❑ The project determined that the workmanship risk and potential damage to NICER of performing disassembly post-ship and using Mechanical Ground Support Equipment to move the articulated arm was more significant than the risk the actuators would be seized by pooled lubricant.

Examples from Lunar Reconnaissance Orbiter (LRO) (1 of 2)

➢ Mission Overview

- ❑ Launched in 2009, Class C
- ❑ 50 km mean Lunar Polar Orbit
- ❑ LRO mission objectives are to conduct investigations specifically targeted to prepare for and support future human exploration of the moon
- ❑ Locate Potential Resources
- ❑ Safe Landing Sites
- ❑ Understand the Space Environment



➢ Example Mitigated Risk from 2007

- ❑ If the flight power converters for the C&DH do not arrive on time, then the flight C&DH will not be delivered on time, delaying the launch. Context: The flight power converters were very late and the vendor was not providing a delivery date. The C&DH was needed for system-level testing.

➢ How we used the written risk to mitigate the concern:

- ❑ When the C&DH lead mentioned this concern during a regular one-on-one risk meeting, he thought the project was aware of his concern, since he had mentioned it to the project's parts expert.
- ❑ Needless to say, the project manager wasn't closely tracking every part delivery on the project, but it was clear to the systems engineer at this meeting that this part could end up being a big problem.
- ❑ The center director contacted the company to ask about the part status and apply some urgency to the delivery.
- ❑ In parallel, the project started the process of up-screening some engineering parts which were already in hand.
- ❑ Building up the spare card bought time—the C&DH team integrated the box and worked through the various issues that pop up during integration.
- ❑ The system-level integration went forward with very little impact to the mission schedule.

Examples from Lunar Reconnaissance Orbiter (LRO) (2 of 2)

➢ Example Residual Risk from 2006

- ❑ If: A failure or error occurs during the critical Lunar Orbit Insertion (LOI) phase of the mission, then loss of the mission may occur.

➢ How we used the written risk to mitigate the concern:

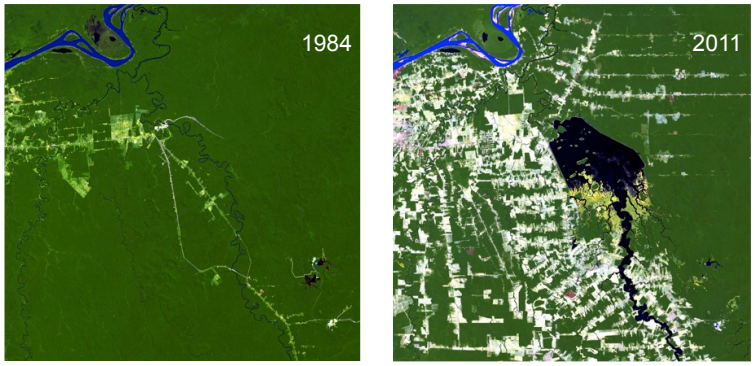
- ❑ The LOI was a critical, one-time event that needed to occur on time, with the burn in the correct direction for the correct duration.
- ❑ LRO utilized a direct trajectory to the Moon, so the LOI would occur just five (5) days after launch. If the burn was missed, getting back to the Moon was somewhere between unlikely and impossible.
- ❑ The project assigned a dedicated phase lead, who was also the Deputy Mission Systems Engineer, to track all aspects of LOI.
- ❑ The final LOI burn design only required the team execute half the planned change in velocity (delta V), which allowed for failure of half the thrusters or an early end to the burn while still successfully capturing into lunar orbit.
- ❑ The other major risk mitigation was the careful planning of the operations, including ground-in-the-loop contingencies.
- ❑ The LRO team prepared to handle unexpected issues by thoroughly planning and training for contingencies, including unexpected situations that might require real-time troubleshooting and commanding.
- ❑ After all ground simulations were complete, the team accepted the remaining residual risk of an unsuccessful LOI.

- ❑ Even though this risk did not manifest as a problem, all the preparation gave the team confidence that they were ready for any survivable anomaly.

Examples from Landsat 9 (1 of 2)

➢ Mission Overview

- ❑ Landsat Launched in 2021, Class B
- ❑ LEO 705 km, 10:11 am MLT descending node
- ❑ Landsat provides multispectral imagery supporting key science and societal benefit areas:
  - ❑ *Mapping Land Use & Change*
  - ❑ *Forest Dynamics*
  - ❑ *Agriculture & Evapotranspiration*
  - ❑ *Ecosystem Science*
  - ❑ *Surface Water Quality*
  - ❑ *Glacier & Ice Sheet dynamics*
  - ❑ *Geology and Natural Resources*
- ❑ Landsat remains the most *widely cited* land remote sensing system in the peer-reviewed literature and provided $2.06B of *economic benefits* to the U.S. in 2017*.



Forest Change

➢ Example Mitigated Risk from 2020

- ❑ Given that: Landsat 9 is going to conduct their observatory-level thermal vacuum test in the midst of the Global COVID 19 pandemic; There is a possibility that: key personnel will not be able to support the test onsite and may miss a performance or functional anomaly that could result in damage to Landsat 9, Resulting in: schedule loss to recover.

➢ How we used the written risk to mitigate the concern:

- ❑ There were extensive conversations conducted within the team including the prime contractor and instrument providers about how best to mitigate this significantly likely risk.
- ❑ Multiple thermal vacuum planning sessions that focused on the unique remote support were conducted team wide.
- ❑ We developed unique Webex enabled remote terminals that allowed remote support to view key telemetry pages and trending graphs.
- ❑ We tasked on-site support to communicate clearly with remote support what was happening within the control room. We developed protocols and console spaces that protected the on-site workers.
- ❑ We paused after each test phase was completed and ensured all the technical stakeholders had been able to review the telemetry and performance data to ensure no anomalous behavior was observed in the previous phase.

Examples from Landsat 9 (2 of 2)

➢ Example Mitigated Risk from 2020

- ❑ Given that the common JPSS/Landsat9 Solar Array Drive Assembly design Life Test Unit, failed during Life Test and the FRB concluded the failure was due to inadequate harmonic drive lubrication, there is a possibility that the Landsat 9 unit will fail prematurely or if replaced fail due inadequate post-repair qualification testing, Resulting in shorter mission life of Landsat 9.

➢ How we used the written risk to mitigate the concern:

- ❑ The life test failure itself occurred before Observatory-level testing of Landsat 9.
- ❑ The life test failure occurred after the nominal 2 times lifetime for Landsat 9 had been completed (JPSS has a longer baselined mission lifetime).
- ❑ As the investigation continued, it became apparent the under-lubrication of the actuator would induce an unknown limited life of the Landsat 9 Solar Array Drive Assembly (SADA).
- ❑ Once we decided we needed to refurbish our SADA, we noticed that a refurbished unit would arrive after our scheduled Observatory T-Vac test.
- ❑ We performed a risk-risk study, looking at the risk of an inadequate Observatory T-Vac test without the flight SADA versus the risk of delaying the test to wait for the flight SADA.
- ❑ We determined the SADA wasn't in the flight or thermal configuration during Observatory testing anyway, therefore, the risk for testing without the flight SADA was low.
- ❑ We completed Observatory T-Vac, and then installed the flight SADA after all regression testing was completed.

Example from OSIRIS REx

➢ Mission Overview

- ❑ The OSIRIS-REx planetary spacecraft launched on September 8, 2016.
- ❑ OSIRIS-REx is a Class B mission.
- ❑ It entered the asteroid Bennu's vicinity in 2018.
- ❑ It successfully retrieved a sample of Bennu on October 20, 2020.
- ❑ Bennu may contain the molecular precursors to the origin of life and the Earth's oceans.
- ❑ Bennu is also one of the most potentially hazardous asteroids, as it has a relatively high probability (~1:1800) of impacting the Earth late in the 22nd century.
- ❑ OSIRIS-REx determined Bennu's physical and chemical properties, which will be critical to know in the event of an impact mitigation mission.
- ❑ Finally, asteroids like Bennu contain natural resources such as water, organics, and precious metals.

➢ Example Mitigated Risk from 2012

- ❑ If: Ground performance and life testing of GNC Lidar is insufficient to uncover latent defects in design or manufacturing, Then: There may be technical impacts related to reliability on-orbit affecting [the mission critical] Touch And Go (TAG) success." Context: A small company with limited experience was selected to build the lidar. The design was based on a lidar that only needed to operate in low-Earth orbit for a short period of time. There was question about the maturity of the technology the company planned to fly.

➢ How we used the written risk to mitigate the concern:

- ❑ Several components of the lidar were identified as less than TRL-6, and project management worked with the vendor to establish a plan to build and test these key components before mission PDR.
- ❑ During this testing, several failures occurred, and the vendor updated the design appropriately.
- ❑ Engineering had identified an option to use cameras instead of the lidar to navigate to the surface of the asteroid for sample collection, but this capability would require significant software development.
- ❑ At the time of the Pre-Ship Review (PSR), the flight lidars were not yet on the spacecraft because of all of the development issues. But because of the fully-implemented and qualified status of Natural Feature Tracking (NFT), the project was able to hold schedule and ship to the launch site, where both lidars were integrated just 3 months before launch.
- ❑ Upon arrival at Bennu, the team discovered the asteroid to be much rockier than expected resulting in NFT being more accurate and safer than the Lidar.

Summary

- **Risk Management is an important tool that helps to identify, mitigate, and sometimes accept unique risks during the development of missions.**
- **Effective Risk Management has helped enable key NASA missions of various classes to be successfully launched and meet their mission objectives, while remaining within cost and schedule constraints.**
- **At the mission systems level, it is a key tool to help identify previously unknown concerns, quantify their likelihood and consequence, and develop a mitigation plan to reduce these concerns.**
- **Without this tool, projects will experience an increased number of problems, erosion of schedule, and increased cost during development, as well as additional problems post launch that may jeopardize their mission.**
- **Understanding how to optimize the value of risk management, and minimize formal process effort, is what every project strives to do. Examples from NICER, LRO, Landsat 9, and OSIRIS-REx will hopefully aid in that endeavor.**