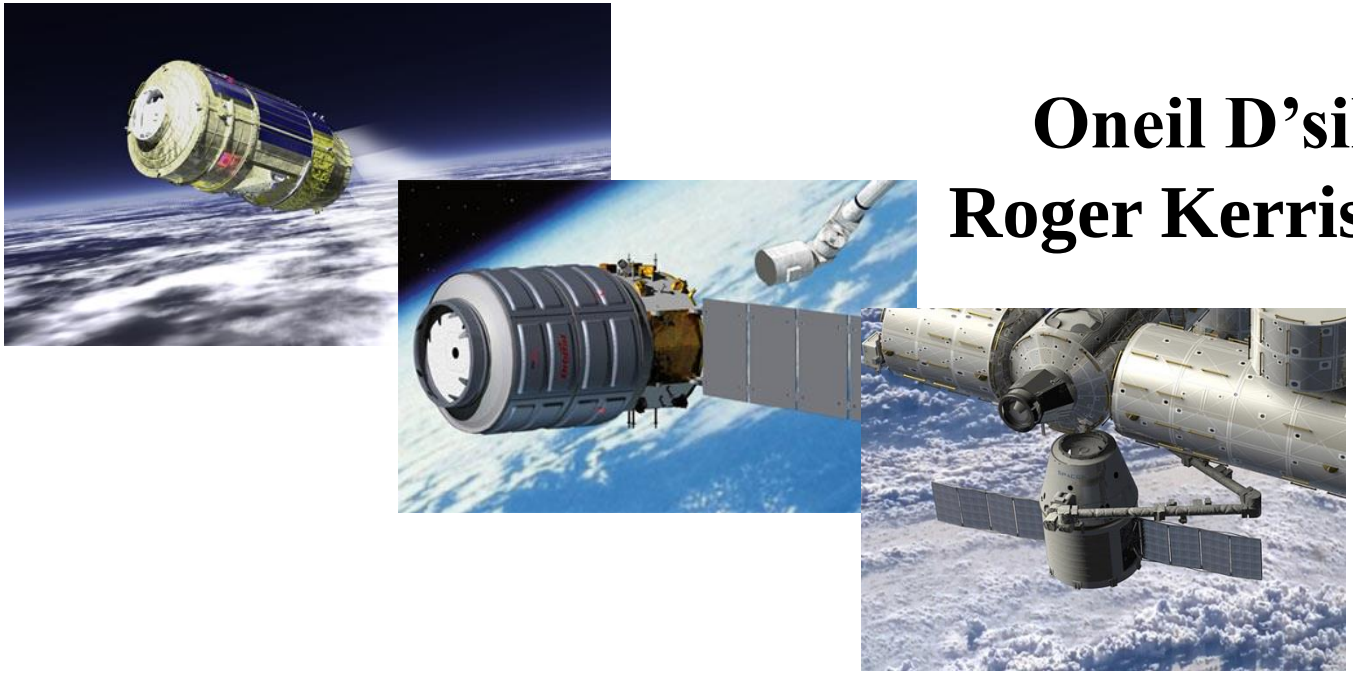
Probability Risk Assessment Methodology Usage on Space Robotics for Free Flyer Capture



Oneil D'silva
Roger Kerrison

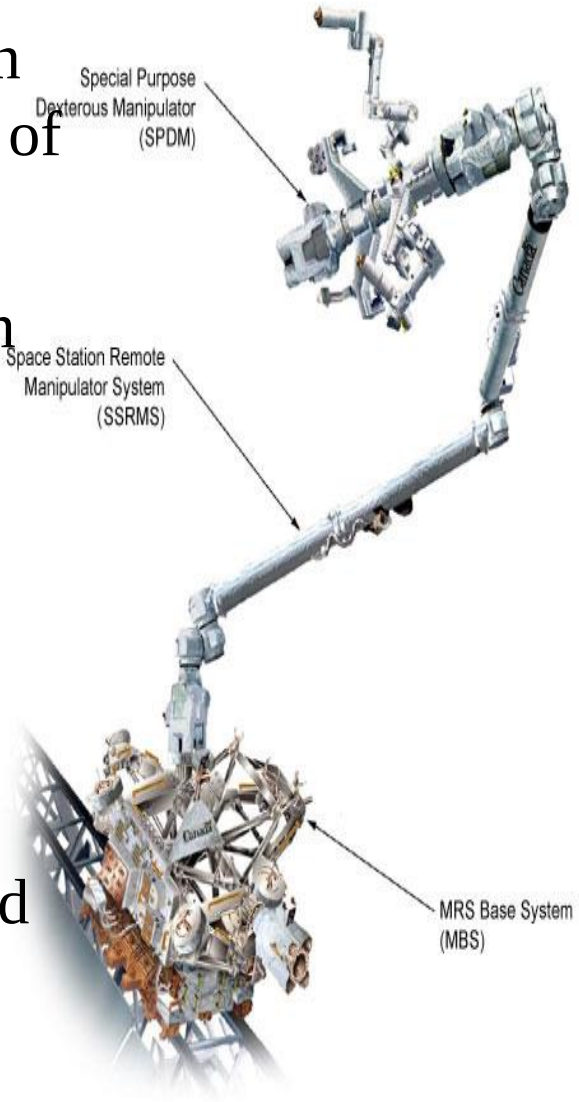
Agenda

- Introduction
- Background
- Applicability of existing Industry standard Probability risk Assessment Methodologies
- Application of Probability Risk Assessments methodology
- Results of Application of Probability Risk Assessments methodology to the SSRMS
- Conclusion / Recommendations
- Video of Free Flyer Capture

- The purpose of this paper was to summarize the guidelines and assumptions that cover the usage of PRA methodology for Space Robotics.
- PRA methodology was used to assess the level of risk that is associated with the potentially hazardous event of collision of a Free flyer with the International Space Station (ISS), and provide a guideline to help either mitigate and/or accept the risk.
- The collision could potentially be generated by an unsuccessful capture of a Free Flyer (HTV, Dragon, Cygnus) by the Mobile Servicing system (MSS).

Background

- The CSA Mobile Servicing system (MSS) is an electromechanical robotic system that consists of three system robots:
  - Space Station Remote Manipulator System (SSRMS) (Canadarm2)
  - Mobile Servicing System (MBS)
  - Special Purpose Dexterous Manipulator (SPDM).
- The MSS's main duties consist of transferring cargo, Extra-vehicular Activity (EVA) crew and assorted scientific and supply payloads to various external locations on the ISS.



Background

- SSRMS role being expanded to include Free Flyer Capture.
- The SSRMS consists of seven motorized Joints, two Latching End Effectors (LEEs) (a base and a tip), and fully redundant (active and backup) power and data electronic strings.

- The SSRMS can be controlled via the Robotic Workstation (RWS) aboard the ISS or by Ground Control (GC) at NASA.
- The RWS or GC can also be used to perform a full electrical and mechanical system readiness verification known as a Checkout.

Applicability of existing PRA methodologies

- The ISS program requires all orbital systems to be two-fault tolerant.
- MSS hazards were dealt with using the standard techniques as outlined below:
  - Analysis of Design/Concept
  - Failure Modes and Effects Analyses (FMEA)
  - Standardized Hazard Checklists
  - Application of additional techniques such as:
    - Design for minimum risk.
    - Incorporation of safety devices.
    - Incorporation of warning devices.
    - Develop procedures and training.

Applicability of existing PRA methodologies

- Current design of the MSS is mature and currently in use on-orbit.
- The risks of a possible Free flyer collision with the ISS due to a failed capture cannot be completely eliminated using standard techniques previously stated.
- Application of Probability risk assessment methodology allows us to manage and/or accept the risk of Free flyer capture.
- For rare events, for which there is no past failure experience at all or the data are very sparse, probabilistic failure models can be developed with tools like fault trees analysis (FTA).

Applicability of existing PRA methodologies

- Using FTA to quantify the hazard risk is only a part of the overall probability risk assessment methodology.
- In order to properly assess the likelihood of an event occurring and the magnitude of the risk involved, hazard risk probability ranges can be compared to the hazard risk values calculated from the FTA.
- Hazard risk probability range values outlined in MIL-STD-882 DoD Safety Practices standards are generally used as a starting point for the majority of United States (U.S.) military and civilian space and aviation FTA analyses.
    - FAA has adopted and recommended use of the identical Probability range values.

Applicability of existing PRA methodologies

Description	Level	Individual Item	Probability Range
Frequent	A	Likely to occur often in the life of an item	Probability of occurrence greater than or equal to 10^{-1}.
Probable	B	Will occur several times in the life of an item	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}.
Occasional	C	Likely to occur sometime in the life of an item	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}.
Remote	D	Unlikely, but possible to occur in the life of an item	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Probability of occurrence less than 10^{-6}.
Eliminated	F	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.	

MIL-STD-882: DoD Standard Practice System Safety.

Applicability of existing PRA methodologies

- European Aviation Safety Agency (EASA) CS-25 Book 2 regulations have different risk failure condition values :
  - Probable Failure Condition: Greater than 10^{-5}.
  - Remote Failure Condition: Less than or equal to 10^{-5} and greater than 10^{-7}.
  - Extremely Remote failure condition: Less than or equal to 10^{-7} and greater than 10^{-9}.
  - Extremely Improbable Failure Conditions: Less than or equal to 10^{-9}.
- These regulations were adopted from the original European Joint Aviation Authorities (JAA) JAR-25 regulations.

Application of PRA methodology

- The Free Flyer capture FTA analyzed the SSRMS for single and multiple point failures, based on Failure rate values and the probability of failure during a specified hazardous window.
- Failure rate values involved in the FTA analysis are as follows:
  - Hardware Failure Rates: Based on MIL-HDBK-217 F2.
  - Duty Cycle: Includes periods of operation and dormancy. SSRMS spends most of time in dormant phase.
  - Induced Errors: Included as K-factor and covers factors such as environmental damage and operator error. Operator Error: Included as part of the induced K-factor.
  - Software Error: Considered Negligible due to prior testing.
  - Aging/Wearout: Considered Negligible based on the use of Checkout.

Application of PRA methodology

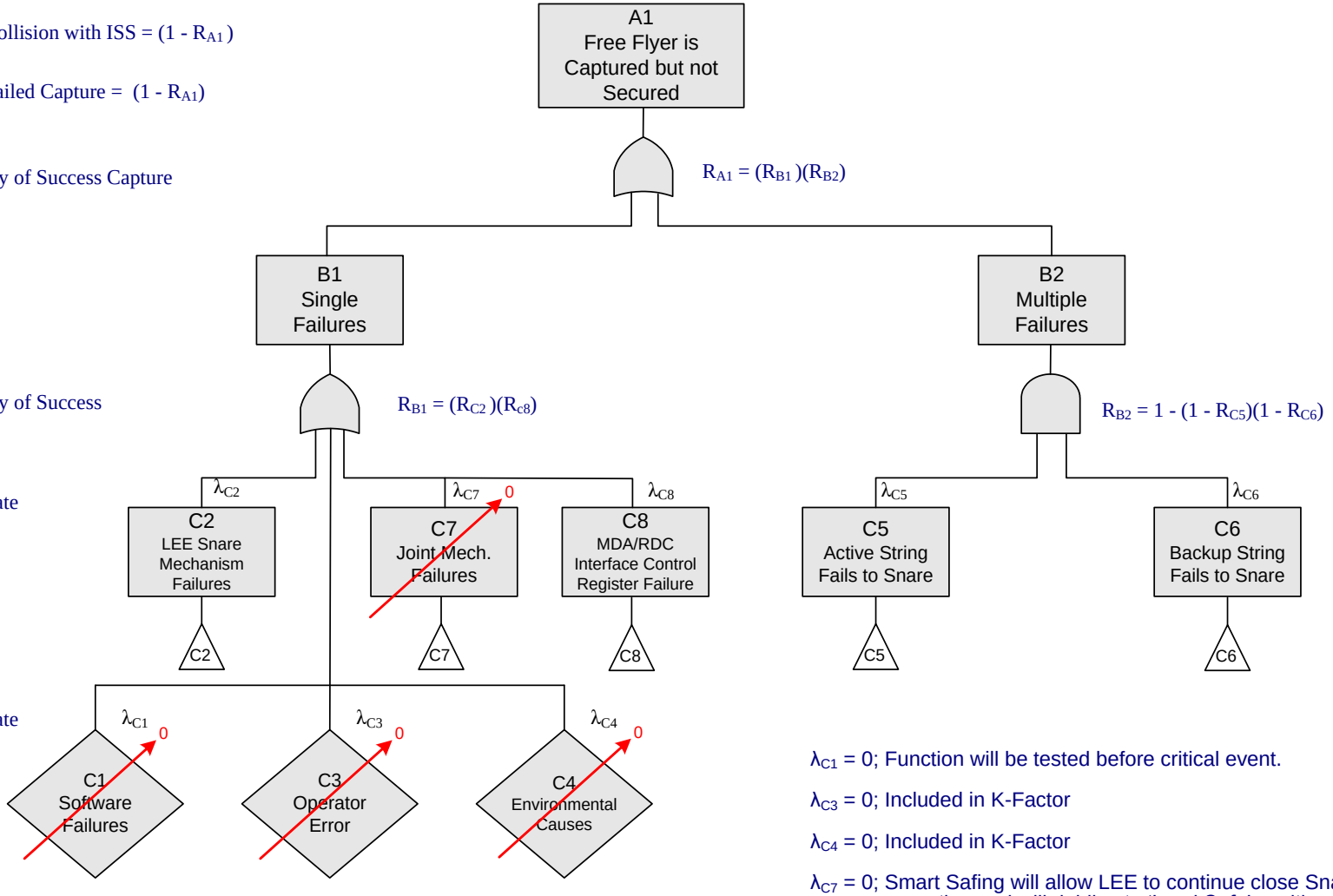
- Given that the SSRMS has already been designed, built and launched, failure rate values can be considered non-variable.
- Thus, FTA is dependent on the overall size of the hazardous window:
  - FTA was done for the period beginning from Free flyer launch to Free flyer capture.
  - Analysis assumed that any undetected failures during either the dormant Approach phase and/or the active Capture phase could result in a failure of the SSRMS to capture and secure the Free Flyer.
  - Analysis assumed that the SSRMS could be tested / "checked out" anytime before the Free flyer capture attempt in order to properly determine the risk of collision.

Application of PRA methodology

Risk of Collision with ISS = $(1 - R_{A1})$

Risk of Failed Capture = $(1 - R_{A1})$

Probability of Success Capture



Probability of Success

Failure Rate

Failure Rate

$\lambda_{C1} = 0$; Function will be tested before critical event.

$\lambda_{C3} = 0$; Included in K-Factor

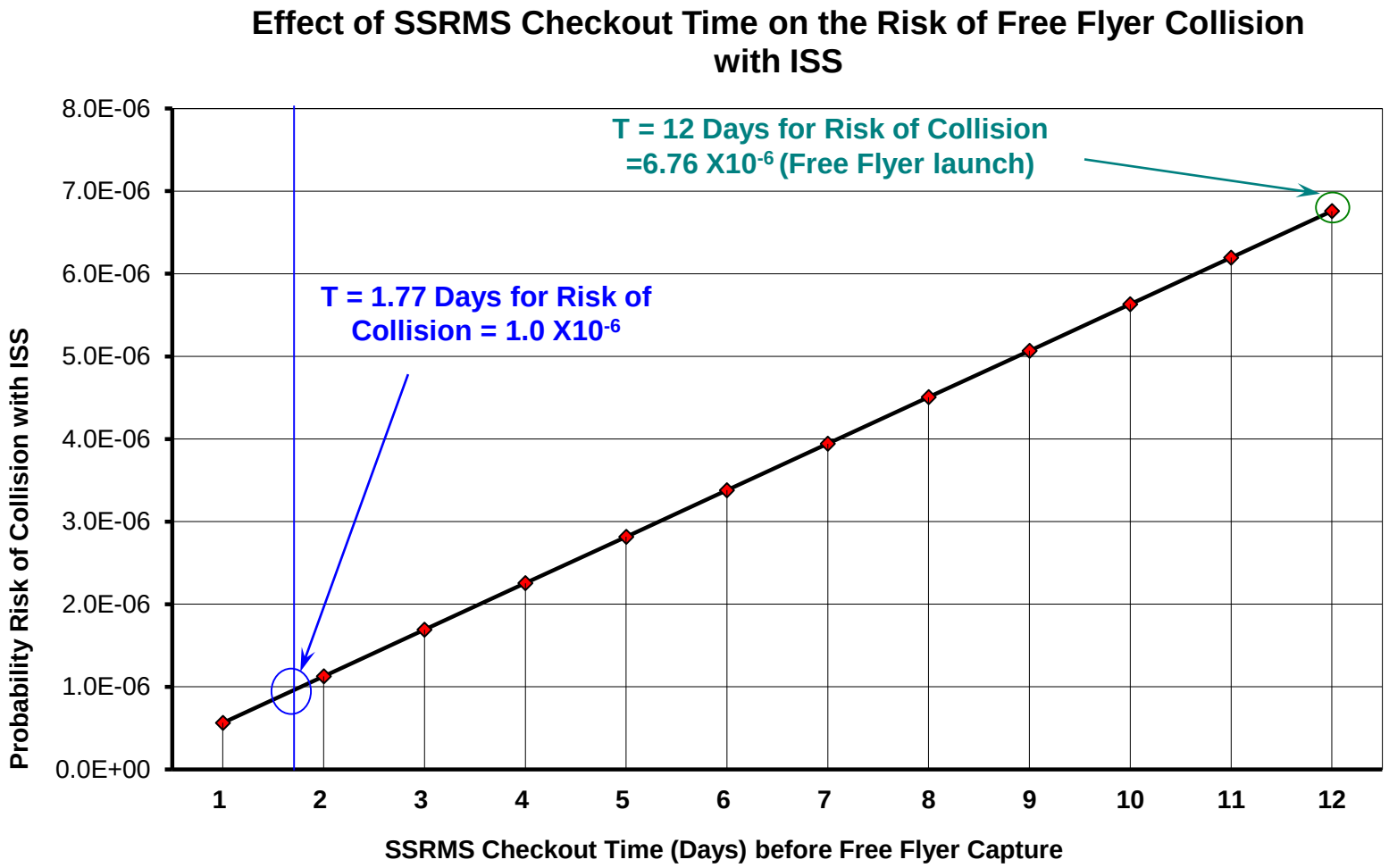
$\lambda_{C4} = 0$; Included in K-Factor

$\lambda_{C7} = 0$; Smart Safing will allow LEE to continue close Snare operation and will rigidize to 'Load Safe' position.

Results of PRA methodology

- The Hazardous window associated with the capture of a Free flyer is potentially in the order of 12 days (time from last checkout prior to launch of the free flyer)
- Overall risk of a Free flyer capture during that interval falls into the FAA/DoD Remote and EASA CS Remote hazard risk probability ranges or lower.
- If the Hazardous window is reduced to the order of 1.77 days, the risk falls into the FAA/DoD Improbable (Remote) range.
- These risk values allow the ISS Program to quantify and “Accept” the risk, which allowed the SSRMS to proceed with Free flyer capture.

Results of PRA methodology



- A major conservative assumption in this FTA is that the Probability Risk of a Free flyer collision with the ISS was assumed to be equal to the Probability risk of a failure of the SSRMS to capture the Free flyer.
  - Incorporation of the Free flyer's safety devices (such as the ability to release the grapple fixture); and the effects of orbital trajectory effects, would have reduced the overall risk range even further.
- Additionally, the ISS crew is trained to recognize the first failure and to switch to an active redundant string, and thus regain control of the situation.
- MSS is capable of Smart Safing, which 'safes' the failed item rather than the entire system.

Conclusion / Recommendations

- Extremely valuable tool that can be used in all phases of a systems life cycle.
  - Allows for a means to accept risks for hazards that cannot be mitigated, thus allowing for expanded mission utilization.
  - PRA methodology is a specialized tool that can be used to analyze specific failure scenarios and must be used together with the other standard hazard analysis techniques (e.g. FMEA) when evaluating system safety.
- PRA methodology is highly recommended as a means to increase safety, reliability and usability for new operational roles in space exploration, while controlling overall program costs.
  - In the case of the MSS, this includes Free Flyer Capture and any possible future operational roles.

Video of Free Flyer Capture