Dynamic Positioning Committee

Marine Technology Society

DYNAMIC POSITIONING CONFERENCE
October 10-11, 2017

RISK / TESTING SESSION

Dynamic Positioning System (DPS) Risk Analysis Using Probabilistic Risk Assessment (PRA)

Eric B. Thigpen

NASA/SAIC

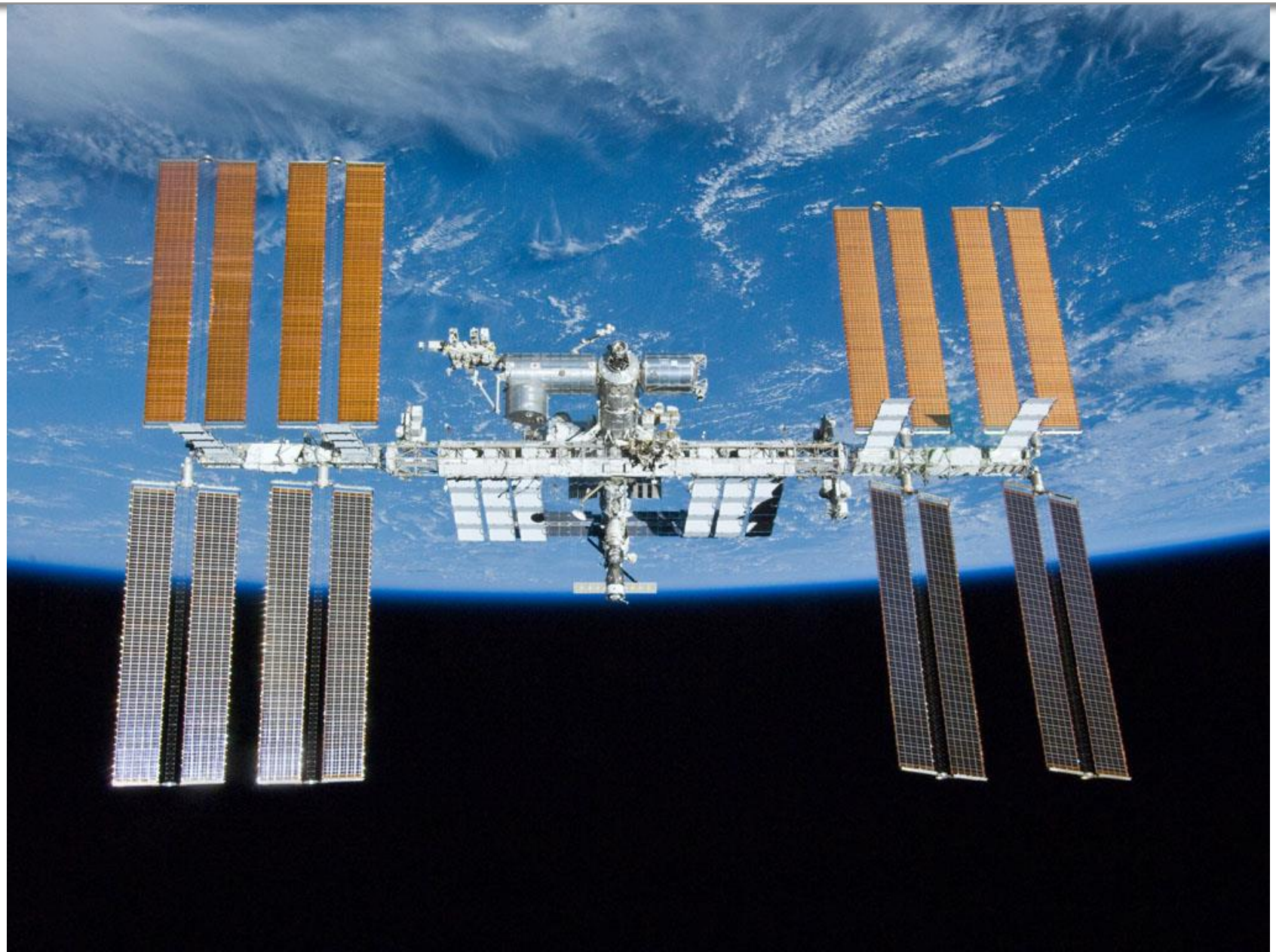
eric.b.thigpen@nasa.gov

1. Why NASA's experience is relevant to the oil and gas industry.

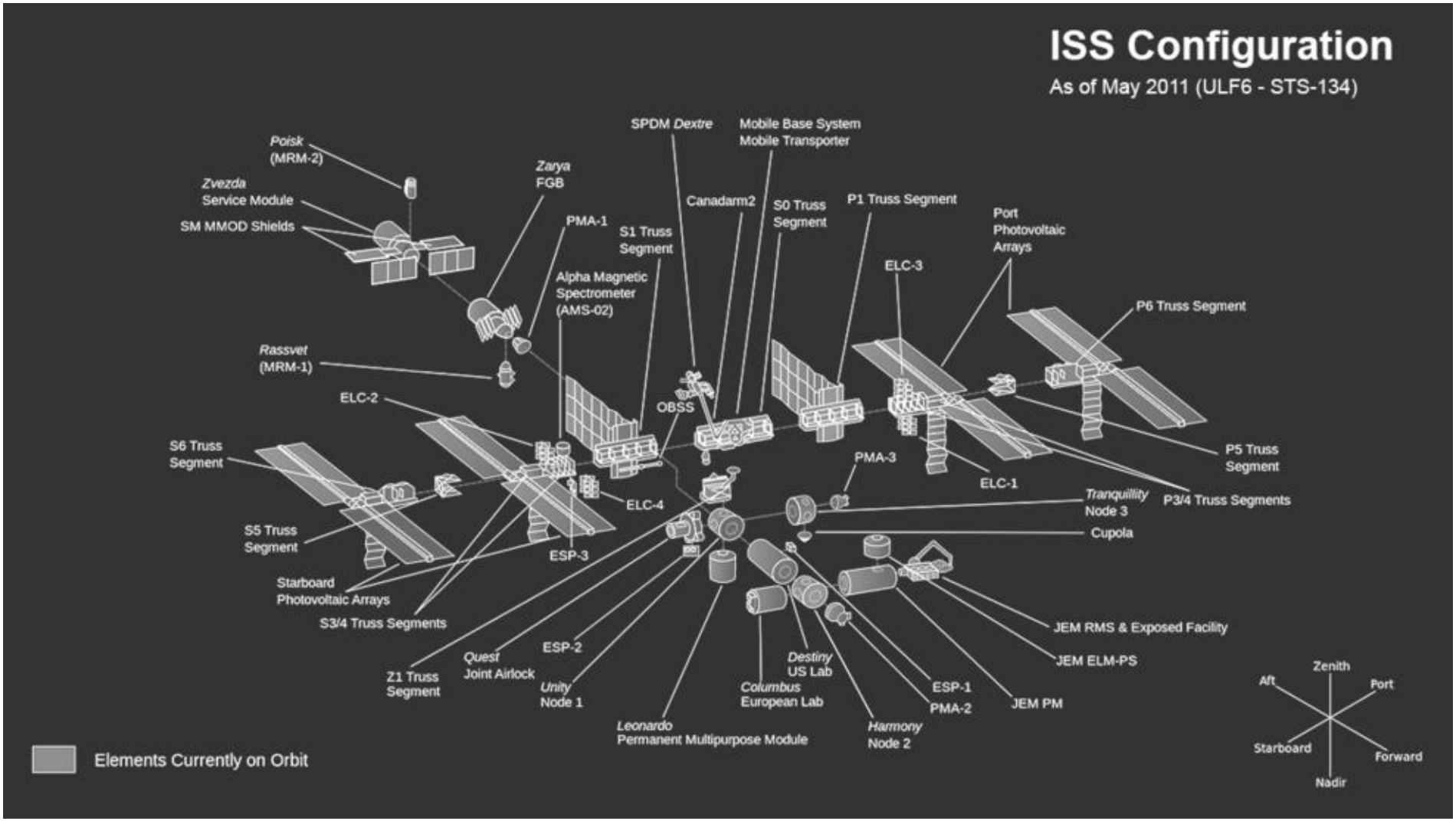
2. Probabilistic Risk Assessment (PRA) overview.

3. Application of the PRA process to a Dynamic Positioning System (DPS).

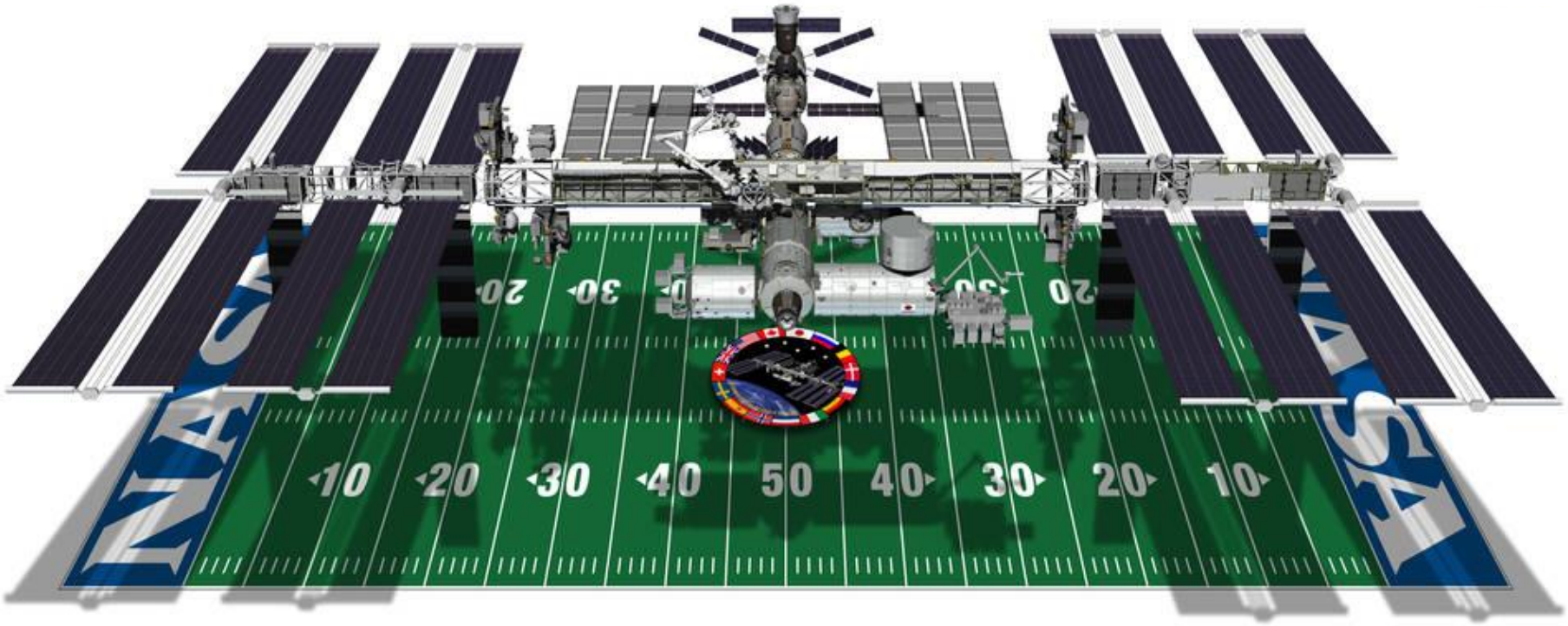
International Space Station



International Space Station

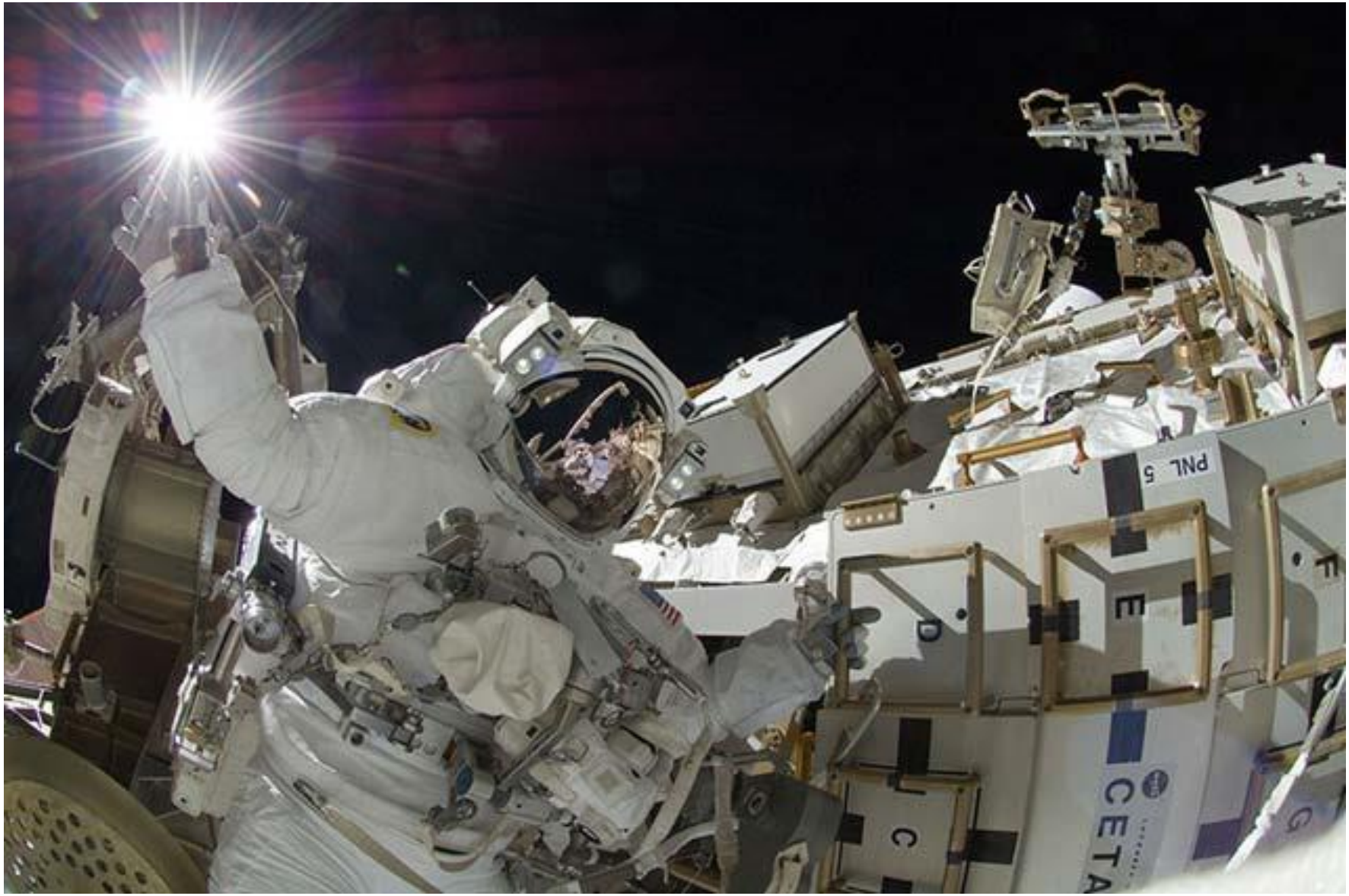


International Space Station

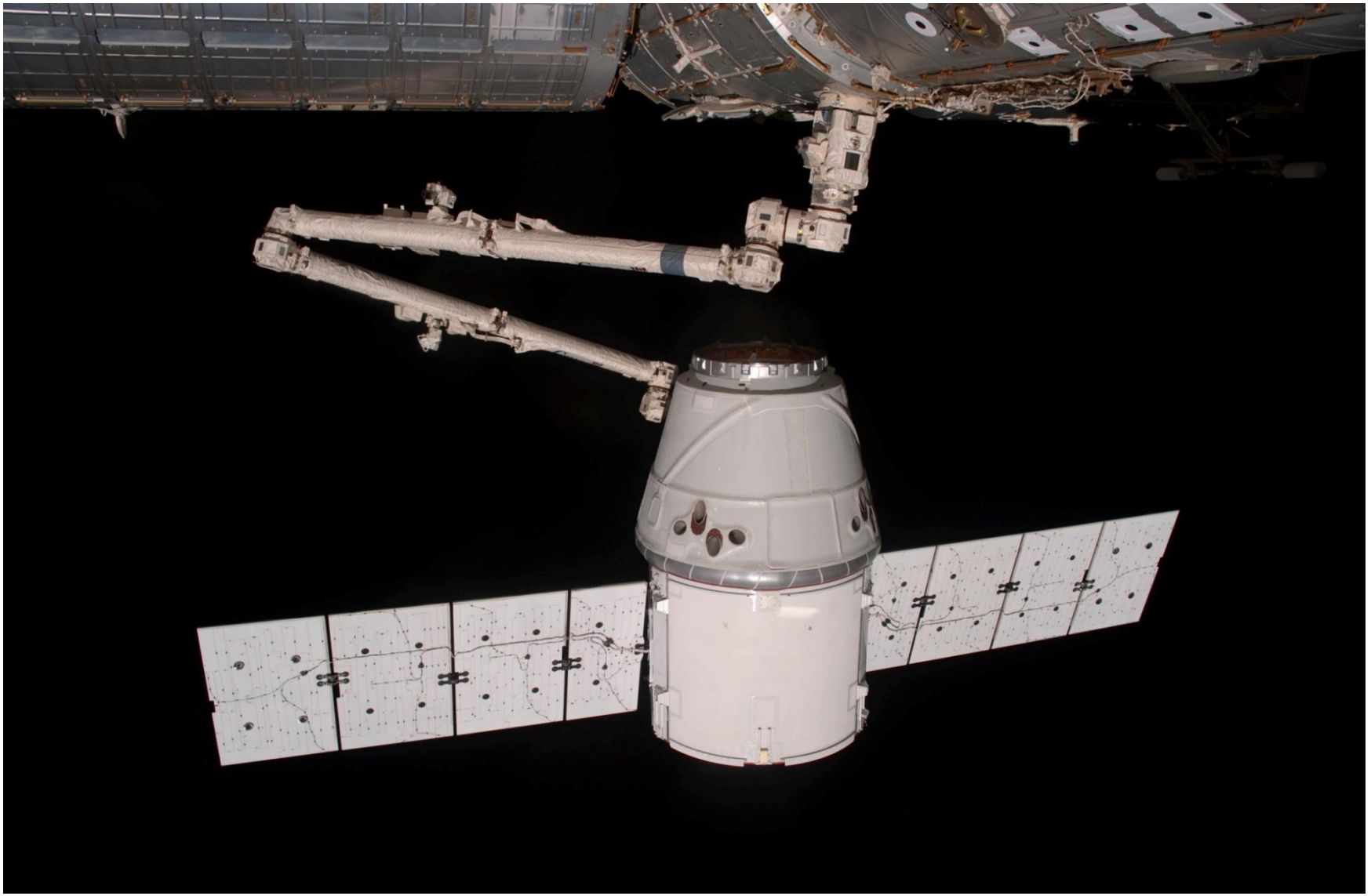


Complex Operations Dependent on Human Involvement

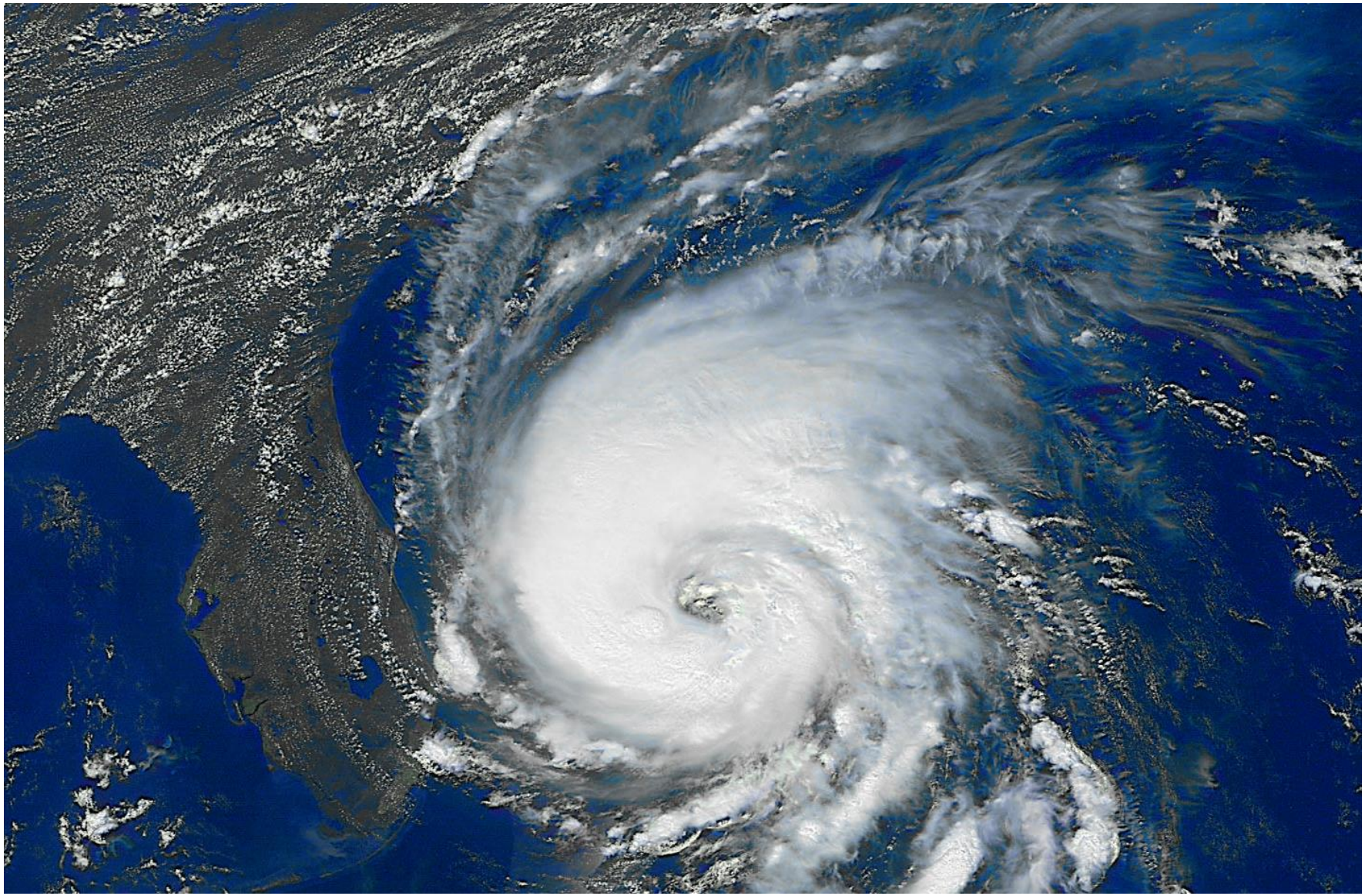
Repair and Maintenance Operations in a Hostile Environment



Ongoing Resupply Operations



Isolated and Not Easily Accessible



1. Why NASA's experience is relevant to the oil and gas industry.

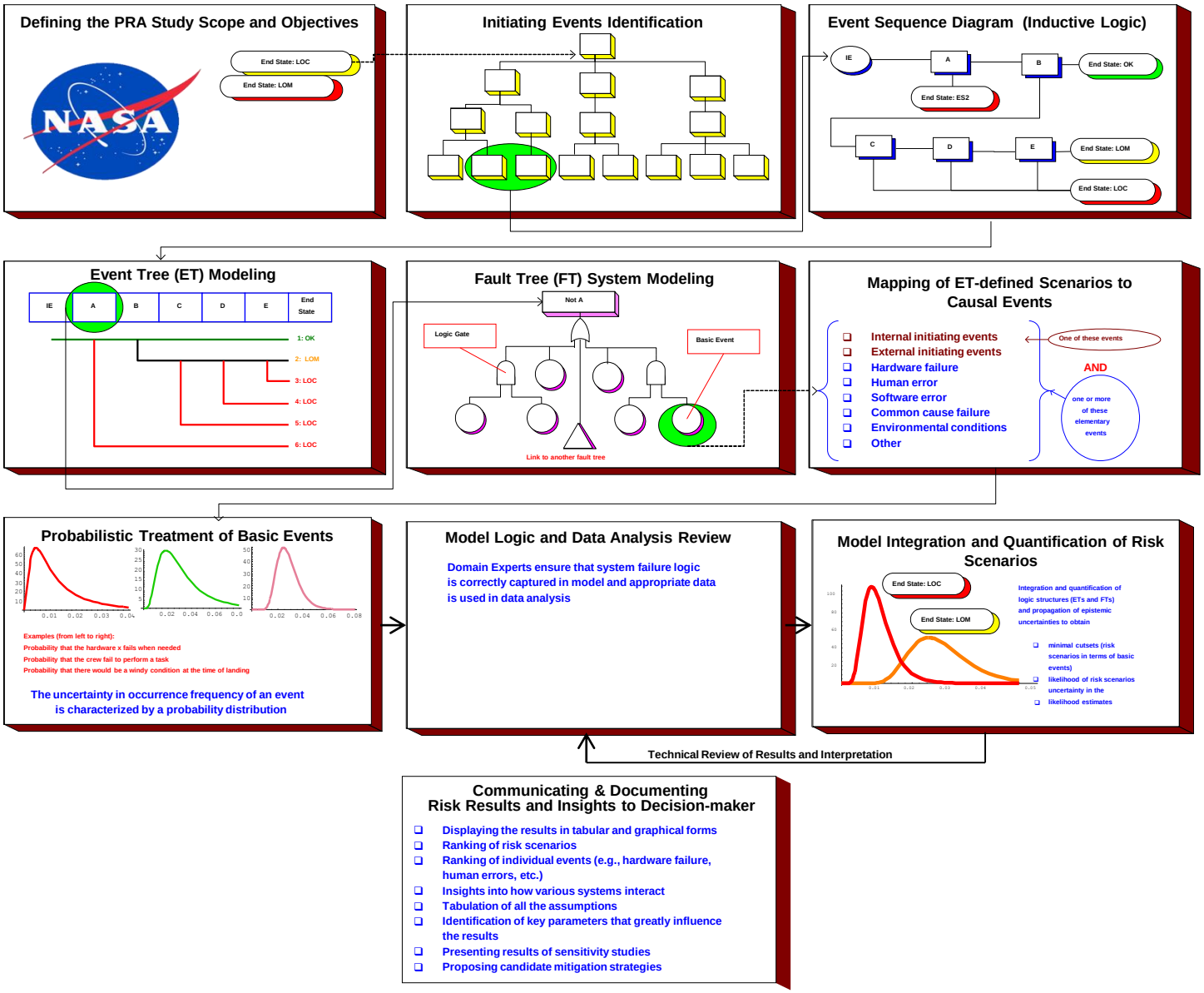
2. Probabilistic Risk Assessment (PRA) overview.

3. Application of the PRA process to a Dynamic Positioning System (DPS).

What is a PRA?

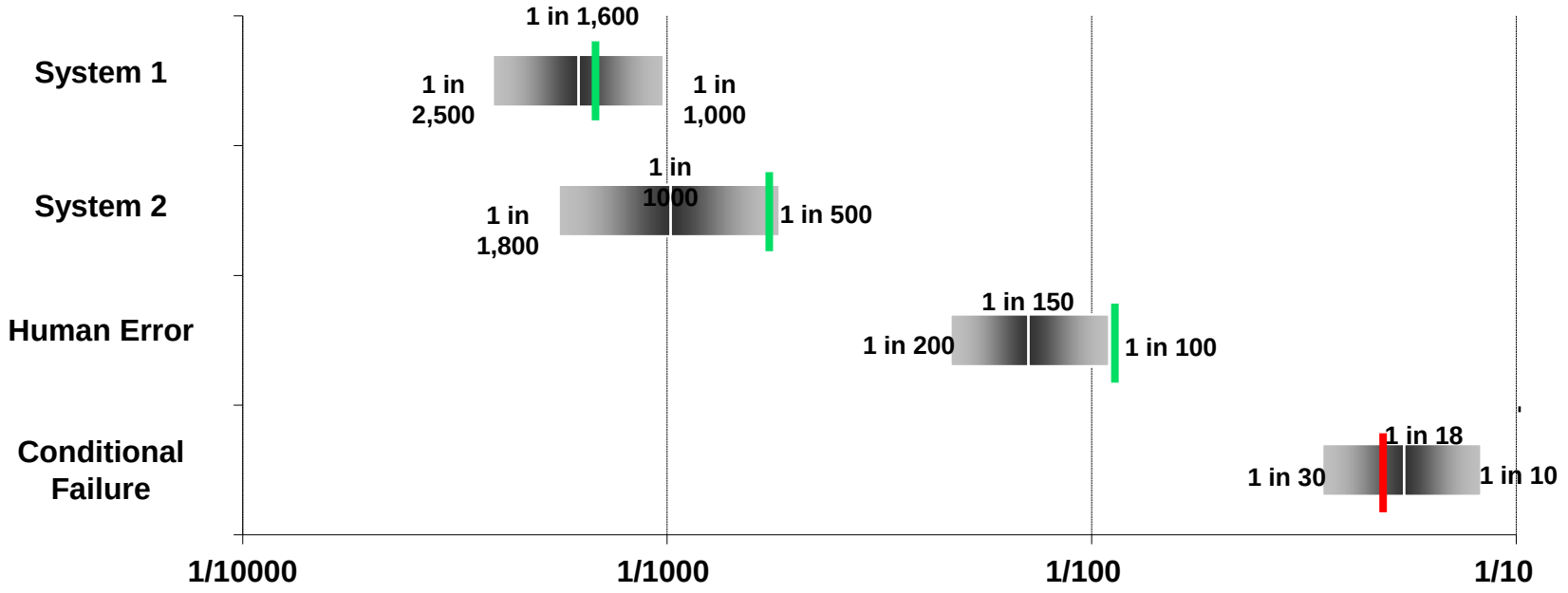
- PRA is a quantitative approach to identifying and analyzing risk in engineered systems and/or processes. It attempts to answers to three basic questions:
  - ✓ What kinds of events or scenarios can occur (i.e., what can go wrong)?
  - ✓ What are the likelihoods and associated uncertainties of the events or scenarios?
  - ✓ What consequences could result from these events or scenarios (e.g., Loss of Crew and Loss of Mission)?
- PRAs are used to model and quantify rare events
- One advantage of PRA is that conventional reliability studies quantify risk but do not take into account human error, external events, and common cause

PRA Development Process



PRA Results with Respect to Requirements (Example)

Notional



Green Bar shows Requirement Value is met
Red Bar shows Requirement Value is not met

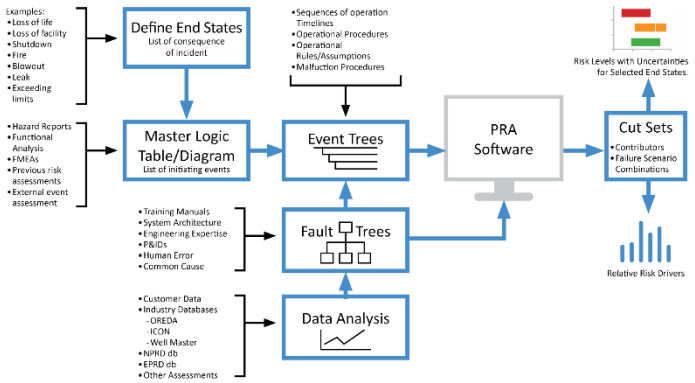
1. Why NASA's experience is relevant to the oil and gas industry.

2. Probabilistic Risk Assessment (PRA) overview.

3. Application of the PRA process to a Dynamic Positioning System (DPS).

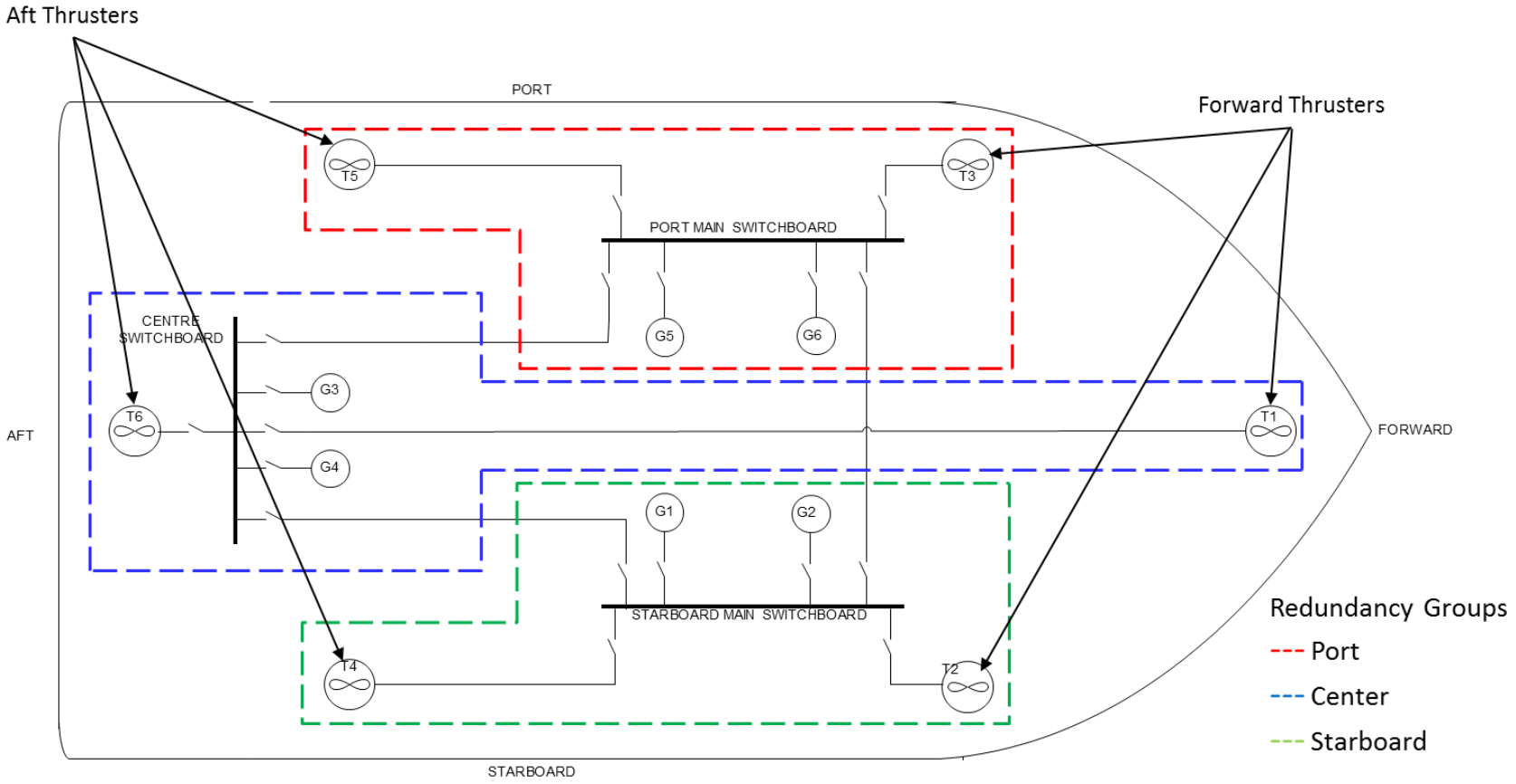
Dynamic Positioning System PRA

- NASA personnel at the Johnson Space Center (JSC) have applied their knowledge and experience with Probabilistic Risk Assessment (PRA) to a number of industries.
- A recent Space Act Agreement signed with members of the oil and gas industry has made NASA's PRA expertise available.
- As a result, NASA was recently commissioned to conduct a PRA to estimate the risk of a Mobile Offshore Drilling Unit (MODU) equipped with a generically configured Dynamic Positioning System (DPS) losing location.
- The DPS modeled in this PRA is generic such that the vessel meets the general requirements of an International Maritime Organization (IMO) Maritime Safety Committee (MSC)/Circ. 645 Class 3 dynamically positioned vessel.



Basic System Architecture

The DPS for the Class 3 MODU is assumed to be equipped with six diesel generators arranged in three redundancy groups which are isolated from one another in separate compartments on the MODU.



Scope and Objectives

Scope

- The DPS PRA is intended to address only failures of the DPS that can result in a loss of location (i. e. probability of loss of location).
- Failures associated with other shipboard equipment or drilling hardware are beyond the scope of this analysis, although human error as it pertains to operation of the DPS is included.

Objectives

- The fundamental objective of this analysis is to determine the probability of the DP vessel losing location during well operations.
- Of equal importance in this analysis is to determine which elements of the DPS are the principal contributors to the overall risk and their relative risk ranking.

Initiating Events and Success Criteria

Initiating Event(s)

The initiating condition or event for these models is a fully functioning DPS. In other words, there is no initiating failure at the outset of the failure sequence that ultimately results in a loss of location by the vessel.

Success Criteria

The analysis does take into consideration the possibility that certain weather conditions will affect the level of DPS failure that the vessel can withstand and still maintain position.

- In a normal weather environment with calm seas, low winds, and mild currents, the vessel requires less power or thruster control. A vessel with a Class 3 certification must be able to withstand and remain operational during Worst Case Failure (WCF) which is defined as the loss of a single redundancy group or one pair of generators or thrusters. Since the DPS must be able to maintain location with the loss of a redundancy group, it was assumed that any system failure occurring after the loss of a redundancy group would be considered failure.
- In an elevated or high weather environment, such as sudden hurricanes, the MODU requires more power and thruster capability to keep station; therefore, loss of a single thruster or generator was assumed to result in a loss of location.

Event Trees

An event tree is an inductive analytical diagramming technique that employs Boolean logic to capture failure events that could result in predetermined outcomes or end states. The end states for this analysis were established by identifying the general failure modes by which the MODU could lose location. The three separate end states were identified: drift-off, drive-off, and push-off.

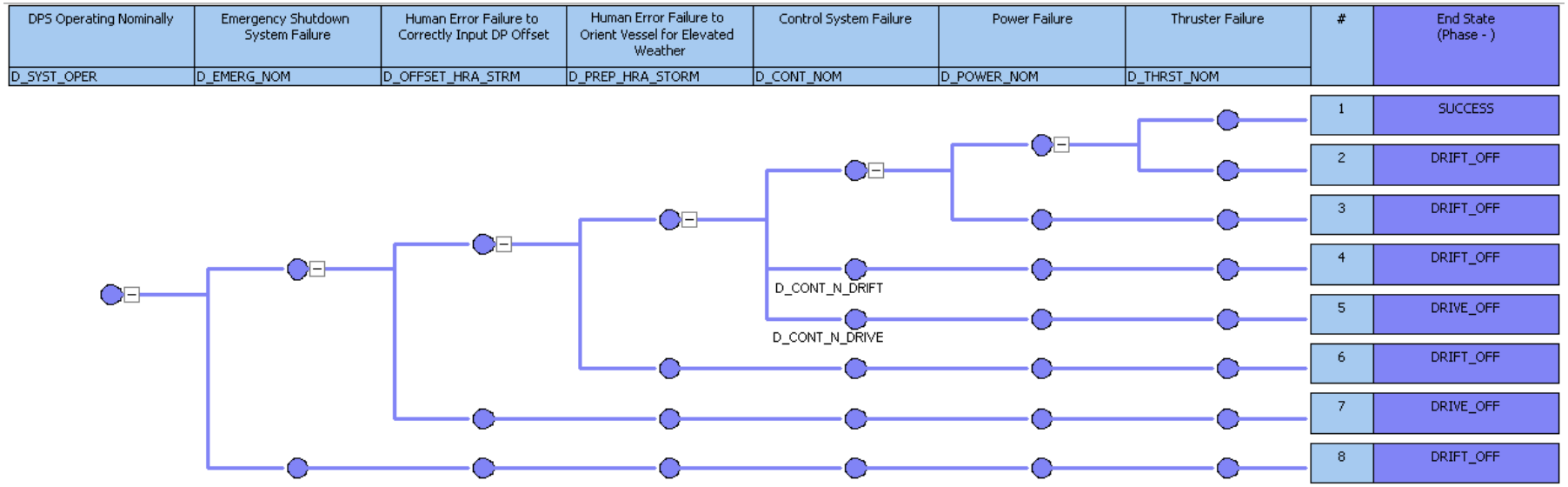
1. Drift-off occurs when one or more failures inhibit the DPS from maintaining vessel location and it drifts beyond the designated radius of operation.

2. Drive-off occurs when the DPS experiences operational degradation to an extent where human intervention is required. During this intervention, human error causes the thrusters to begin moving the MODU off location. As the vessel gains momentum, the risk of potential damage to subsea equipment before re-establishing position becomes unacceptably high resulting in the initiation of an emergency disconnect.

3. Push-off occurs when the weather environment exceeds the position keeping capabilities of a fully operational DPS resulting in the vessel losing location and an emergency disconnect must be initiated.

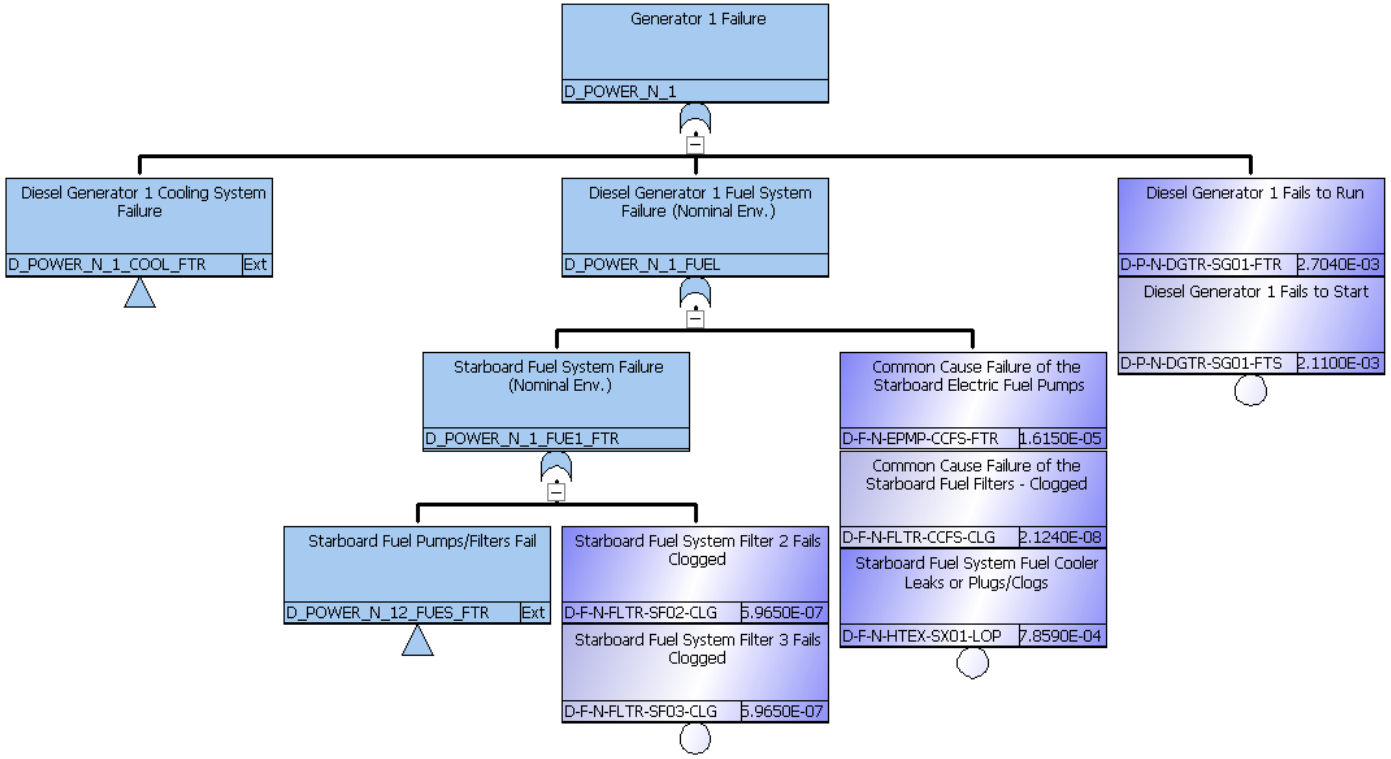
Event Trees (cont'd.)

Normal Weather Environment Event Tree



- Top Events contain both component level failures and human error.
- The two end states for the normal weather environment event tree are drift-off and drive-off.

Fault Trees



- A fault tree is a top down, deductive failure mapping approach in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events.
- For the most part the fault tree captured hardware failures such as loss of power generation capability, or control system failures; however, human error was also incorporated using fault tree logic.

Data Development

Generic Data

- Oil and gas industry specific generic data was used when available, and non-industry specific generic data was used otherwise.
- Most published data was also somewhat dated and may not have represented the most recent conditions or uses for the equipment.

Weather Data

- For this analysis extreme weather frequency was determined from weather data in the Gulf of Mexico.
- The weather frequency estimates along with vessel DP capability plots provided by the system expert were used to establish the extreme weather environment based on wind speed.

Human Reliability Analysis (HRA)

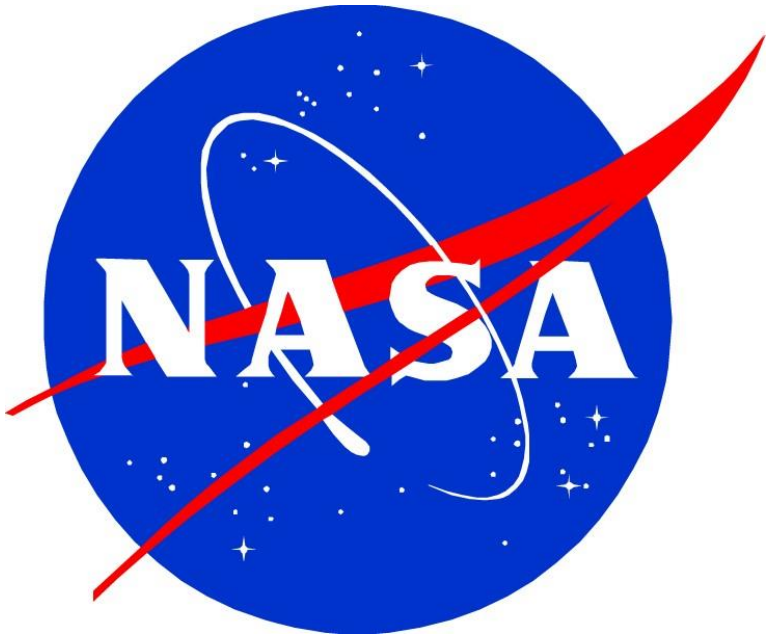
- Human actions can be added to recover or improve the system performance but then the probability of failure to perform these recovery/improvements must be estimated.
- HRA does not view human error as the product of individual weaknesses but rather as the result of circumstantial and situational factors that affect human performance. These factors are commonly referred to as performance shaping factors, which serve to enhance or degrade human performance relative to a reference point or baseline.

Conclusions

- Aggregating the results of the DPS PRA model indicates that the MODU losing location and initiating an emergency disconnect during DP operations would be less than 5% of the time. This assumes no shutdown or refurbishment between wells; however, routine maintenance was taken into consideration in the models.
- Looking into the risk of initiating an emergency disconnect as a function of the operating environment reveals that failures occurring in the normal weather environment are the largest contributors to the overall risk at over 90%, because as approximated by the analysis for the Gulf of Mexico, the vessel spends most of its operation time in the nominal environment.
- Human error is the dominant risk contributor to the overall risk. For this reason, it may be prudent to focus risk reduction efforts on improving human factors, vessel specific training, ergonomics, automation, or decision support tools or technology rather than improve hardware reliability.
- The importance of the generators and thrusters to the DPS cannot be overstated; however, from a risk perspective they are relatively low contributors at less than 10% of the overall risk. The reason for this low occurrence rate is due primarily to the ability of the vessel to operate in a degraded state during nominal operations, the respective levels of redundancy within the generator and thruster subsystems, the independence of the redundancy groups, and the fact that repairs are possible during nominal operations.

Summation

- PRAs are used to model and quantify rare events
- One advantage of PRA is that conventional reliability studies quantify risk but do not take into account human error, external events, and common cause

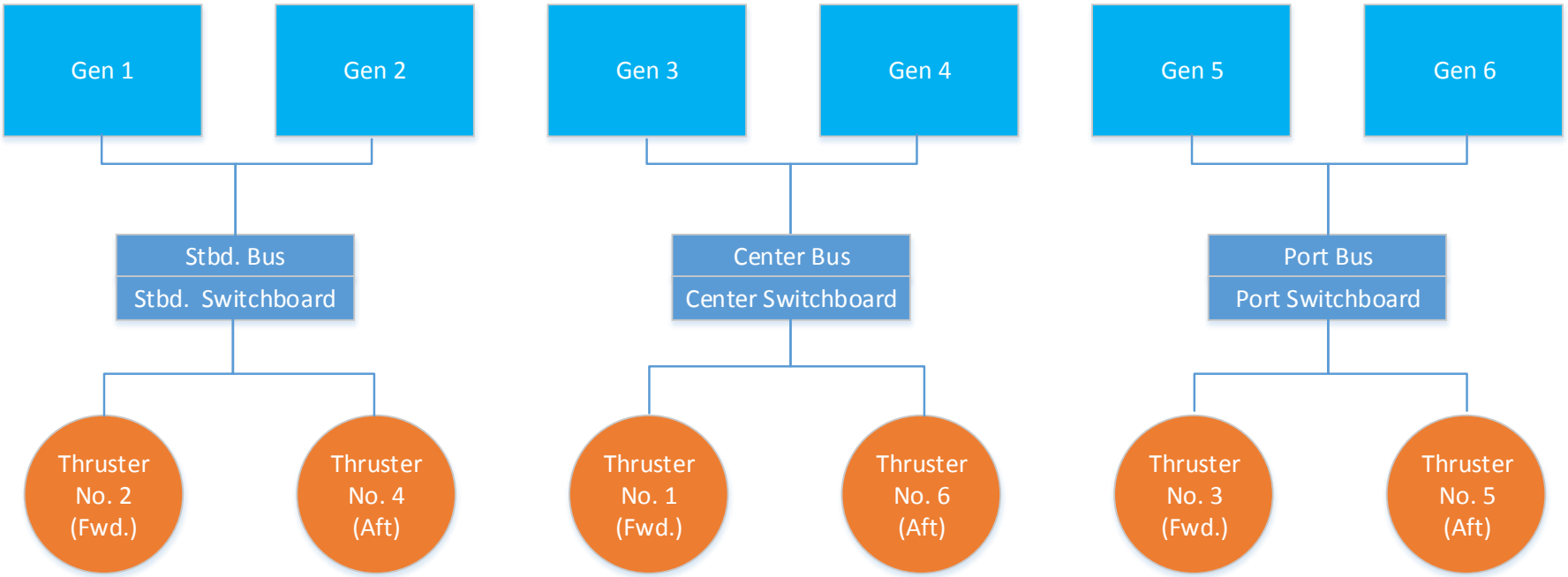


Thank you for your attention!

Back-up Slides

Basic System Architecture (cont'd.)

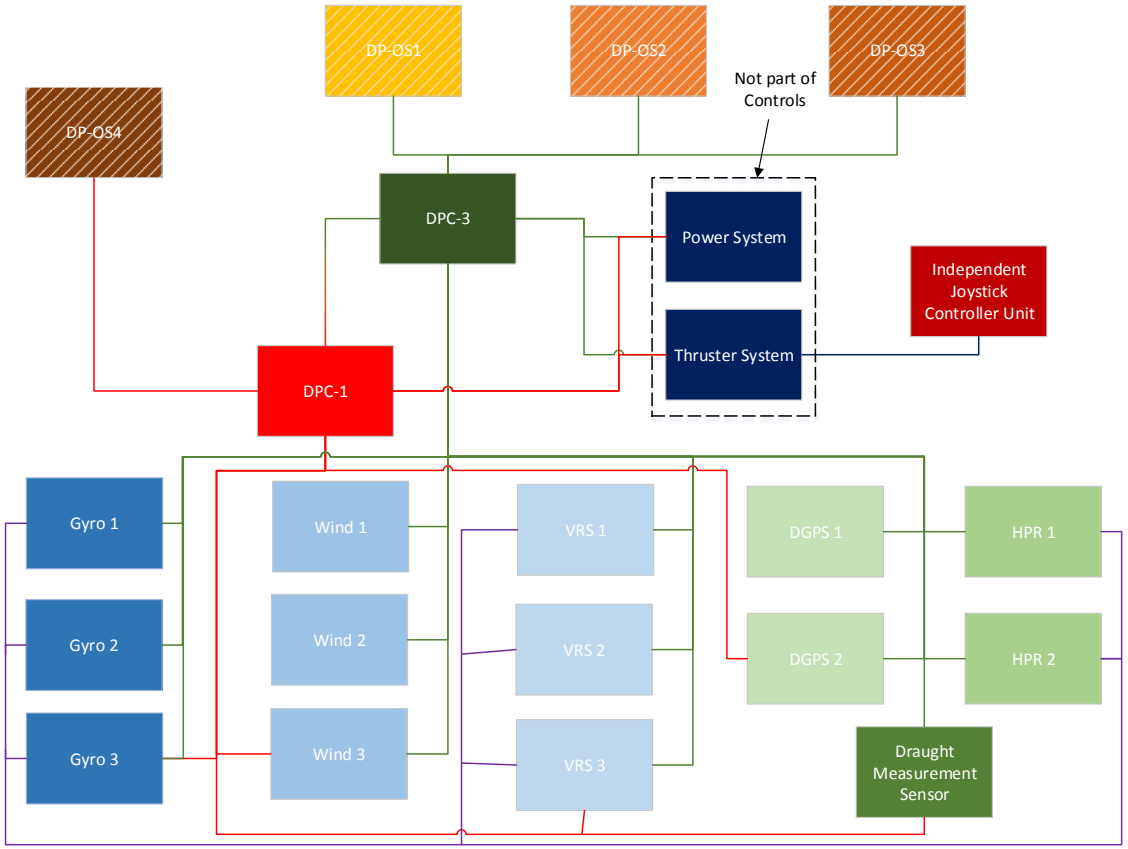
The three redundancy groups, two generators and thrusters per group, provide a level of robustness against single point failures.



Support systems for the diesel generators and thrusters, such as the fuel system and cooling systems are also captured in this PRA although they are not shown here.

Control System Architecture (cont'd.)

The DP control system, as modeled for this analysis, is comprised of a variety of sensors that monitor various aspects of the environment in which the MODU is operating. It incorporates a high level of redundancy and there is also functional overlap to increase the robustness of the design.



Event Tree Analysis

- Event trees are the tools that model the overall mission starting at launch and ending with landing.
- The event trees are timelines of critical events that occur during a mission with branch points that generally represent a successful event or a failure during the event.
  - A failed branch in an event tree is the start of a scenario that may end directly in LOCV for a criticality 1/1 type event, or it may have mitigations associated with it such as ascent aborts or tile repair.
  - Each branch of the event tree is followed in an inductive fashion to its end state, which for Shuttle is a successful landing or LOCV.
- Multiple event trees are used in order to model a complete mission, and the event trees are linked together to get the appropriate potential event sequences.
  - An example of a Shuttle event tree is shown on the following page.
- The results of the event tree analysis is a list of ranked “cutsets” or failure scenarios for the entire mission that can be categorized by phase, element, system, etc.

Fault Tree Analysis

- Fault trees are the tools that model the individual events in the event trees.
  - Typically failure of a system or function.
- The fault trees are developed in a deductive fashion, starting with a top event and developing logic that will result in the top event occurring
- Many systems are used in multiple mission phases, e.g. power, so fault trees must account for partial losses in multiple phases resulting in a total loss of the system or function.
- Recovery actions may be included in the logic of the fault tree, that require both a failure to occur and a failure to recover.
- Fault tree logic is developed downward to a level compatible with existing data.
- Each fault tree produces “cutsets” or failure scenarios for that top event. The fault trees are input into the event trees to develop overall integrated mission level results.

Data Analysis (Types of Data)

- **Functional** – A functional failure event is generally defined as failure of a component type, such as a valve or pump, to perform its intended function. Functional failures are specified by a component type (e.g., motor pump) and by a failure mode for the component type (e.g., fails to start). Functional failures are generally defined at the major component level such as Line Replaceable Unit (LRU) or Shop Replaceable Unit (SRU). Functional failures typically fall into two categories, time-based and demand-based. Bayesian update as Shuttle specific data becomes available.

- **Phenomenological** – Phenomenological events include non-functional events that are not solely based on equipment performance but on complex interactions between systems and their environment or other external factors or events. Phenomenological events can cover a broad range of failure scenarios, including leaks of flammable/explosive fluids, engine burn through, over-pressurization, ascent debris, structural failure, and other similar situations.

- **Human** – Three types of human errors are generally included in fault trees: pre-initiating event, initiating event (or human-induced initiators), and post-initiating event interactions.

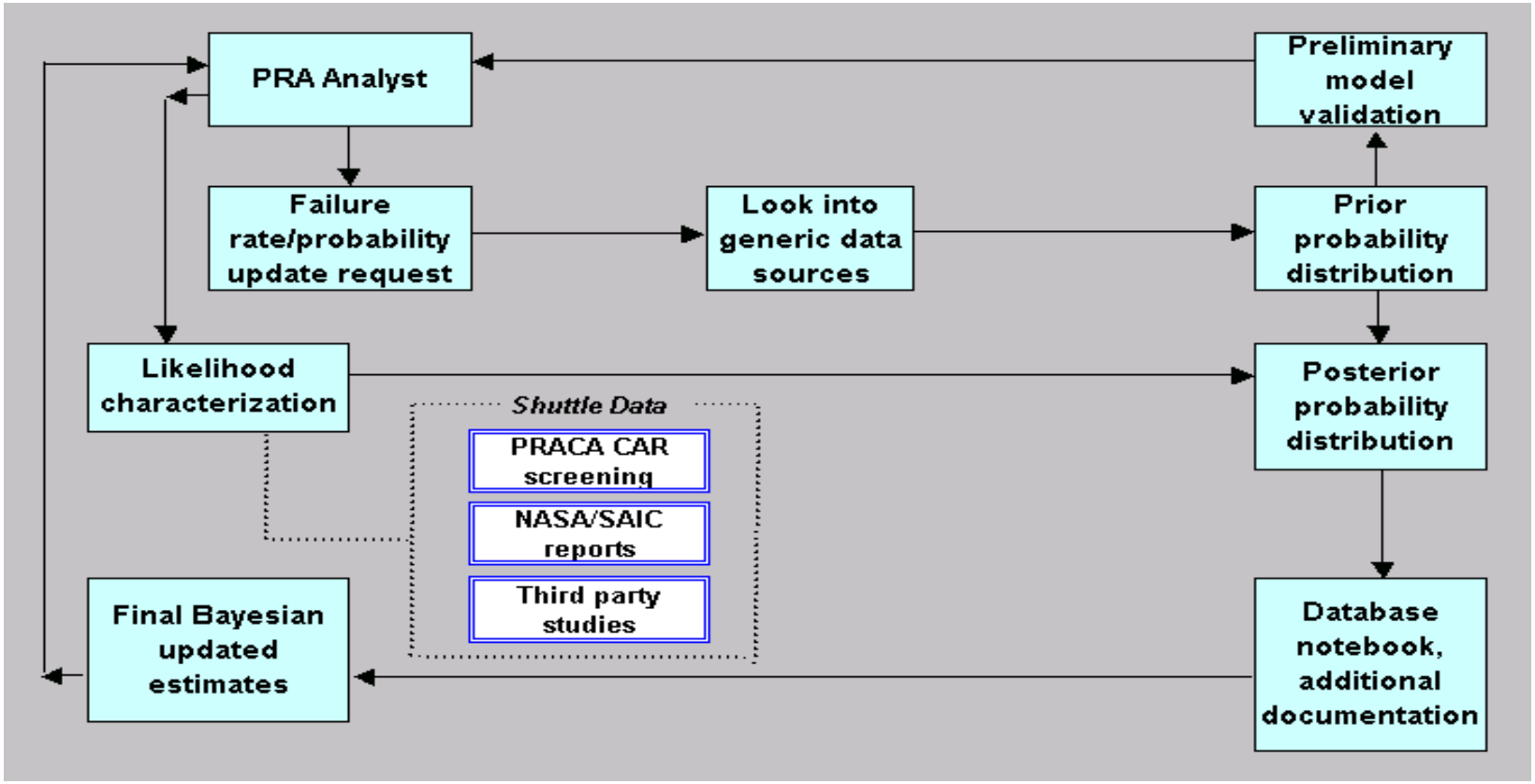
- **Common Cause** – Common Cause Failures (CCFs) are multiple failures of similar components within a system that occur within a specified period of time due to a shared cause.

- **Conditional** – A probability that is conditional upon another event, i.e. given that an event has already happened what is the probability that successive events will fail

Data Analysis (Functional Data Sources)

- NASA's PRACA databases are sources for Shuttle specific failure data
- Prime contractor data, when available
- Non-electric Part Reliability Database (NPRD) is a generic data source for run time failure data for mechanical components
- Electric Parts Reliability Data (EPRD) is a generic data source for run time failure data for electrical components
- Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) is a generic data source for on demand failures
- Expert Opinion
- Miscellaneous references

Data Analysis (Functional Data Development)



Data Analysis (Bayesian Updating of Functional Data)

- What?
  - It is a recognized, and standard, practice for functional failures
  - Utilizes generic databases
  - Applies a statistical technique to allow System specific data to update the generic values
- Why?
  - Provides a tool to utilize sparse data from the specific System to generate more accurate estimates of failure rates
  - Provides a less conservative way to estimate failure rates for components with zero failures
- Inputs
  - Total hours of operation or number of demands for a component
  - Number of failures experienced (derived from CAR screening and input from Engineers)

Data Analysis (Human Reliability Analysis (HRA))

- HRA is a method used to describe, qualitatively and quantitatively, the occurrence of human failures in the operation of complex machines that affect availability and reliability.
- Modeling human actions with their corresponding failure in a PRA provides a more complete picture of the risk and risk contributions.
- A high quality HRA can provide valuable information on potential areas for improvement, including training, procedural and equipment design.
- Screening analysis is performed on the bulk of the human errors with a detailed analysis only performed on the significant contributors
- There are Many Different Methodologies for Model Human Errors in PRA
  - For the Shuttle PRA Cognitive Reliability and Error Analysis Method (CREAM) was selected as the primary method for detailed analysis
    - It was selected as one of the NASA recommended HRA techniques
  - The results from CREAM have been favorably benchmarked against other methodologies and simulator data as part of the Shuttle PRA
  - The majority of HRA events are processed with a screening analysis that is essentially based on the Technique for Human Error Reliability Prediction (THERP) in NUREG/CR-1278. THERP is a recognized HRA technique that has been used for over 20 years, primarily in calculating Human Error Probability (HEP) in nuclear power plant PRAs.
    - The screening table was easy to apply and gave conservative values. If an HRA event that was developed using the screening table became a significant contributor it was then re-modeled using CREAM