Towards a methodology and tooling for Model-Based Probabilistic Risk Assessment (PRA)

Sam Schreiner, Matt Rozek, Andy Kurum, Chet Everline, Mitch Ingham, Jeffery Nunes

Jet Propulsion Laboratory, California Institute of Technology

Jet Propulsion Laboratory
California Institute of Technology

Introduction/Motivation

- PRA definition (from the PRA Procedures Guide for NASA)
  - *Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis method aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance.*

- Traditionally done manually
  - Large amount of knowledge captured in isolated data model that does not conform to a standard format
  - Gathering data about the casual information through layers of system complexity relies upon verbal communication between PRA engineer and SMEs

- High Cost
  - 50% to 90% of PRA costs relate to developing the PRA model (JPL's PRA planning guidelines)

Model-Based PRA

- Causal information is rigorously encoded in a central system model according to the Fault Management Ontology
  - Knowledge from domain experts is encoded in an unambiguous manner at a very focused level
  - Causal info can be used for other analyses (FTA, FMECA, etc.) to avoid duplication of effort

- Methodology uses the causal information in the model to conduct a PRA
  - Ability to modify the PRA in concert with project lifecycle evolution
  - Can track the extent to which system modification impacts requirements compliance

Risk Triplets

- A PRA produces a set of Risk Triplets, each of which contains:
  1. **Consequence**
     - The requirement or set of requirements whose risk is being assessed by the PRA. Additional information is provided for the performing element, the function it performs (which is being specified by the requirement(s)), and the **Performance Constraints** on that function.
  2. **Risk Scenario**
     - A scenario (captured in a **Minimal Cut Set**) that causes the **Consequence** to occur. Additional information is provided via **Violation Explanations** that connect the behavior in a **Risk Scenario** to the violated **Performance Constraints**.
  3. **Probability of Occurrence**
     - A quantitative estimate of the probability of the given **Risk Scenario** occurring. *(Not implemented in this version of the model-based PRA methodology)*

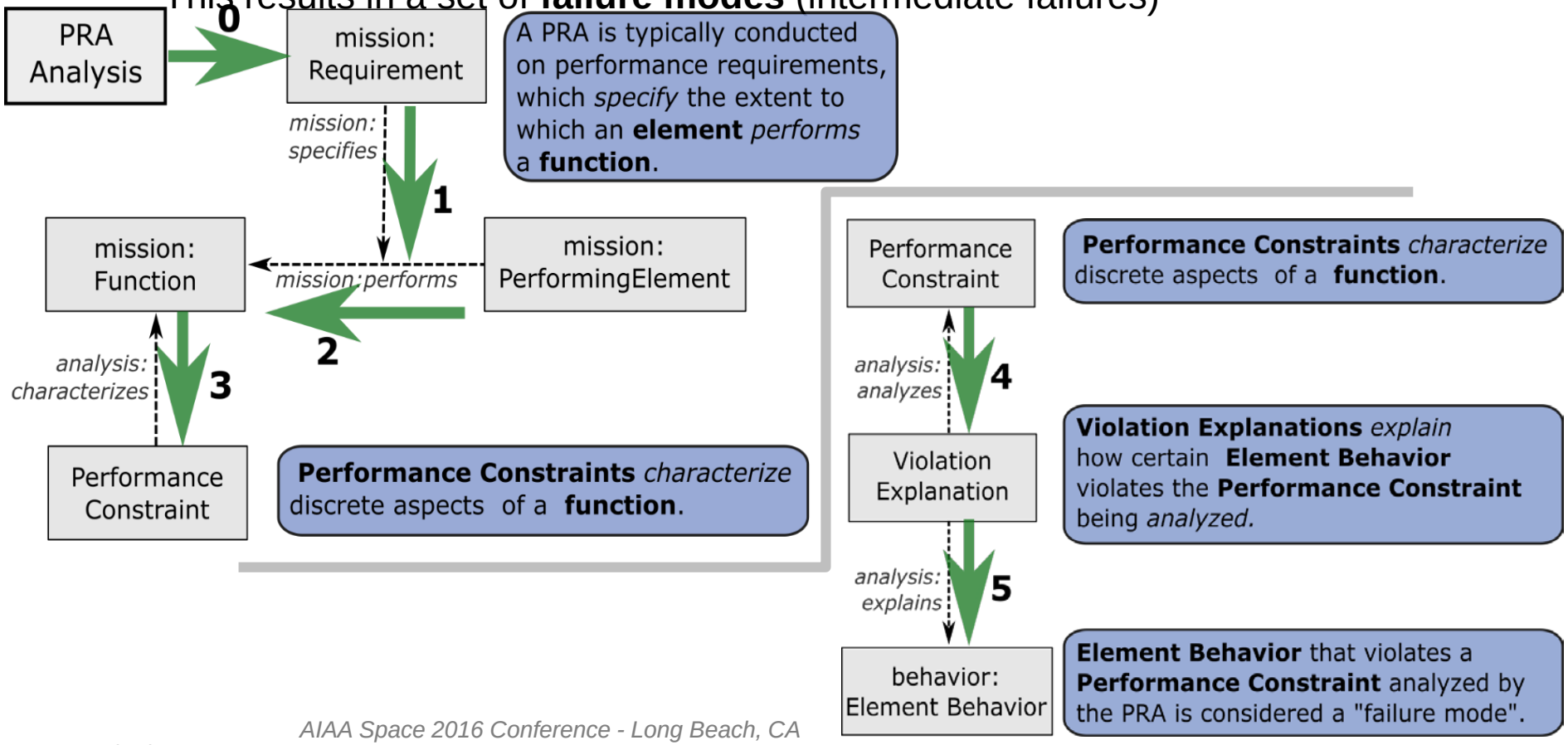
Part 1 – Elaborating Upon the Consequence

Determine which system behaviors are threats to the given requirement

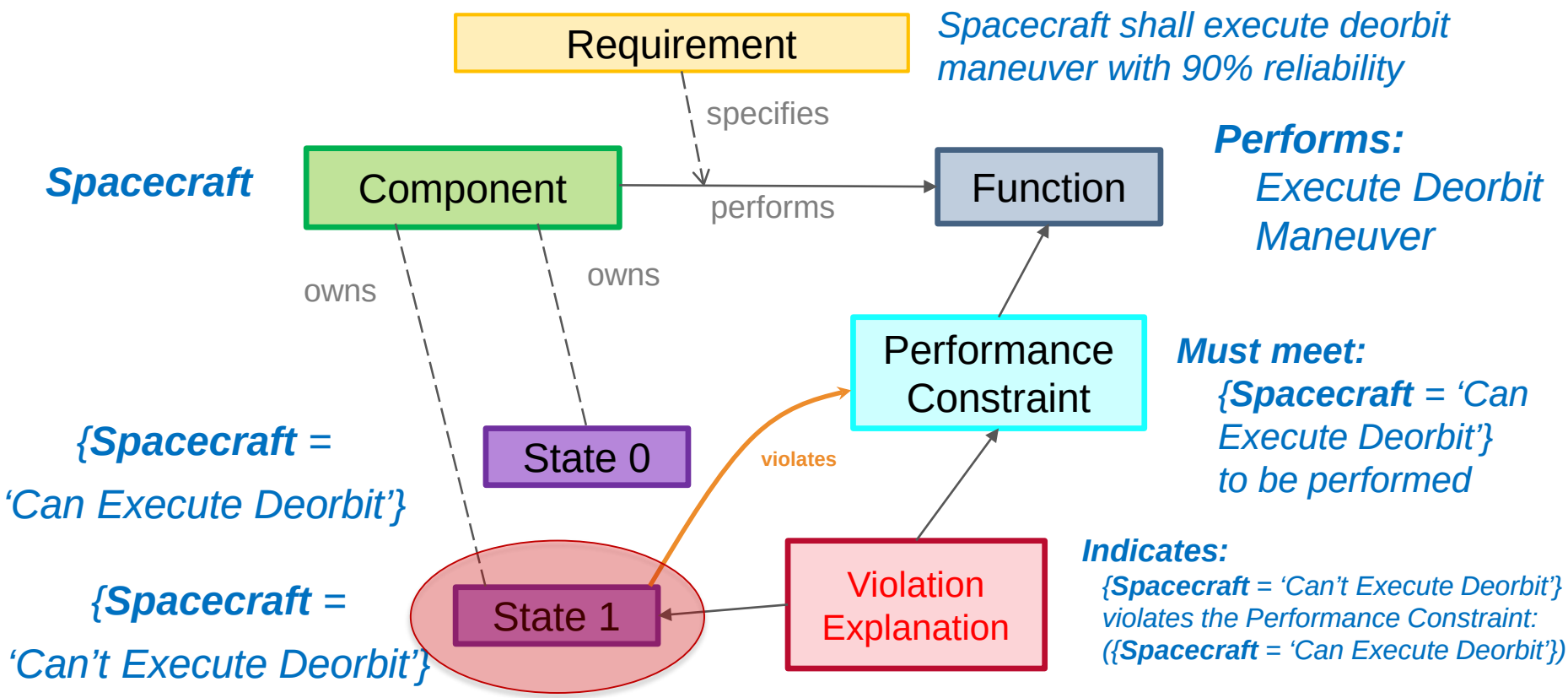
Use a 'Performance Constraint' metric:

Clearly stated boundary defining whether or not a function (specified by the requirement) is performed

This results in a set of **failure modes** (intermediate failures)



1) Tracing Requirement to Intermediate Failures



What the diagram means:

"**{Spacecraft = 'Can't Execute Deorbit'}** results in **{Spacecraft}** not being able to perform **{Execute Deorbit Maneuver}** function"

More Generally:

"***{State 1}*** *results in* ***{Component}*** *not being able to perform* ***{Function}***"

Part 2 - Tracing through Causal Linkages to Generate Risk Scenarios

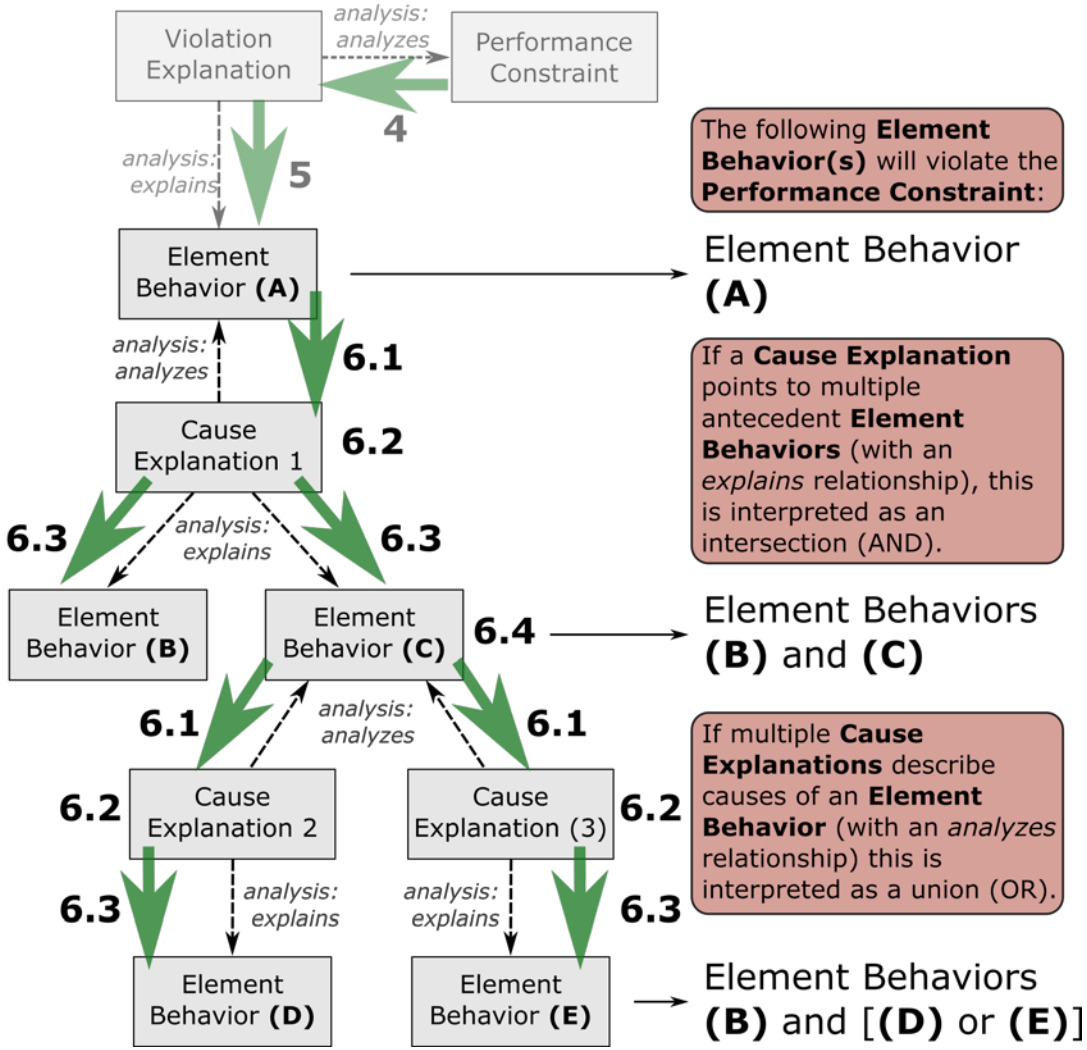
Violation Explanations *explain* how certain **Element Behavior** violates the **Performance Constraint** being *analyzed.*

Element Behavior that violates a **Performance Constraint** is considered a "failure mode".

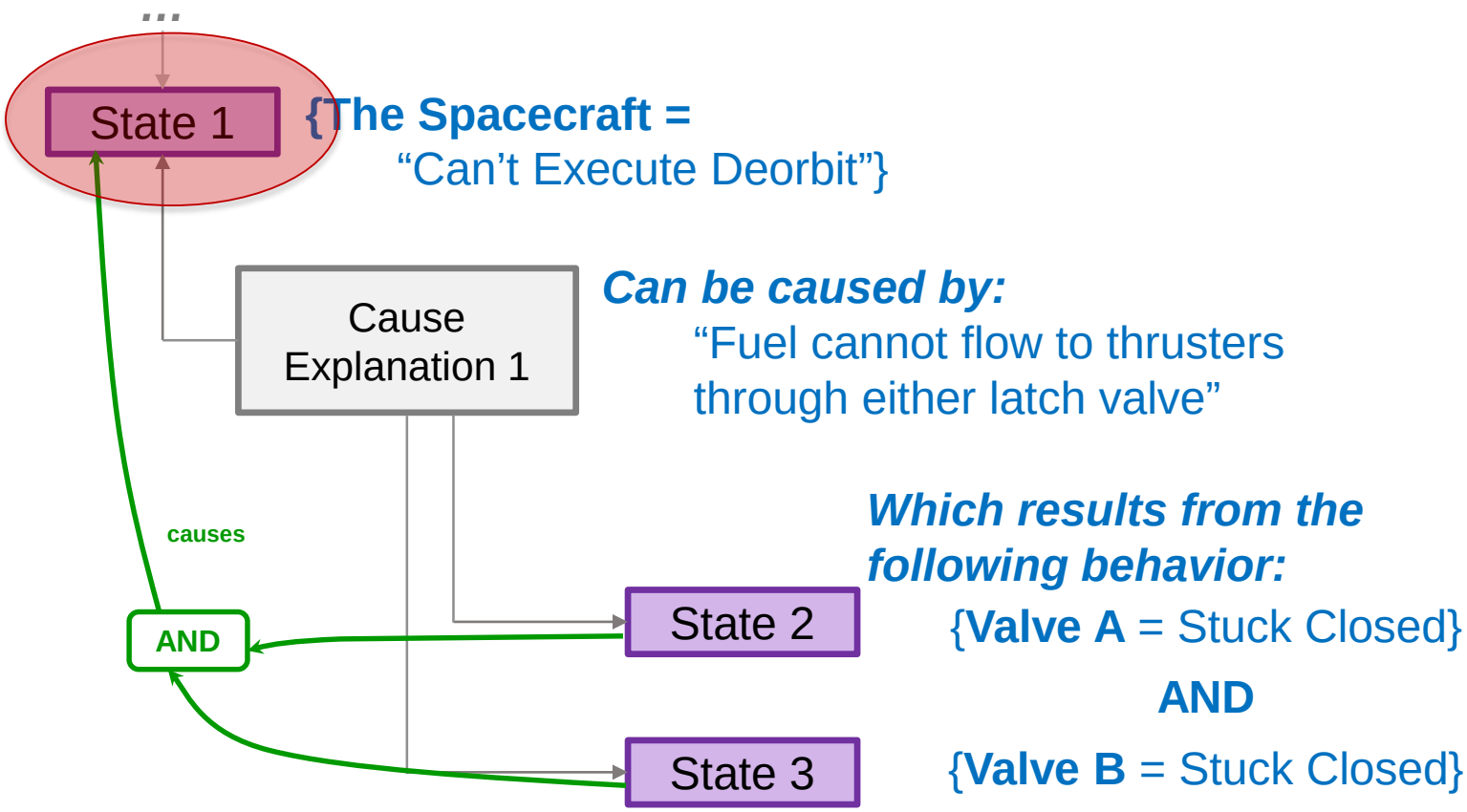
Cause Explanations *analyze* **Element Behavior(s)** and *explain* why other **Element Behavior(s)** may cause it.

Element Behavior that is not *analyzed* by a **Cause Explanation** has no identified causes, which classifies it as "basic behavior" (i.e. Element Behavior B).

The PRA methodology recursively traverses through **Cause Explanations** to locate basic **Element Behaviors**. The occurence of a basic behavior is considered a basic event.



2) Traversing Causal Linkages (recursive)



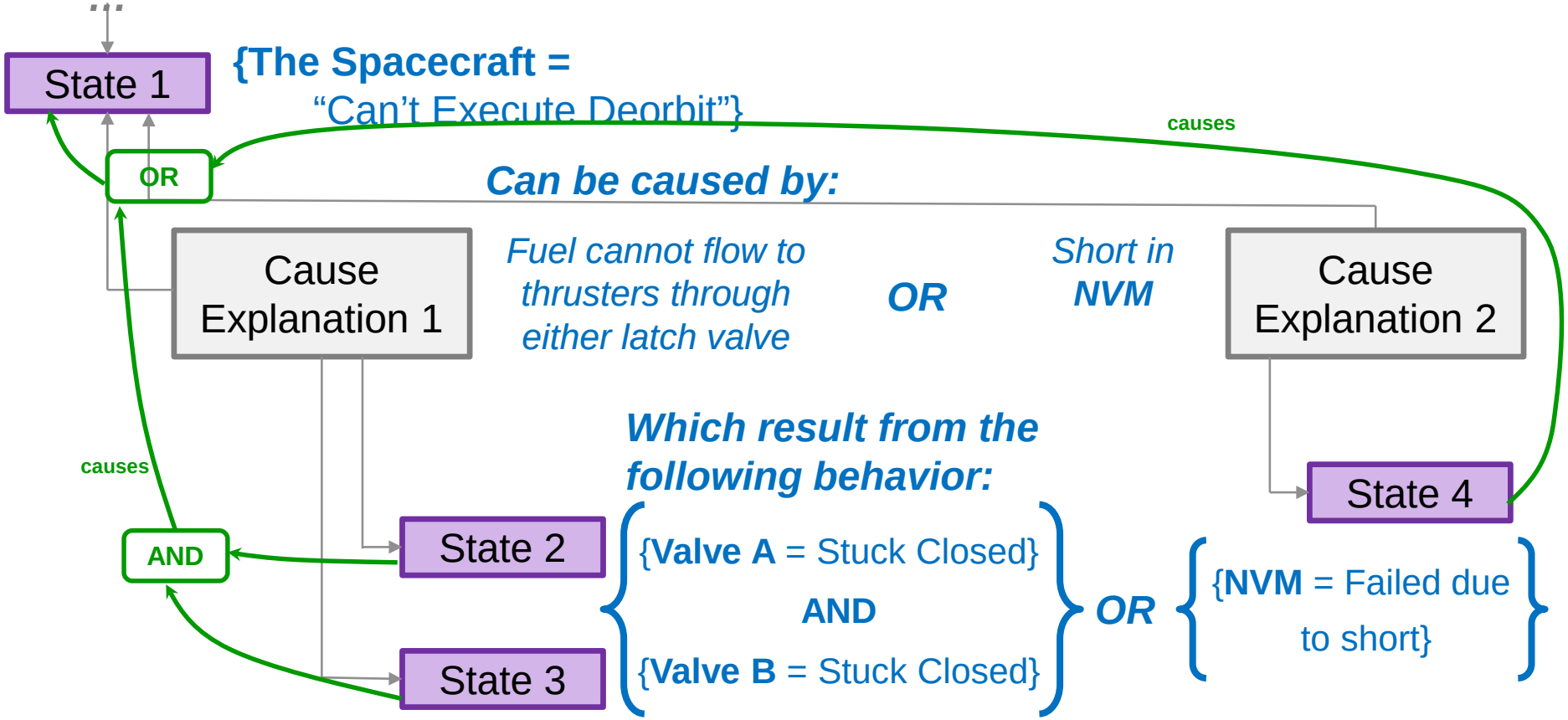
What the diagram means:

"**{Valve A = Stuck Closed}** and **{Valve B = Stuck Closed}** will result in:
{Spacecraft = Can't Execute De-orbit Maneuver}"

More Generally:

*"**{State 2}** and **{State 3}** will result in the system being in **{State 1}**"*

2) Traversing Causal Linkages (recursive)



What the diagram means:

"({**A = Stuck Closed**} and {**B = Stuck Closed**}) or ({**NVM = Failed due to short**}) will result in: {**Spacecraft = Can't Execute De-orbit Maneuver**}"

More Generally:

*"({**State 2**} and {**State 3**}) or {**State 4**} will result in the system being in {**State 1**}"*

Results

Risk Scenarios produced by model-based PRA

For the set of requirements: **{Requirement EOM Maneuver Reliability}**
Which specify the performs relationships for following Performing Elements: **{mission:Component Project System}**
The following Risk Scenarios were identified
...|--> [PerformanceConstraint] [OperatingMode = CAN_DEORBIT]
.....|--> [ViolationExplanation] Project Fails to Conduct Deorbit Maneuver
.....|--> [StateMachineElement] {Project System=Unable to Deorbit Spacecraft}

For "{Project System=Unable to Deorbit Spacecraft}", the basic events are:

433 **Fuel cannot flow to thrusters through either latch valve**
({Latch Valve A=STUCK_CLOSED} AND {Latch Valve B=Stuck Closed})

7 **Flight Computer fails (catastrophically) to perform its function**
{Flight Computer=Unable to perform computation (non-recoverable)}

8 **Flight Computer fails (spuriously) to perform its function and there is the inability to reboot Flight Computer using image stored in NVM (excluding NVM electrical shorts)**
({Flight Computer=Unable to perform computation (recoverable)} AND {NVM=Memory Inaccesible})

9 **NVM fails (electrical short) to perform its function**
{NVM=Memory Inaccesible}

1 **SRU fails to communicate star information**
{SRU=Unable to provide stellar reference locations}

373 **IMU-A fails and Fault Protection fails to swap to IMU-B**
({IMU A=Unable to take intertial measurements} AND {Fault Protection System=(Transition) from IMU-A Operational to IMU-A Operational})

374 **IMU A fails to perform its function, Fault Protection swaps to IMU B, and IMU B fails to perform its function**
({IMU A=Unable to take intertial measurements} AND {IMU B=Unable to take intertial measurements} AND {Fault Protection System=(Transition) from IMU-B Operational to IMU-A Operational})

15 **Normally active heaters 1A and 1B fail**
({Battery Heater 1A=Unable to generate heat} AND {Battery Heater 1B=Unable to generate heat})

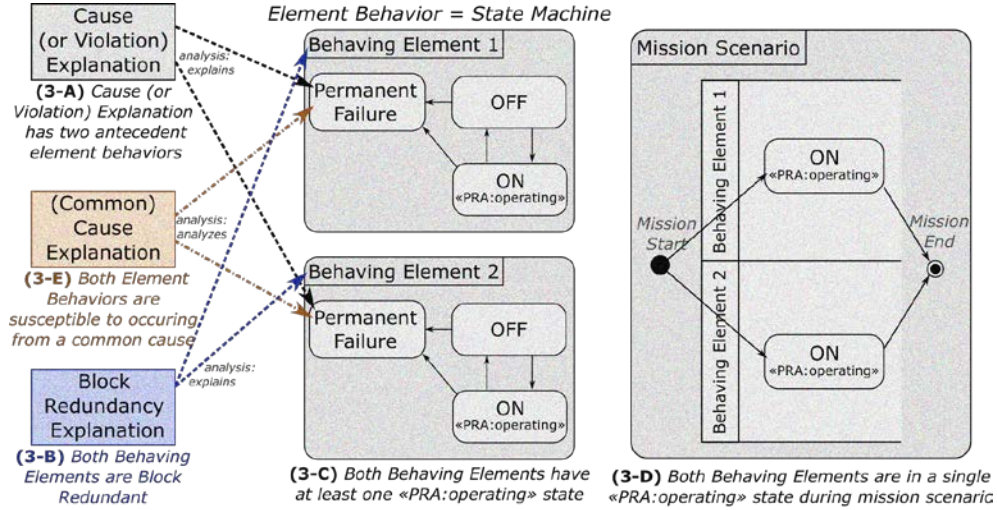
17 **Normally active thermostats 1A and 1B fail**
({Thermostat 1A=Unable to measure temperature} AND {Thermostat 1B=Unable to measure temperature}

18 **Normally active thermostats 1A and 1B fail due to a common cause**
({Thermostat 1A=Unable to measure temperature} AND {Thermostat 1B=Unable to measure temperature}) occur due to a common cause

Part 3 – Quantifying the Likelihood

(3a) For each *risk scenario* (generated from Part 2), determine the appropriate probabilistic equation that characterizes it

Leverage info in the model concerning redundancy, behavior, and operational scenarios:



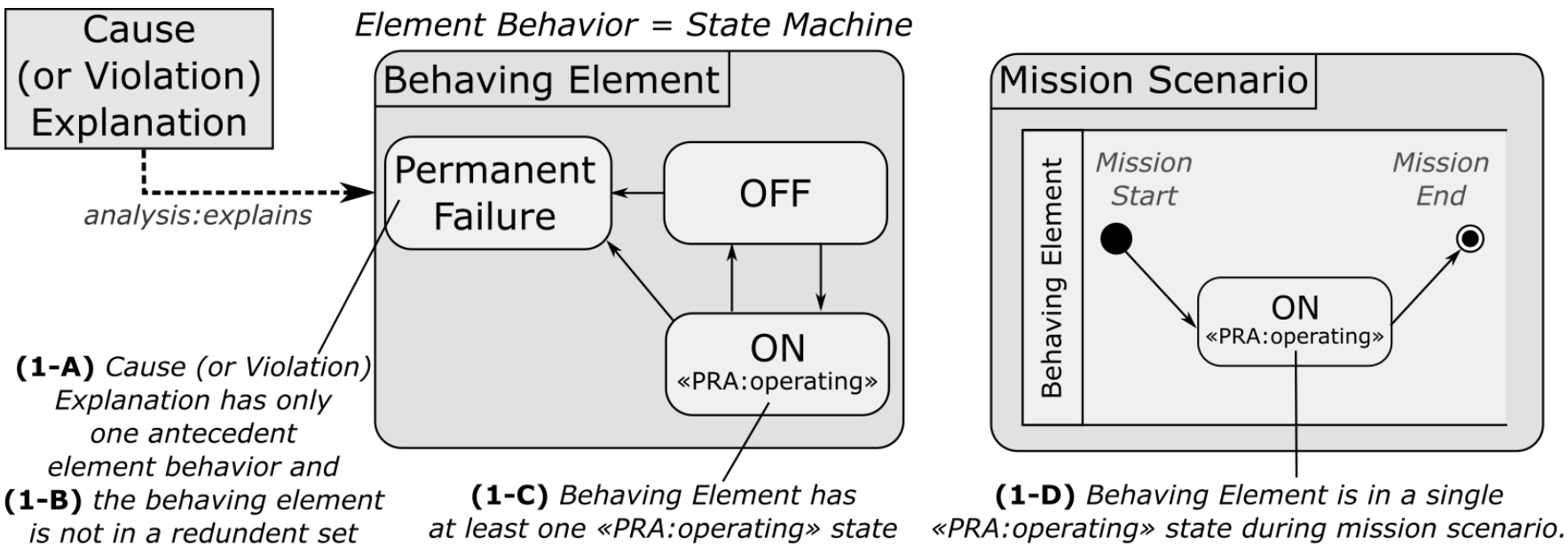
(3b) **[Not yet developed]** *Determine the appropriate values for parameters in the equation and carry out quantitative calculation*

Identifying Equation 1

Single String, Continuous Operation

$$R(t) = e^{-\lambda t}$$

- Describes a single component that has no redundant backups ("single string") and is continuously operational during the mission.

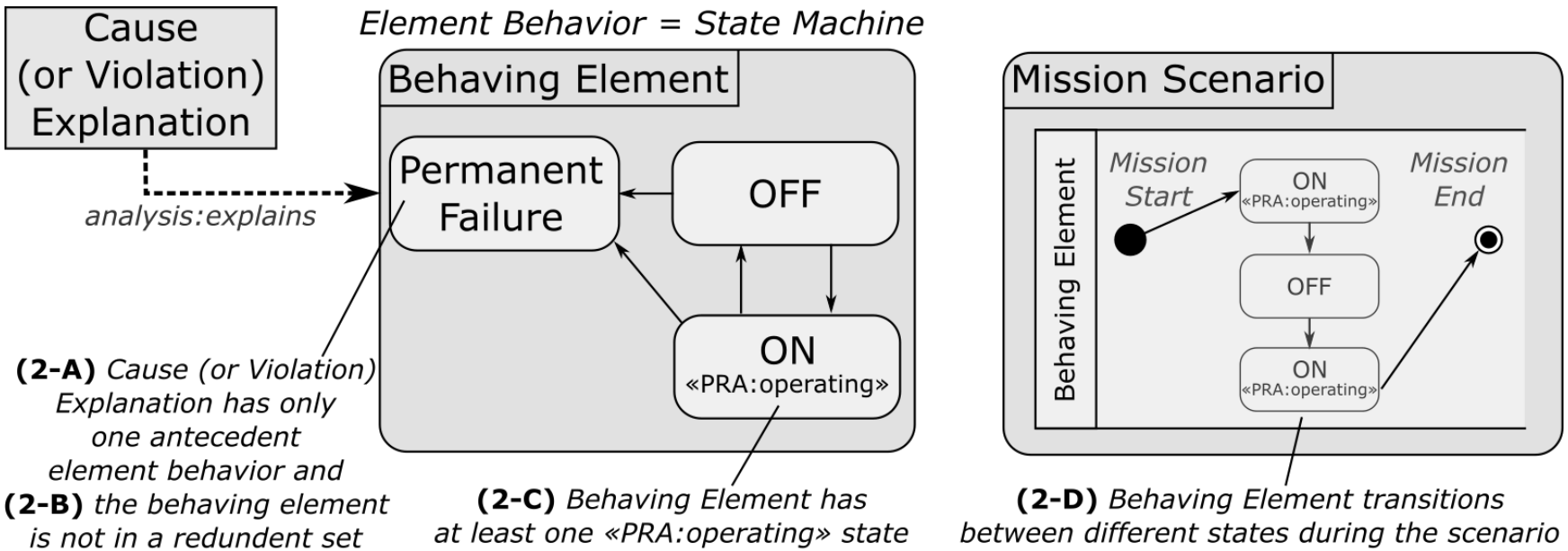


Identifying Equation 2

Single-String, Cyclic Operation

$$R(t) = (1-p)^M (1-q)^N \, exp\left(-\lambda \sum_{n=1}^{N} t_n\right)$$

- Describes a single component that has no redundant backups (a.k.a “single string”) and operates cyclically over the mission.

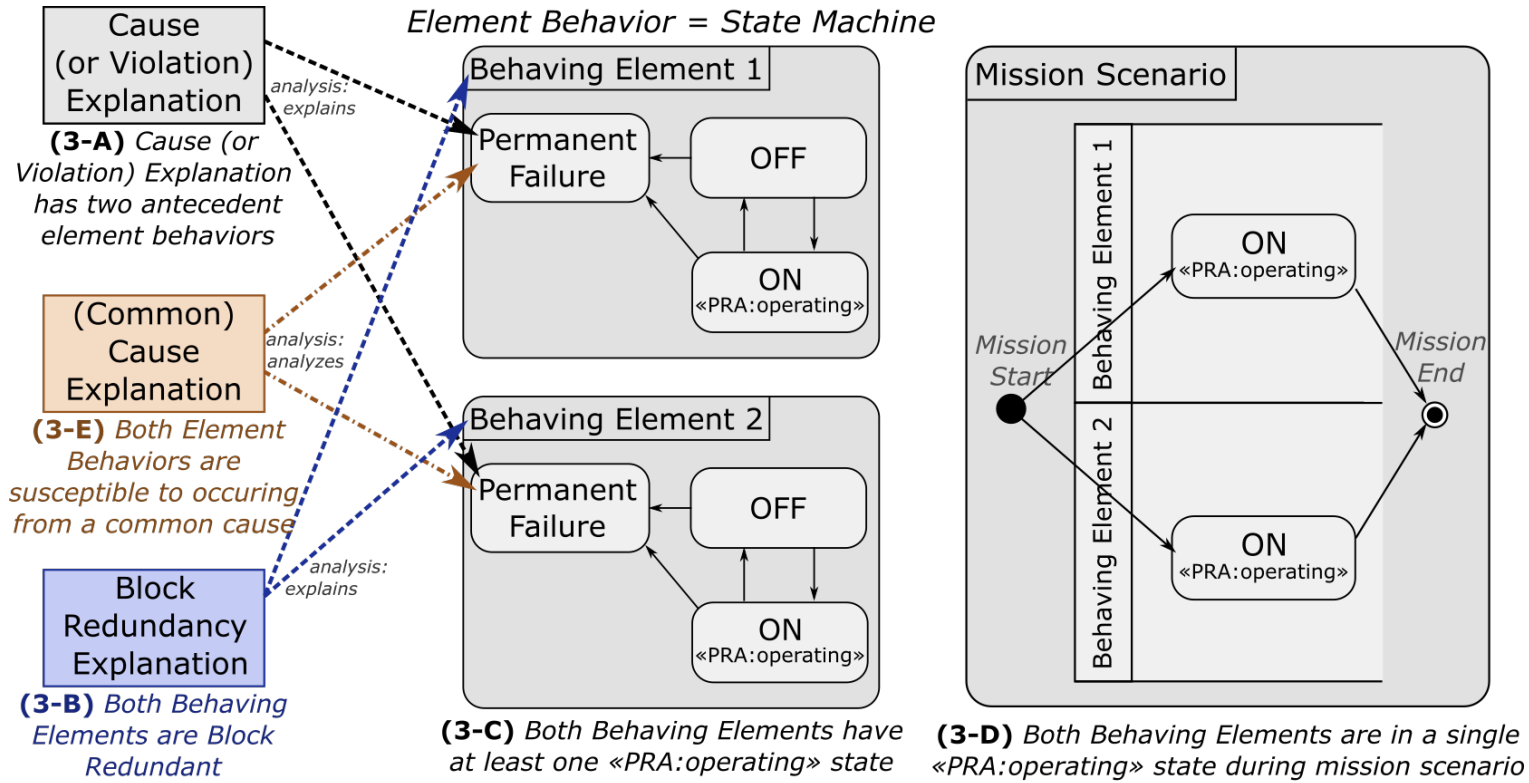


Identifying Equation 3

Redundant, Continuous Operation ("Hot Spare"), Common Cause Failure

$$R(t) = 2\,e^{-(\lambda_I+\lambda_C)t} - e^{-(2\lambda_I+\lambda_C)t}$$

- Describes a grouping of two components that are block redundant, operate continuously over the mission, and can potentially fail due to a common cause failure.

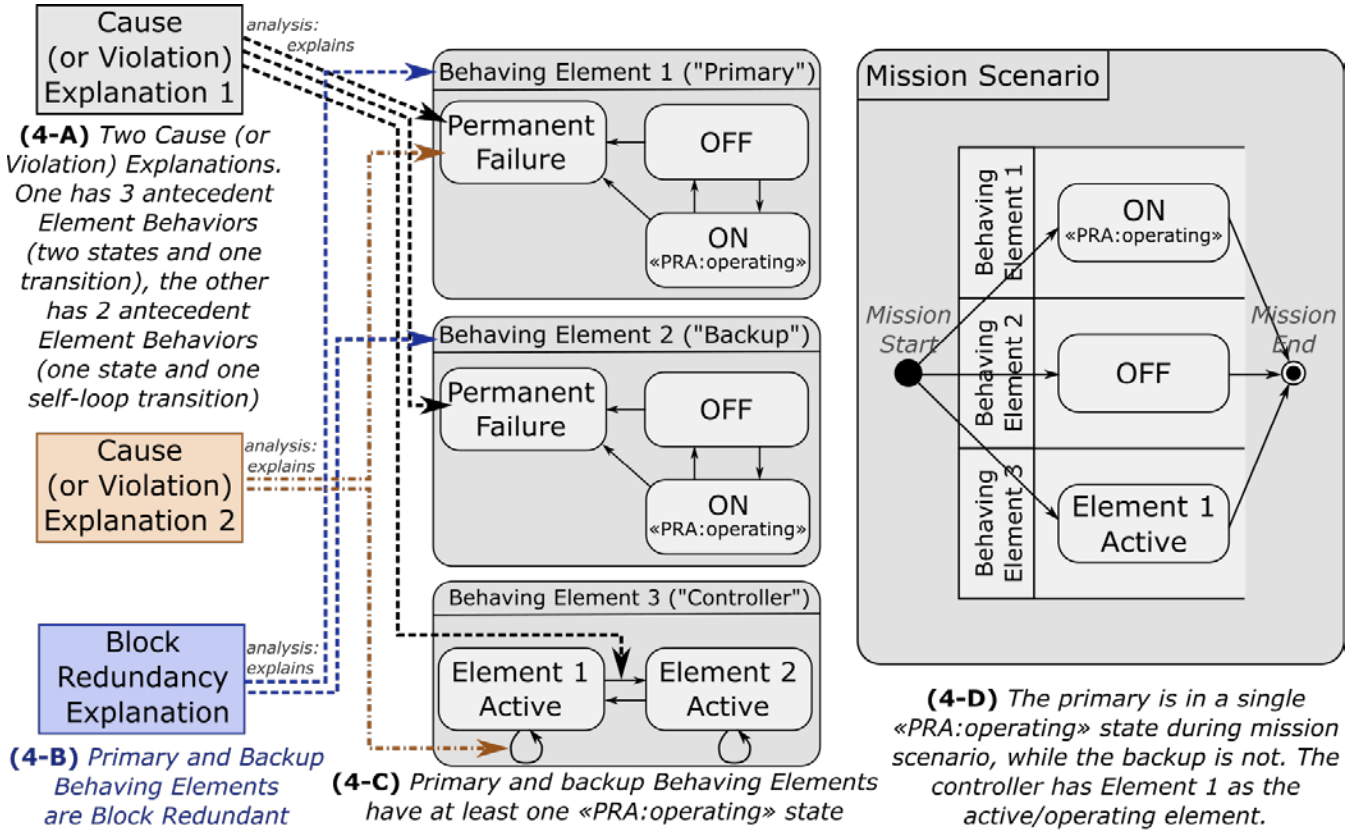


Identifying Equation 4

Redundant, Single Component Operational ("Cold Spare")

$$R(t) = e^{-\lambda t}(1 + (1 - p)\lambda t)$$

- Two block redundant components: "primary" operates continuously while the "backup" is a "cold spare". The third component, the "controller", transfers operation to the backup after the failure of the primary.



(4-A) *Two Cause (or Violation) Explanations. One has 3 antecedent Element Behaviors (two states and one transition), the other has 2 antecedent Element Behaviors (one state and one self-loop transition)*

(4-B) *Primary and Backup Behaving Elements are Block Redundant*

(4-C) *Primary and backup Behaving Elements have at least one «PRA:operating» state*

(4-D) *The primary is in a single «PRA:operating» state during mission scenario, while the backup is not. The controller has Element 1 as the active/operating element.*

Conclusions

- Developed a new methodology for conducting a Model-based PRA
  - Leverages causal information in the model to trace from a given **Consequence** (Requirements) through layers of system complexity, to create **Risk Scenarios**
- Provides an avenue for tackling increasing system complexity
  - Causal links have a focused scope (**easy to add to model**), but when aggregated, they give the algorithm enormous reasoning ability
- Potential to reduce cost of PRA by **automating** some of the process
  - **50% to 90%** of PRA costs relate to developing the PRA model (JPL's PRA planning guidelines)
- Enhances ability of SE team to consider risk during design process
  - Puts the PRA tool in the hands of the SE team to run **sensitivity analyses** and **study the risk-impact** of different architecture/design choices
- By utilizing information that conforms to standard data structures, this methodology can ensure consistency with other analyses
  - Violation and Causal information can also be leveraged for **FTAs, FMECAs**, etc.
  - Same fundamental behavior/scenario models can be used for the PRA as well as for other analyses (i.e., **power profile analysis** or **science data collection modeling**).

Future Work

- Calculating Probability of Occurrence
  - Critical 3rd element of Risk Triplet
  - What is the appropriate role of a human user in selecting appropriate values for probabilistic equations?

- Allow engineers to conduct sensitivity analyses and visualize results in standard formats

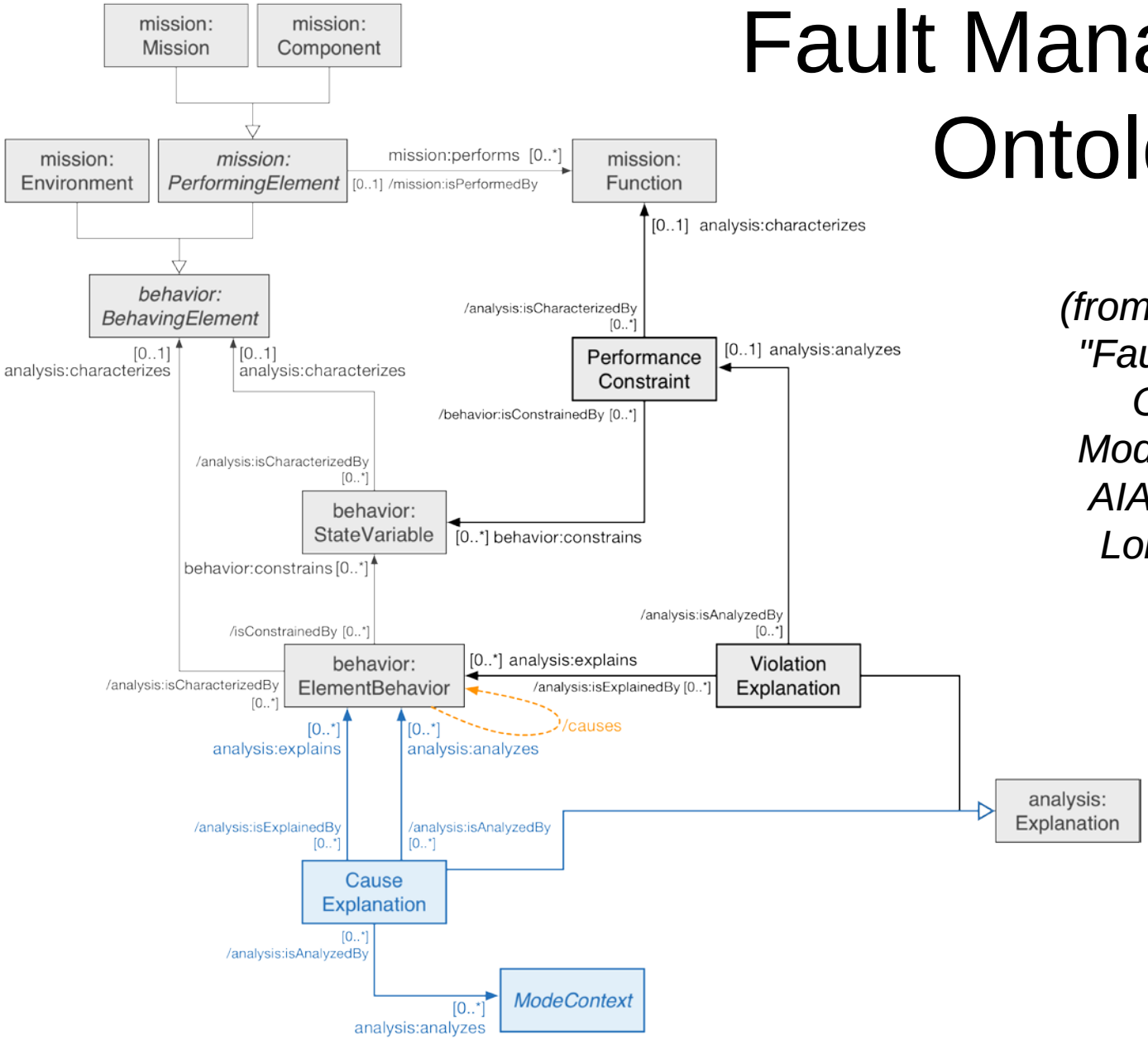
- Additional types of element behavior?
  - Current methodology only works on State Machine Elements (States or Transitions)

Backup Slides

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov

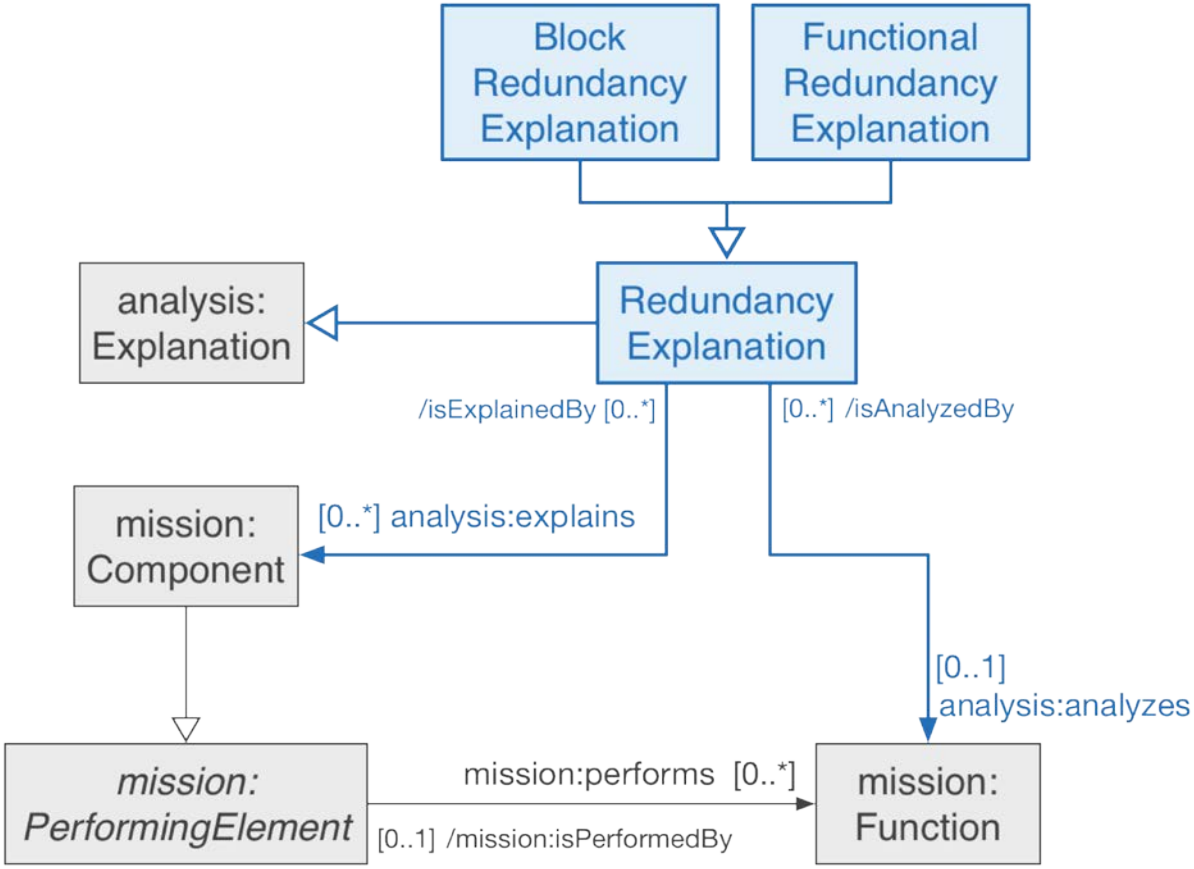
Fault Management Ontology



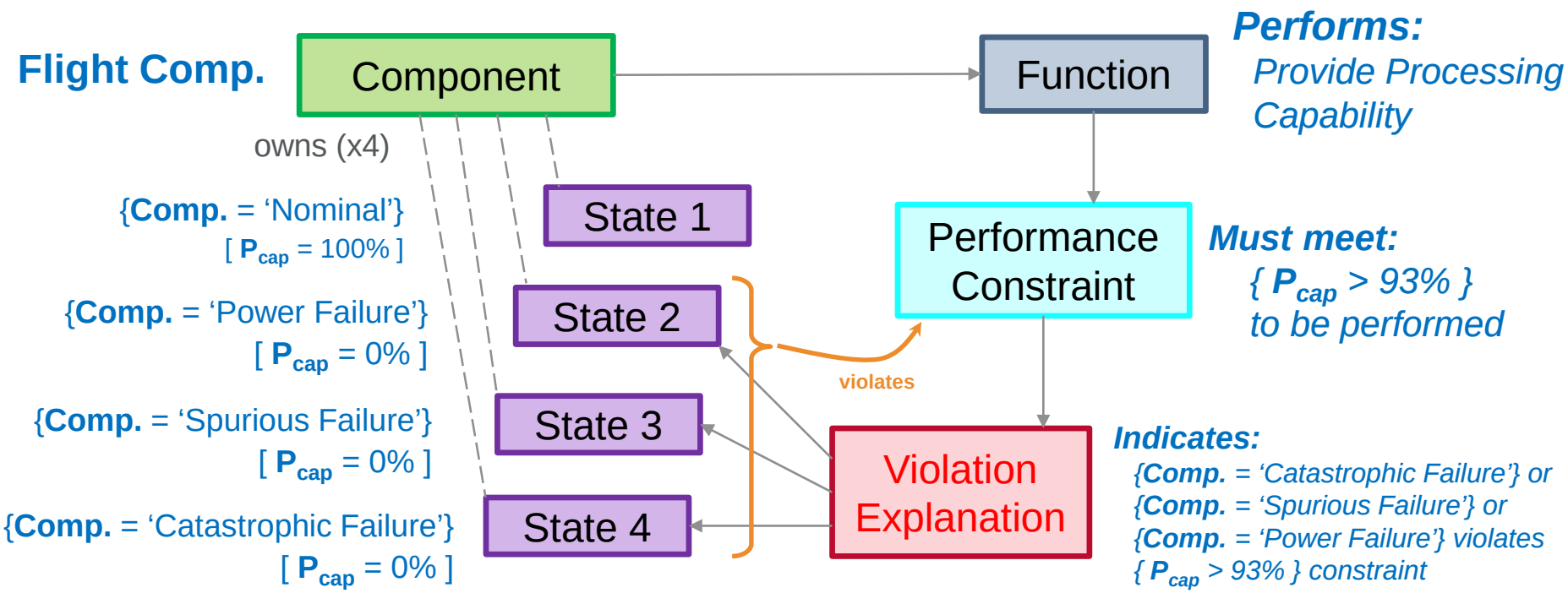
(from Castet, JF et al, "Fault Management Ontology and Modeling Patterns". AIAA Space 2016. Long Beach, CA, 2016.)

Redundancy Concepts

(from Castet, JF et al, "Fault Management Ontology and Modeling Patterns". AIAA Space 2016. Long Beach, CA, 2016.)



Tracing Reqt to Failure Modes – Comp.



What the diagram means:

"(**{Comp. = 'Power Failure'}** or **{Comp. = 'Spurious Failure'}** or **{Comp. = 'Catastrophic Failure'}**) results in **{Comp.}** not being able to perform **{Provide Processing Capability}** function"

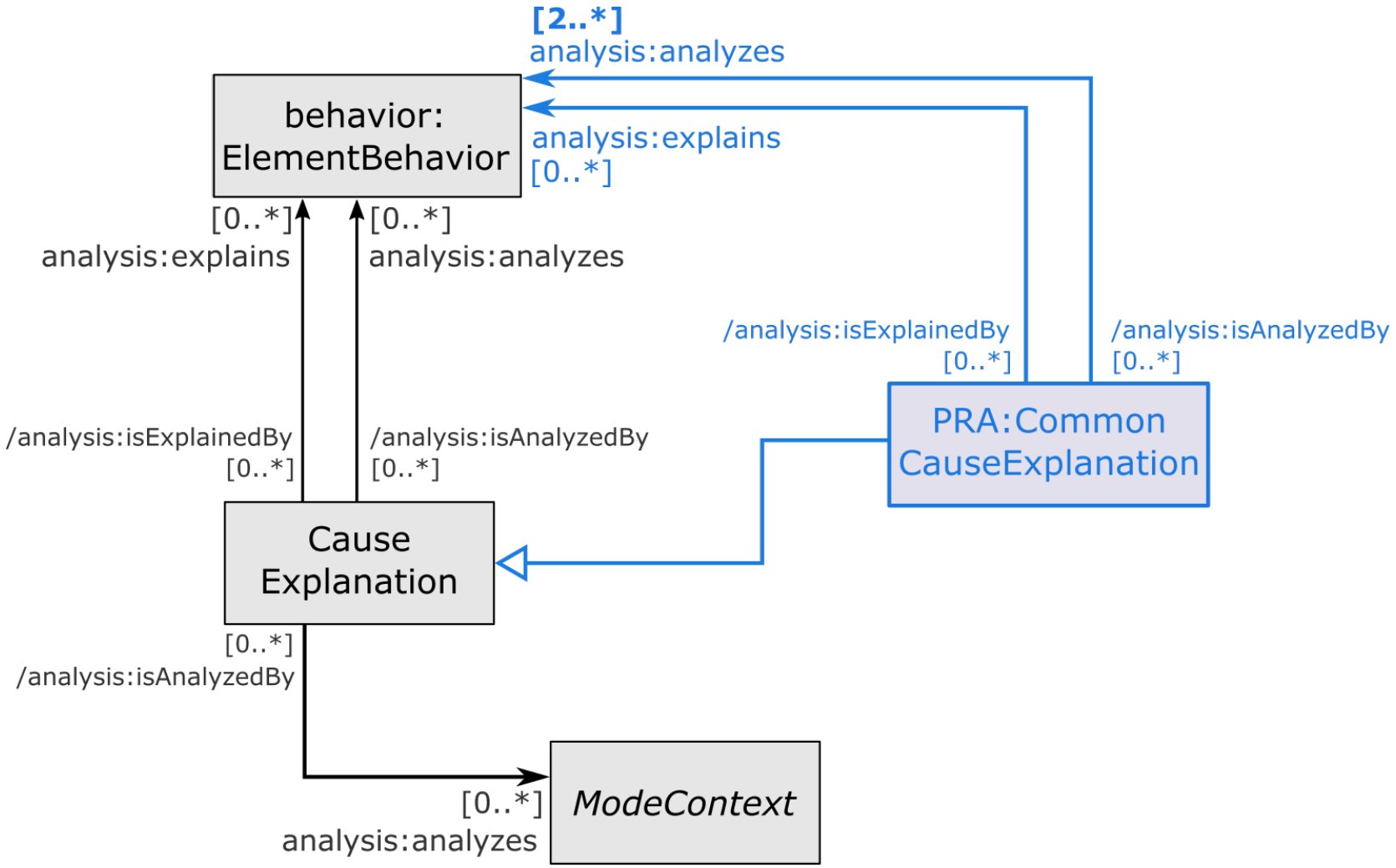
More Generally:

*"(**{State 2}** or **{State 3}** or **{State 4}**) results in **{Component}** not being able to perform **{Function}**"*

Common Cause Ontology

Usage of Common Cause Explanations:

- *Describe how two failures can occur from a common cause*

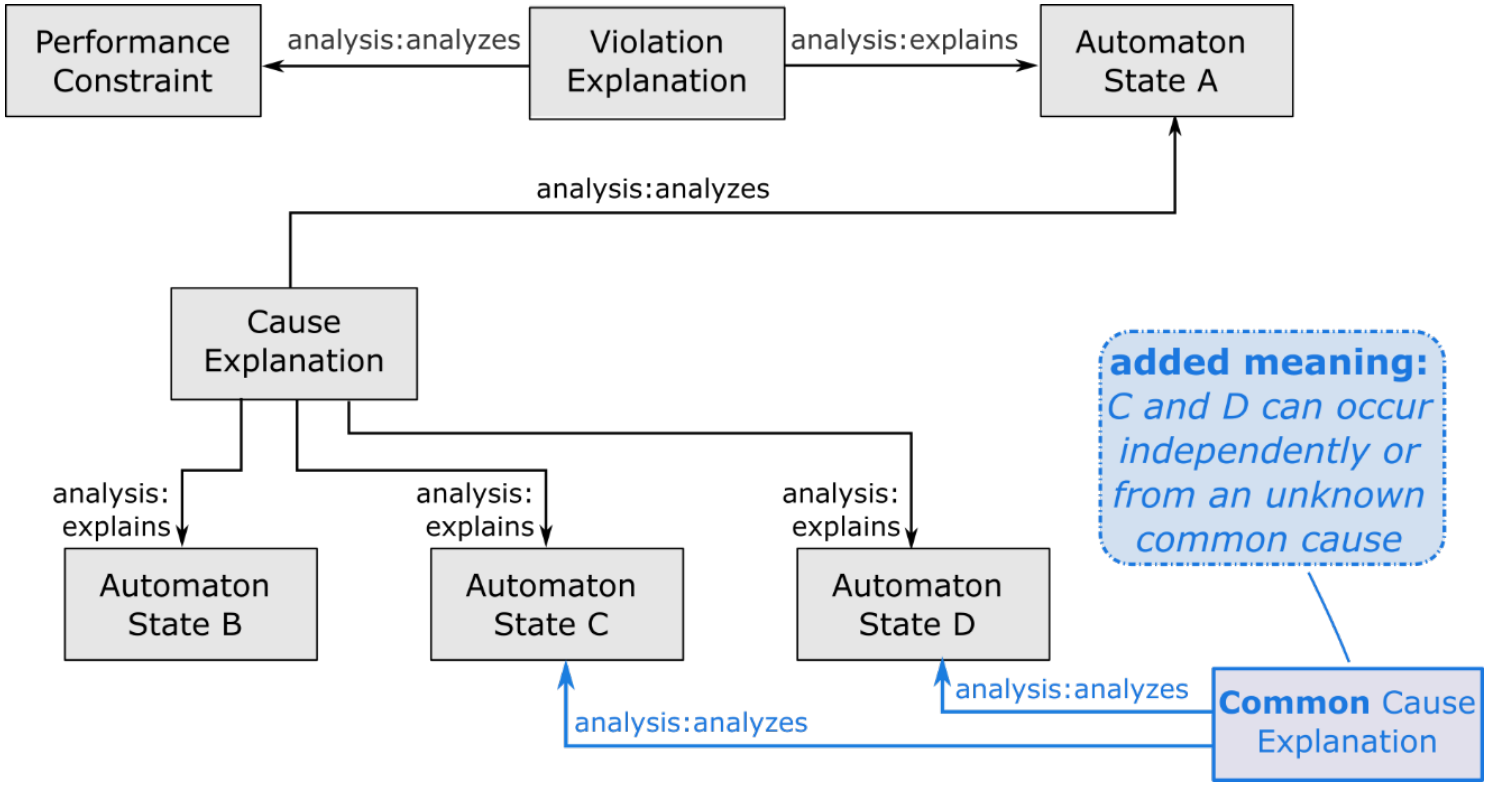


The technical data in this document is controlled under the U.S. Export Regulations, release to foreign persons may require an export authorization. For planning and discussion purposes only.

Common Cause Example

Usage of Common Cause Explanations:

- *Describe how two failures can occur from a common cause*
- *Critical factor in determining correct probabilistic model*



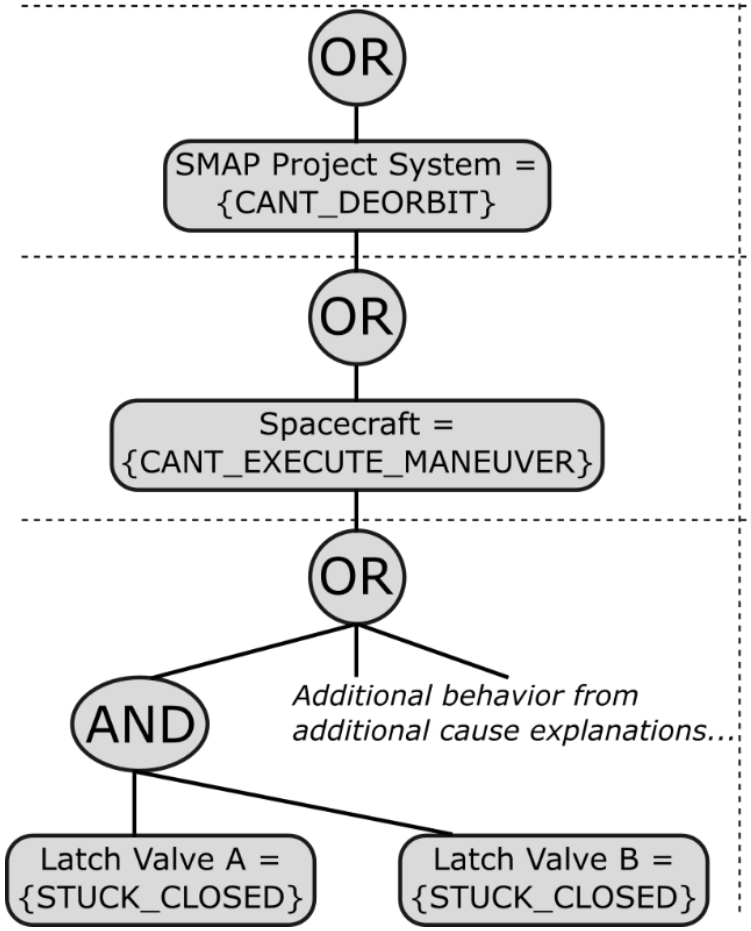
WAS (without Common Cause Explanation)	IS (with Common Cause Explanation)
State A can be caused by being in the intersection ("AND") of States B, C, and D occurring independently	State A can be caused by being in the union ("OR") of: • The intersection of (B, C, and D occurring independently) • The intersection of (B occurring independently and C and D occurring due to a common cause)

The technical data in this document is controlled under the U.S. Export Regulations, release to foreign persons may require an export authorization. For planning and discussion purposes only.

Determining Logical Operators

Levels of granularity in the element behavior tree:

Performance constraint
(SMAP Project System OperatingMode = CAN_DEORBIT)
will be violated if:



SMAP Project System = {CANT_DEORBIT}

Spacecraft = {CANT_EXECUTE_MANEUVER}

(Latch Valve A = {STUCK_CLOSED}
AND
Latch Valve B = {STUCK_CLOSED})

OR

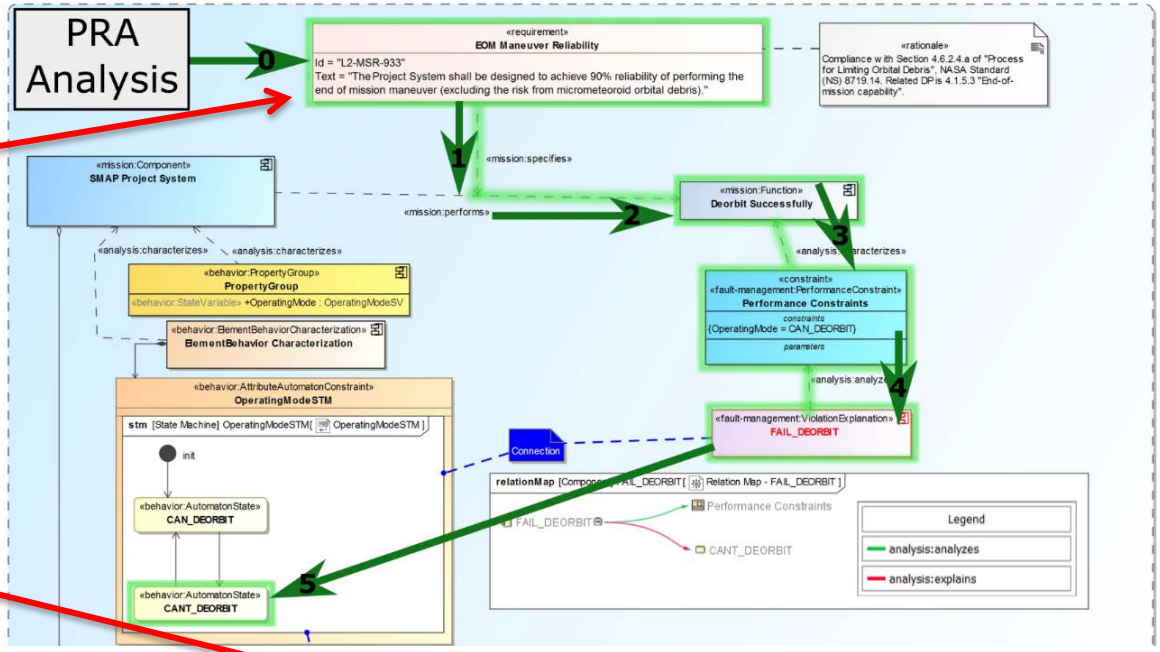
(*Leaf-level behavior from additional cause explanations that analyzed Spacecraft = {CANT_EXECUTE_MANEUVER}*)

Sample Spacecraft Model

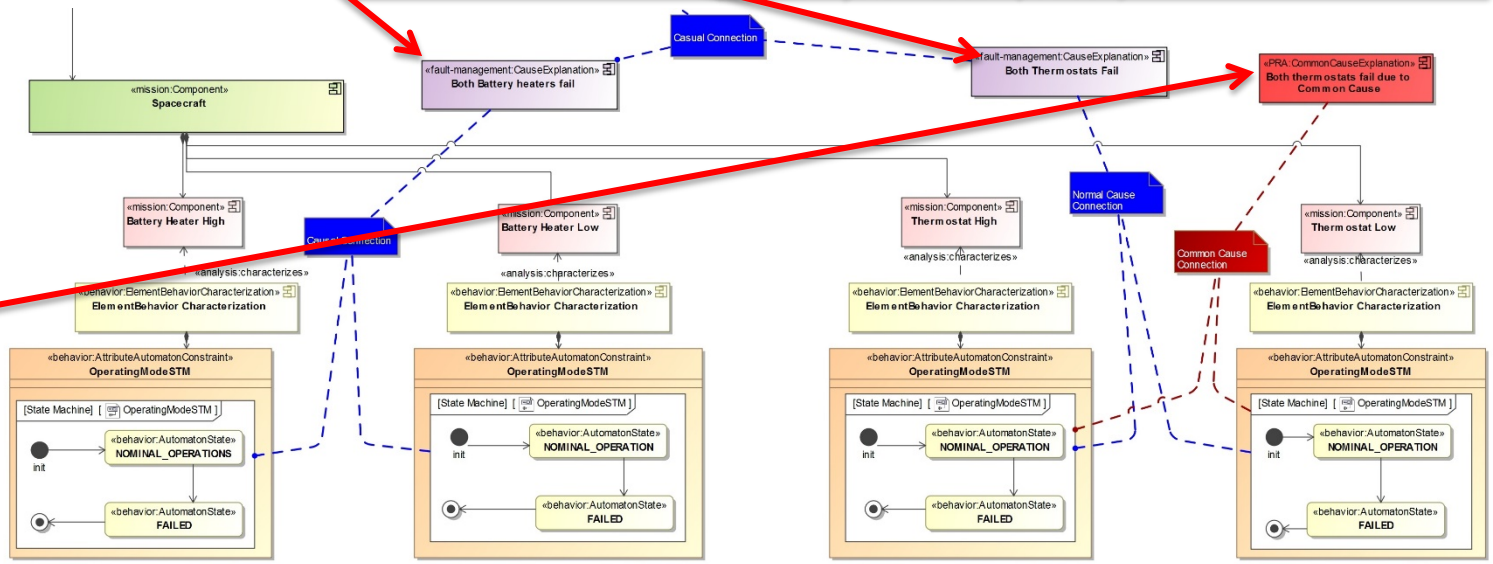
Script starts from a requirement or PRA analysis to match typical PRA methodology

Heater and Thermostat failures are connected as potential causes of Spacecraft failure to deorbit

Additional failure mode for both thermostats failing due to common cause (i.e. mfg defect)



… (layer of system decomposition) …



Steps 0-3

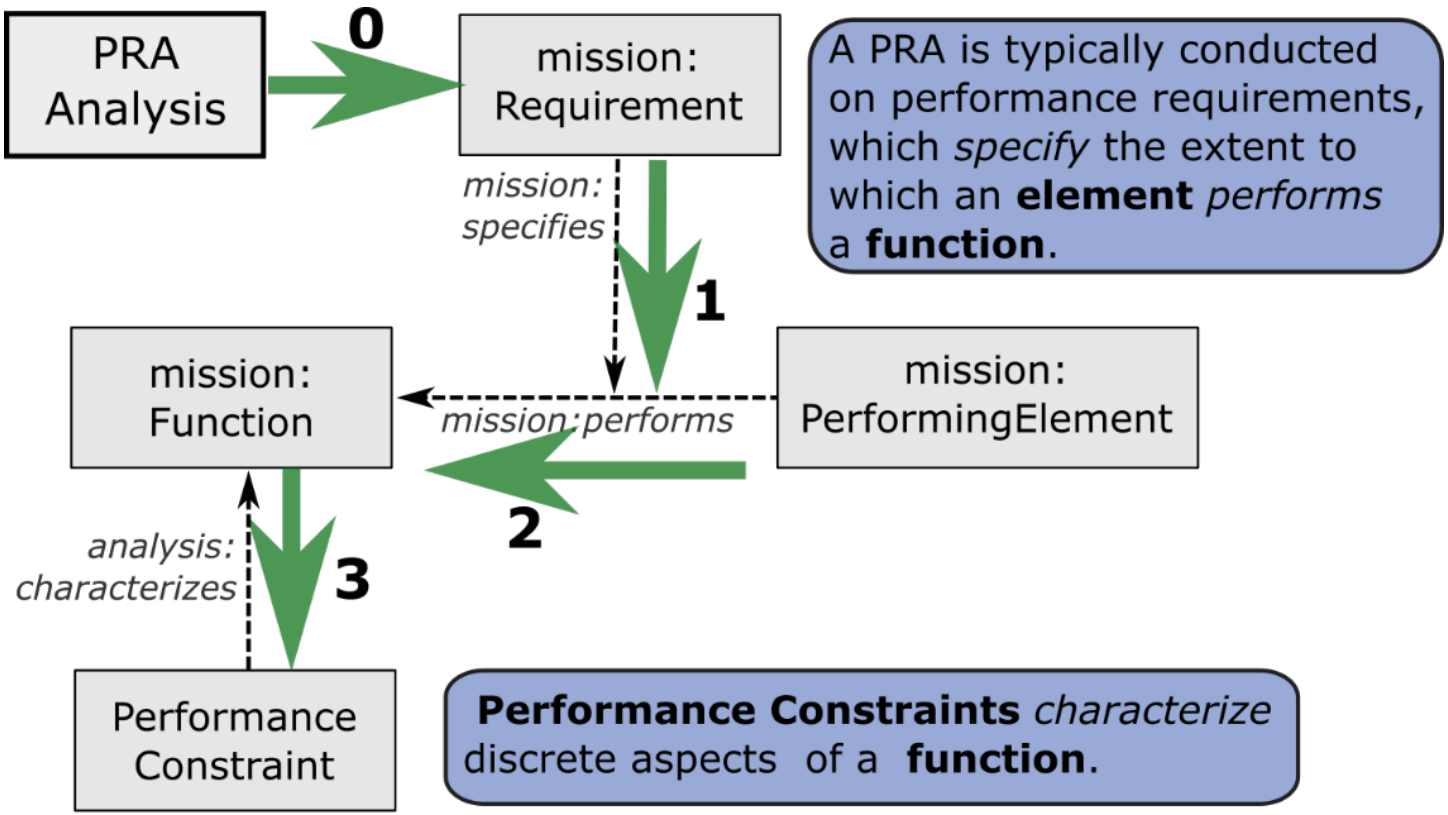


Figure 2. An illustration of steps 0-3 of the model-based probabilistic risk assessment. The methodology traces from one or more requirements (given as an input) to locate performance constraints that represent discrete acceptable levels of performance of an element with respect to the function specified by the requirement. Numbers next to green arrows indicate references to the steps in Table 2.

Steps 4-5

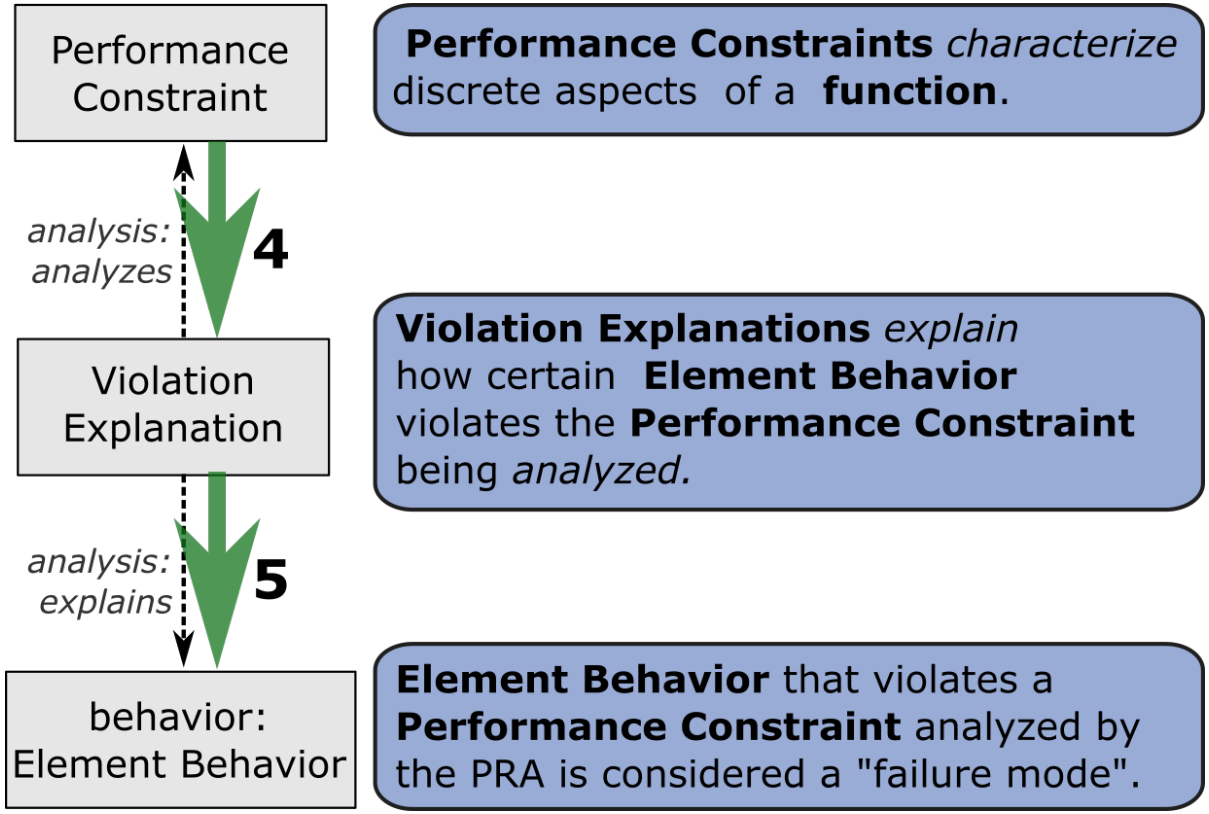


Figure 3. An illustration of steps 4 and 5 of the model-based probabilistic risk assessment. The methodology locates any Violation Explanations that analyze the performance constraint(s) identified in step 3 and explain how they could be violated by one or more element behaviors, called "failure modes". Numbers next to green arrows indicate references to the steps in Table 3.

Steps 5-6 (recursive)

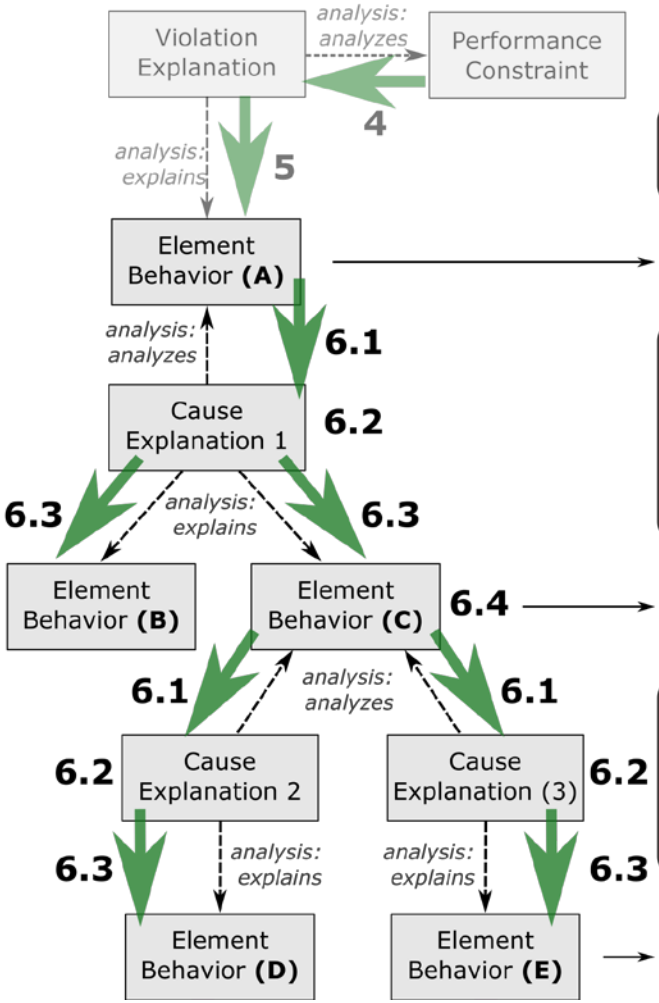
Violation Explanations *explain* how certain **Element Behavior** violates the **Performance Constraint** being *analyzed.*

Element Behavior that violates a **Performance Constraint** is considered a "failure mode".

Cause Explanations *analyze* **Element Behavior(s)** and *explain* why other **Element Behavior(s)** may cause it.

Element Behavior that is not *analyzed* by a **Cause Explanation** has no identified causes, which classifies it as "basic behavior" (i.e. Element Behavior B).

The PRA methodology recursively traverses through **Cause Explanations** to locate basic **Element Behaviors**. The occurence of a basic behavior is considered a basic event.



The following **Element Behavior(s)** will violate the **Performance Constraint**:

Element Behavior **(A)**

If a **Cause Explanation** points to multiple antecedent **Element Behaviors** (with an *explains* relationship), this is interpreted as an intersection (AND).

Element Behaviors **(B)** and **(C)**

If multiple **Cause Explanations** describe causes of an **Element Behavior** (with an *analyzes* relationship) this is interpreted as a union (OR).

Element Behaviors **(B)** and [**(D)** or **(E)**]

Figure 4. An illustration of Step 6 of the PRA methodology, which is executed recursively until it locates a set of basic element behavior that has no identified causes. The methodology for determining the logical expression is presented in red text boxes on the right. Numbers next to green arrows indicate references to the steps in Table 4.