Ground System PRA Data Availability Case Study

Charlie Knapp

GSFC Reliability

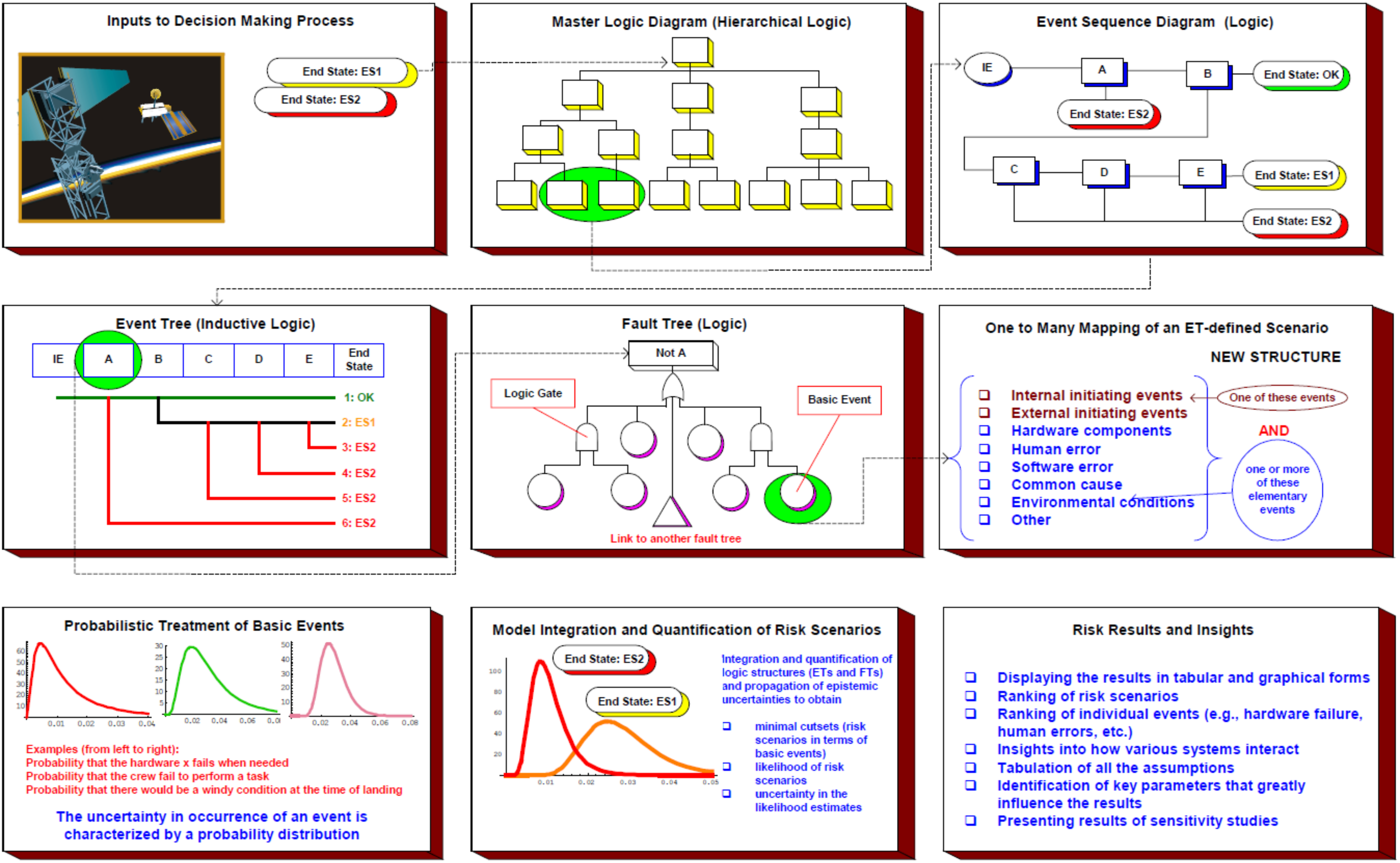
11 Sept 2019

NASA GSFC SMA Directorate

MAMII Meeting, GSFC - Greenbelt, MD

PRA Process

PRA Procedures Guide for Managers and Practitioners – NASA HQ 8/2002



Inputs to Decision Making Process
End State: ES1
End State: ES2
Master Logic Diagram (Hierarchical Logic)
Event Sequence Diagram (Logic)
IE
A
B
End State: OK
End State: ES2
C
D
E
End State: ES1
End State: ES2
Event Tree (Inductive Logic)
IE
A
B
C
D
E
End State
1: OK
2: ES1
3: ES2
4: ES2
5: ES2
6: ES2
Fault Tree (Logic)
Not A
Logic Gate
Basic Event
Link to another fault tree
One to Many Mapping of an ET-defined Scenario
NEW STRUCTURE
One of these events
AND
one or more of these elementary events
Probabilistic Treatment of Basic Events
0.01
0.02
0.03
0.04
0.02
0.04
0.06
0.08
Model Integration and Quantification of Risk Scenarios
End State: ES2
End State: ES1
100
80
60
40
20
0.01
0.02
0.03
0.04
0.05
Risk Results and Insights

- ❑ Internal initiating events
- ❑ External initiating events
- ❑ Hardware components
- ❑ Human error
- ❑ Software error
- ❑ Common cause
- ❑ Environmental conditions
- ❑ Other

Examples (from left to right):
Probability that the hardware x fails when needed
Probability that the crew fail to perform a task
Probability that there would be a windy condition at the time of landing

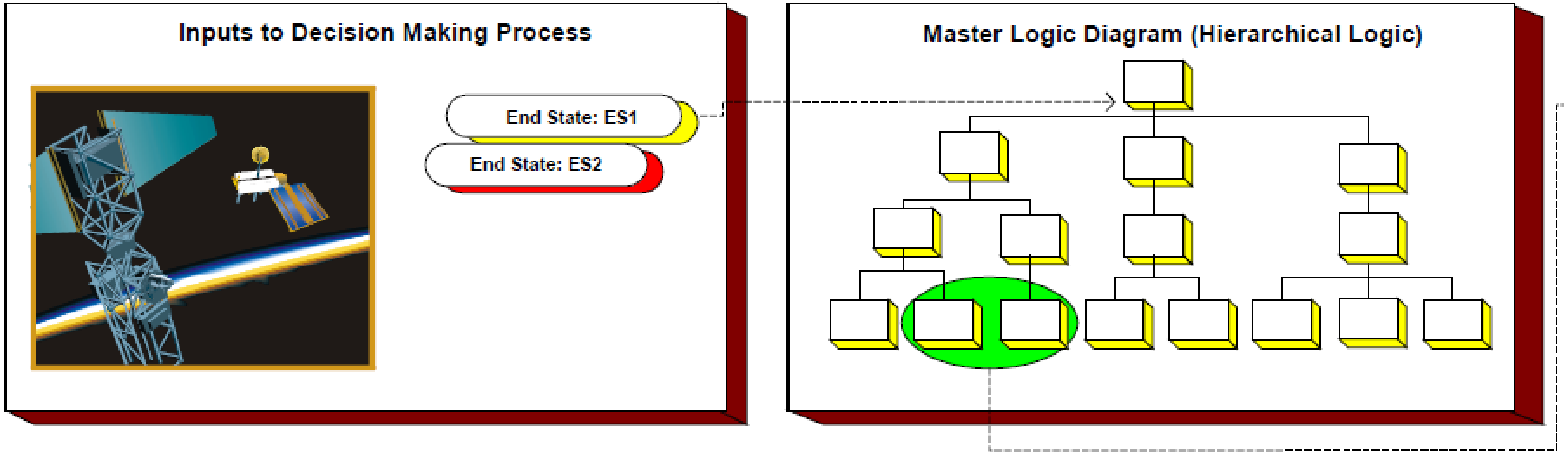
The uncertainty in occurrence of an event is characterized by a probability distribution

Integration and quantification of logic structures (ETs and FTs) and propagation of epistemic uncertainties to obtain

- ❑ minimal cutsets (risk scenarios in terms of basic events)
- ❑ likelihood of risk scenarios
- ❑ uncertainty in the likelihood estimates

- ❑ Displaying the results in tabular and graphical forms
- ❑ Ranking of risk scenarios
- ❑ Ranking of individual events (e.g., hardware failure, human errors, etc.)
- ❑ Insights into how various systems interact
- ❑ Tabulation of all the assumptions
- ❑ Identification of key parameters that greatly influence the results
- ❑ Presenting results of sensitivity studies

PRA Process
End State of Concern / Initiating Event

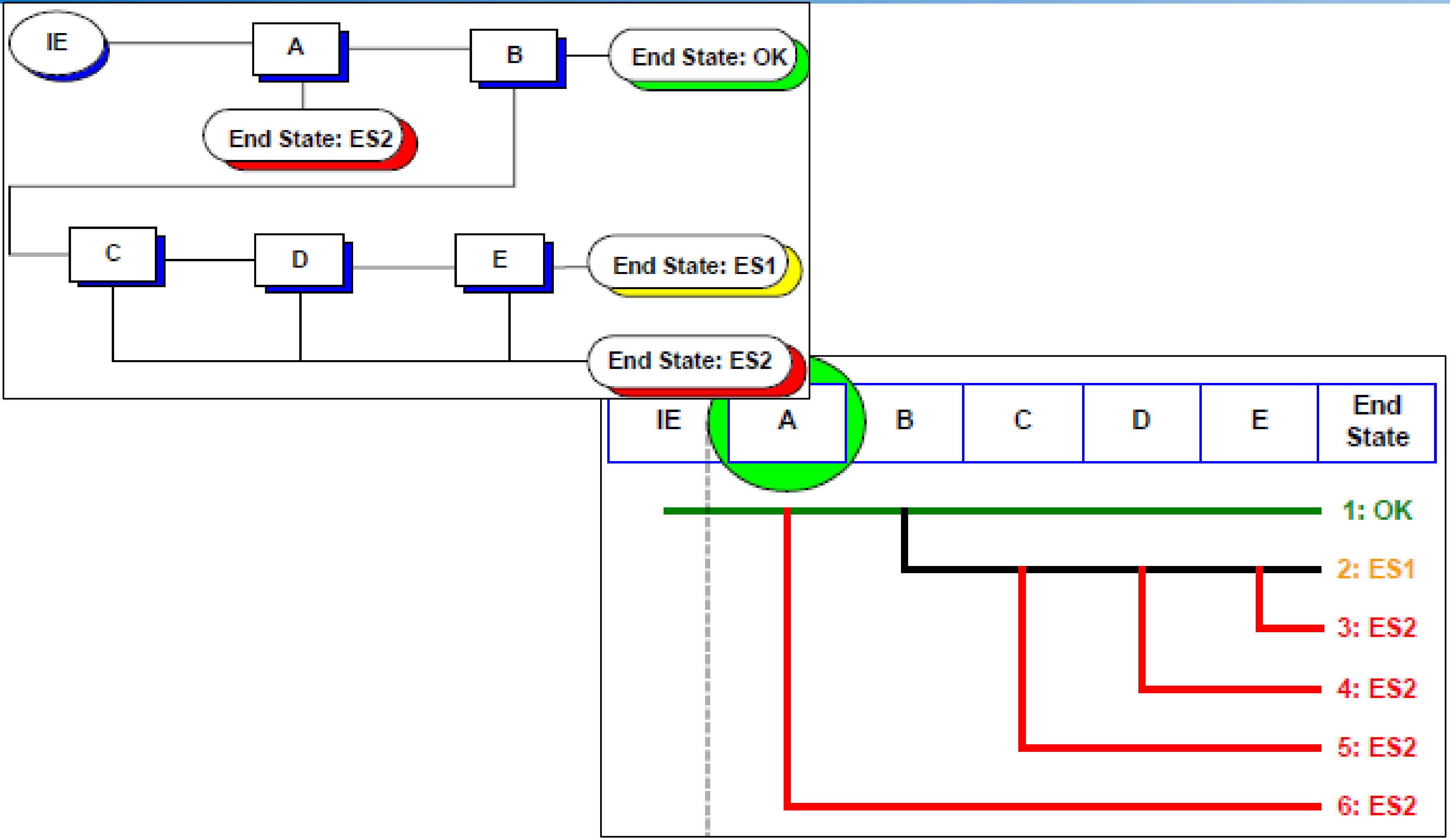

Inputs to Decision Making Process
End State: ES1
End State: ES2
Master Logic Diagram (Hierarchical Logic)

End State of Concern = *Loss of Science Data*

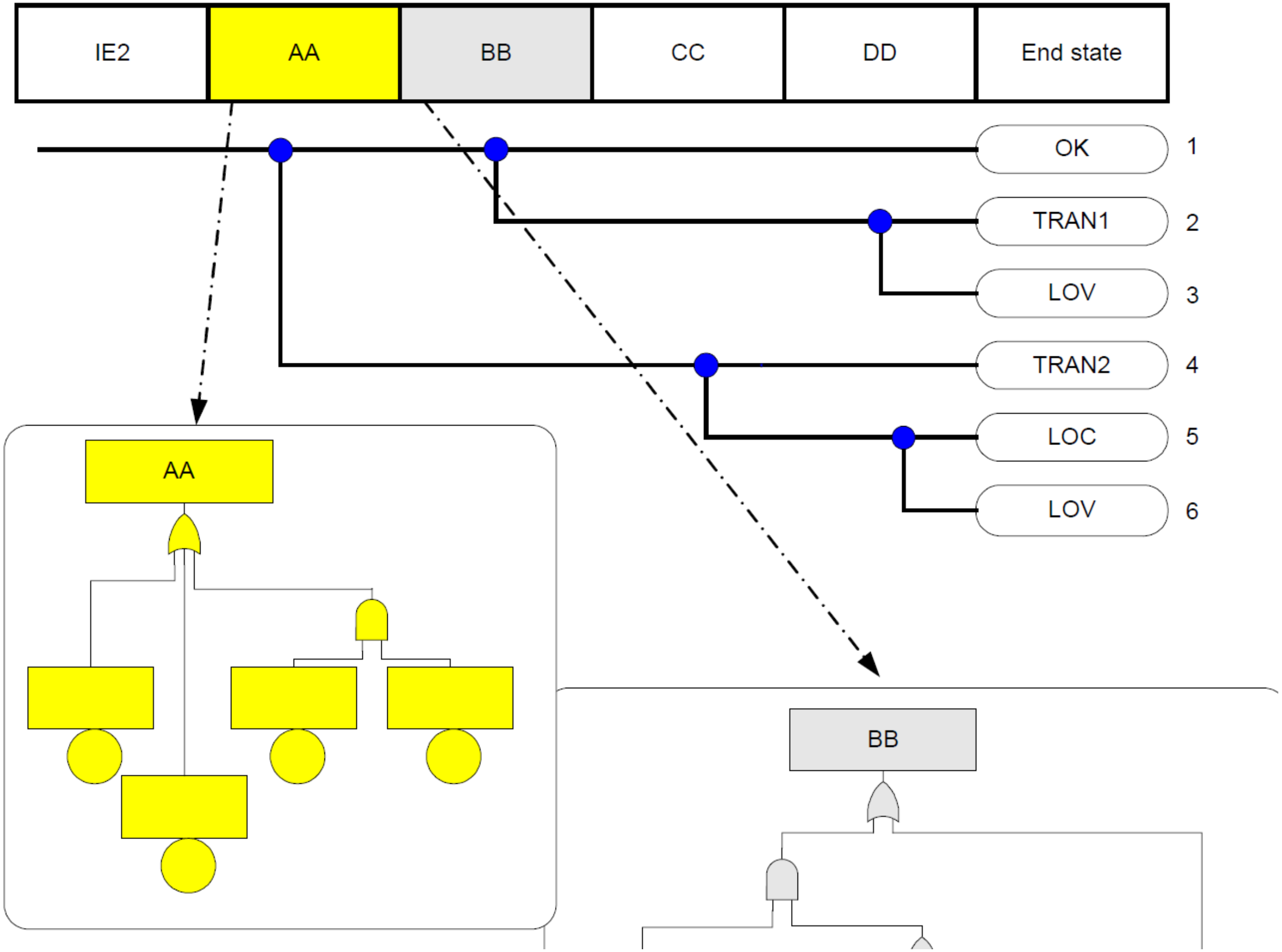
Initiating Event = *MMC Generates Commands*

PRA Process

Event Sequence Diagram - Event Tree



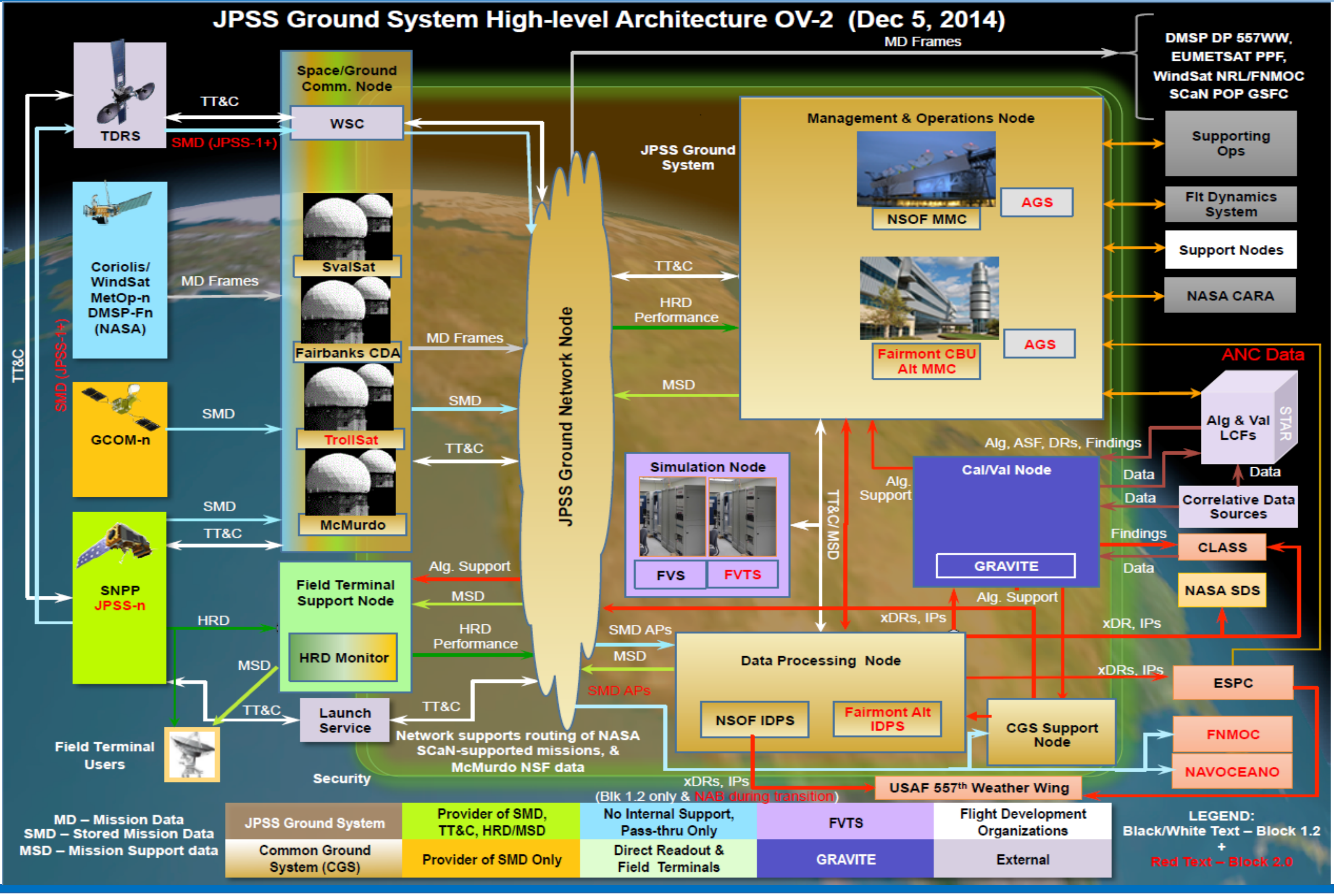
PRA Process
Event Tree - FTA



CASE STUDY

JPSS Ground Data Availability

JPSS Ground System



Data Availability PRA Goals

- Predict data availability for the JPSS Ground System in order to
  - Verify that the system will meet JPSS Level 1 requirement that ≥ 99% of science data collected be delivered to the data processing sites, measured over a 30-day period.
  - Identify the risks that could prevent the system from meeting the Level 1 requirement

What percentage of our data will we lose and why?

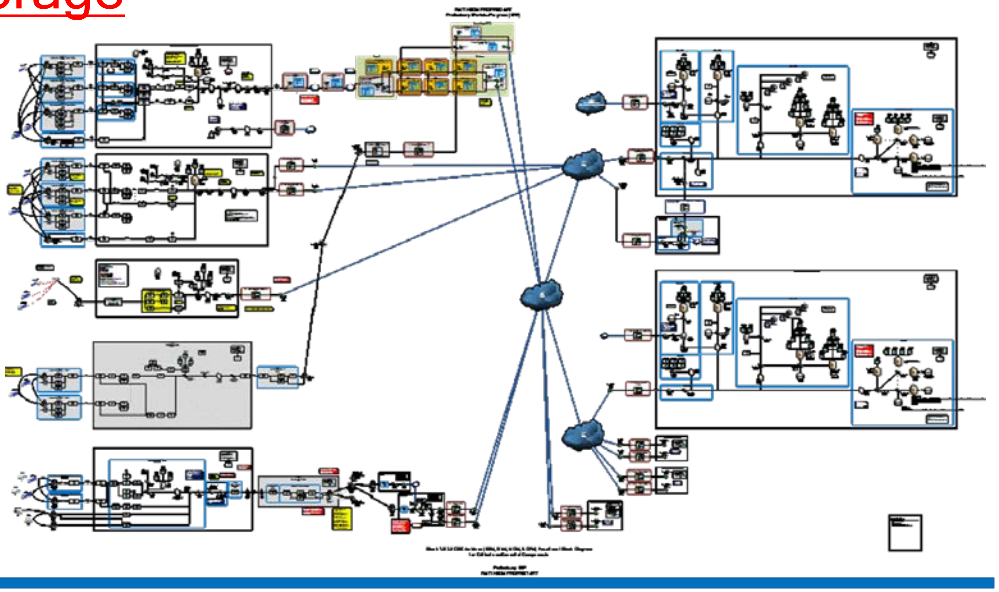
Availability PRA Assumptions/Scope

- **The spacecraft storage limit is 6.8 hours.**
- **All ground stations have a data storage limit of seven days.**
- **Ability to command the spacecraft must be lost for seven days to cause a data loss.**

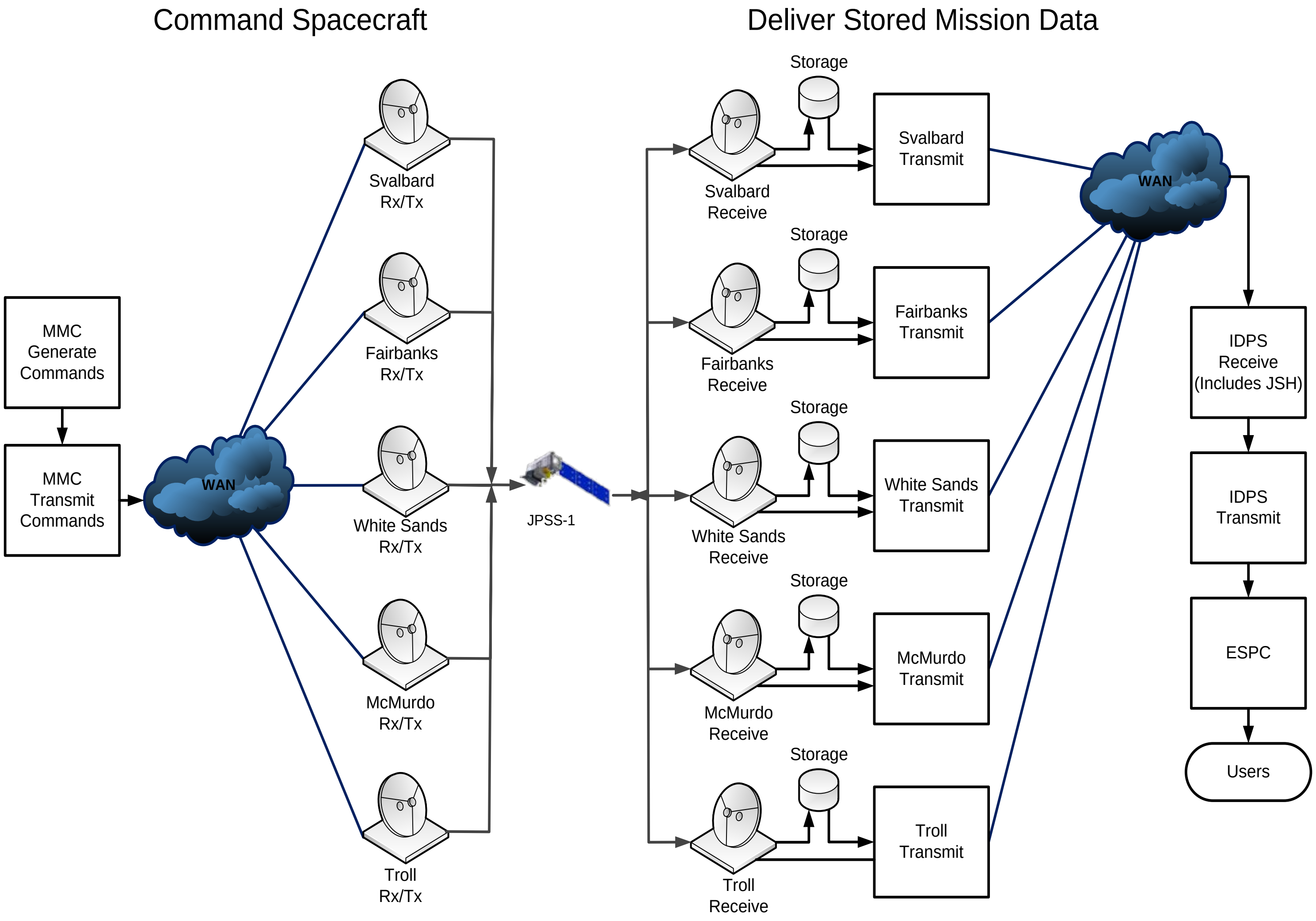
- The spacecraft is always fully functional.
- Latency is not considered.
- Security threats and environmental and other threats beyond the control of the design are not considered.
- Switching to the Consolidated Back-Up (CBU) and the B-Side CGS/DPN is not considered.
- Data storage at the JPSS SMD Hub is not considered.

Availability PRA Challenges

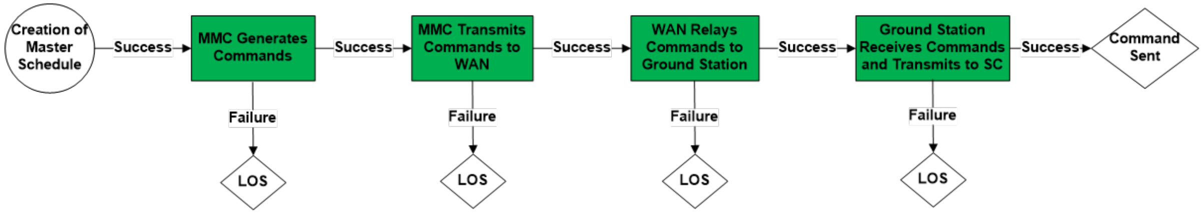
- Complex System
- Data Availability is not Operational Availability
- Data Availability is not Reliability
- Due to Data Storage, Downtime is normally not Data Loss
- Software Limitations
- Parallel Data Paths with Storage

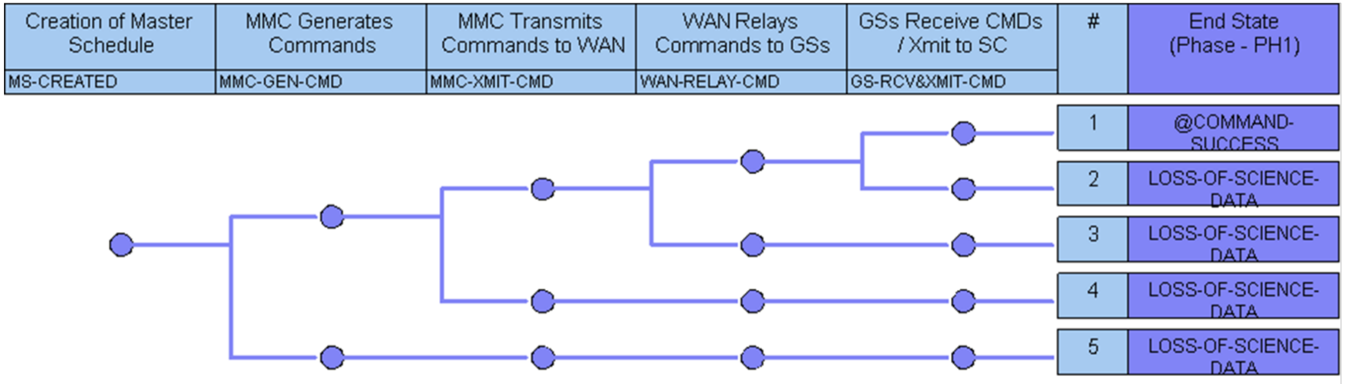


Redefining System of Interest



Event Sequence Diagram and Tree - Command

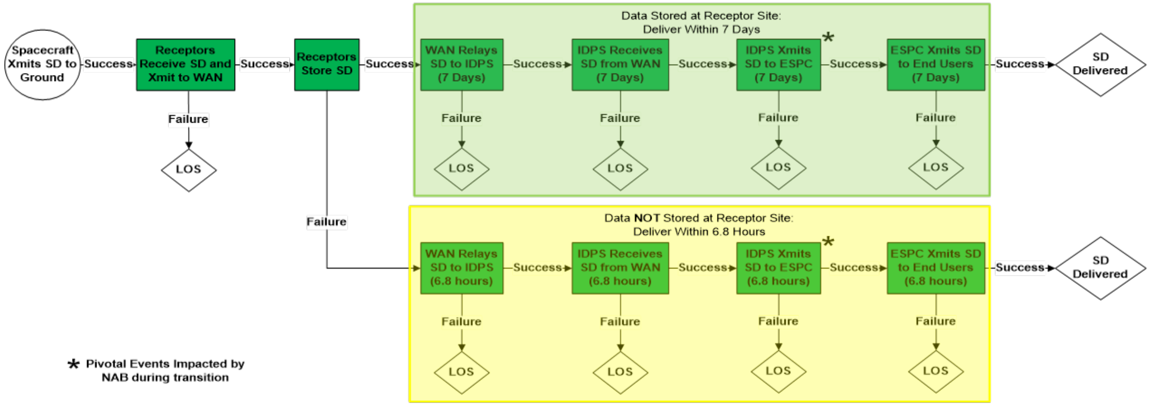

Creation of Master Schedule
Success
MMC Generates Commands
Success
MMC Transmits Commands to WAN
Success
WAN Relays Commands to Ground Station
Success
Ground Station Receives Commands and Transmits to SC
Success
Command Sent
Failure
LOS
Failure
LOS
Failure
LOS
Failure
LOS



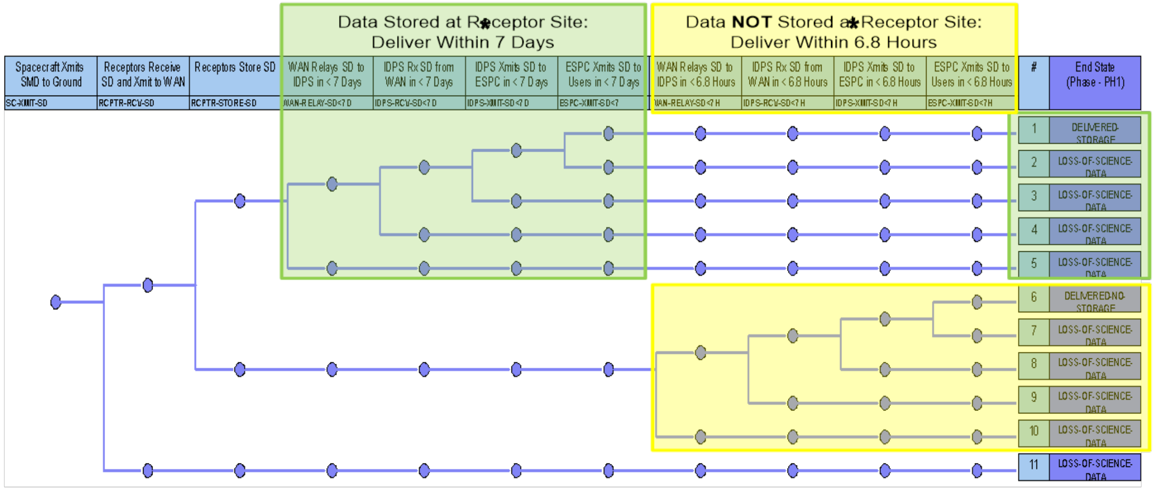
Creation of Master Schedule	MMC Generates Commands	MMC Transmits Commands to WAN	WAN Relays Commands to GSs	GSs Receive CMDs / Xmit to SC	#	End State (Phase - PH1)
MS-CREATED	MMC-GEN-CMD	MMC-XMIT-CMD	WAN-RELAY-CMD	GS-RCV&XMIT-CMD		
					1	@COMMAND-SUCCESS
					2	LOSS-OF-SCIENCE-DATA
					3	LOSS-OF-SCIENCE-DATA
					4	LOSS-OF-SCIENCE-DATA
					5	LOSS-OF-SCIENCE-DATA

- MMC Generates Commands
- MMC Transmits Commands to WAN
- WAN Relays Commands to Ground Station (GS)
- GS Receives Commands and Transmits to SC

Event Sequence Diagram and Tree - Data

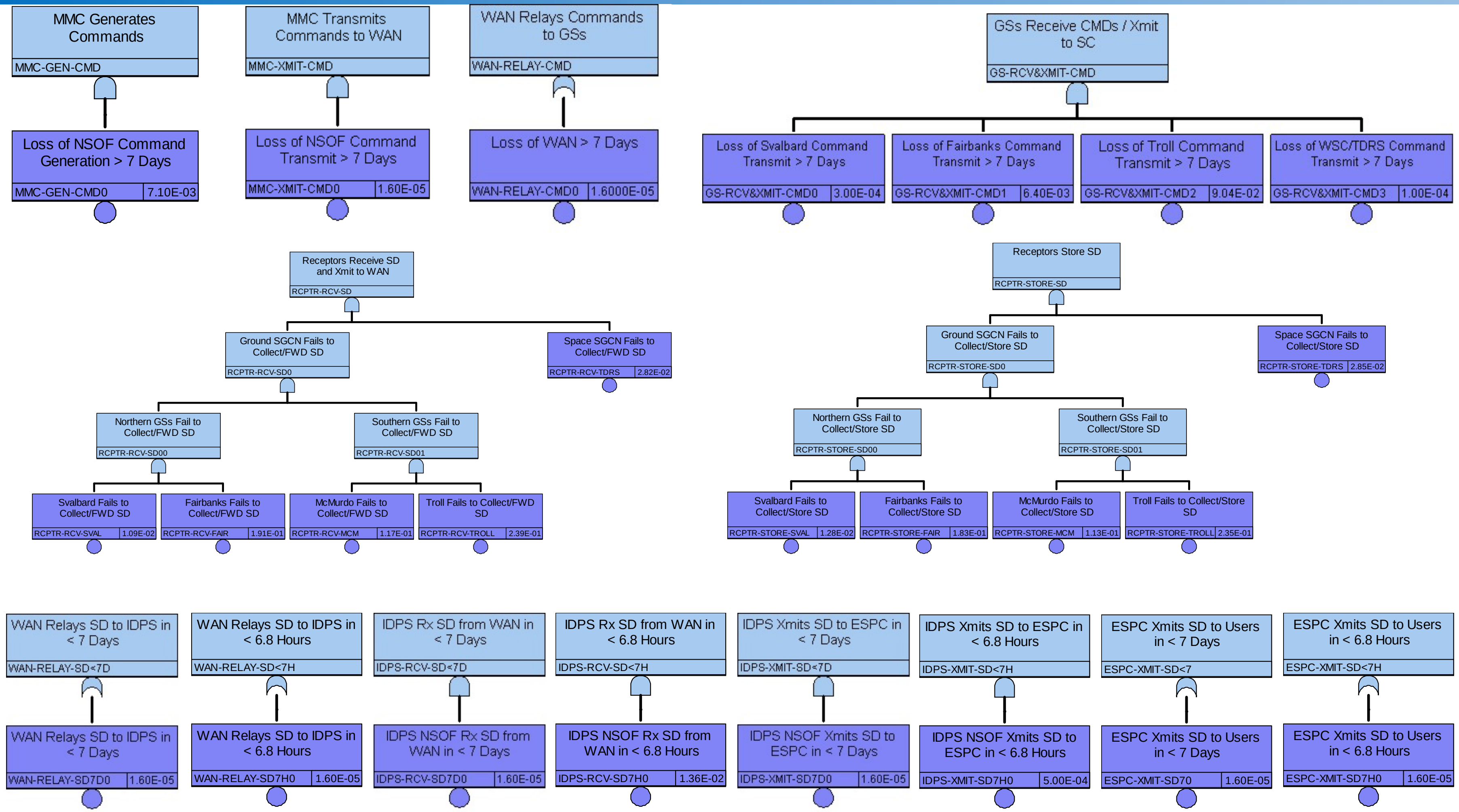

Spacecraft Xmits SD to Ground
Success
Receptors Receive SD and Xmit to WAN
Failure
LOS
Success
Receptors Store SD
Success
Failure
Data Stored at Receptor Site:
Deliver Within 7 Days
WAN Relays SD to IDPS (7 Days)
Success
IDPS Receives SD from WAN (7 Days)
Success
*
IDPS Xmits SD to ESPC (7 Days)
Success
ESPC Xmits SD to End Users (7 Days)
Success
SD Delivered
Failure
LOS
Data NOT Stored at Receptor Site:
Deliver Within 6.8 Hours
WAN Relays SD to IDPS (6.8 hours)
Success
IDPS Receives SD from WAN (6.8 hours)
Success
*
IDPS Xmits SD to ESPC (6.8 hours)
Success
ESPC Xmits SD to End Users (6.8 hours)
Success
SD Delivered
Failure
LOS
* Pivotal Events Impacted by NAB during transition

- Receptors Receive SD
- Receptors Store SD [If successful, 7 Days to deliver; if not, 6.8 hours]
  - o WAN Relays SD to IDPS
  - o IDPS Receives SD from WAN
  - o IDPS Xmits SD to ESPC
  - o ESPC Xmits SD to End Users


Data Stored at R*ceptor Site:
Deliver Within 7 Days
Data NOT Stored a*Receptor Site:
Deliver Within 6.8 Hours
Spacecraft Xmits SMD to Ground
SC-XMIT-SD
Receptors Receive SD and Xmit to WAN
RCPTR-RCV-SD
Receptors Store SD
RCPTR-STORE-SD
WAN Relays SD to IDPS in < 7 Days
WAN-RELAY-SD<7D
IDPS Rx SD from WAN in < 7 Days
IDPS-RCV-SD<7D
IDPS Xmits SD to ESPC in < 7 Days
IDPS-XMIT-SD<7D
ESPC Xmits SD to Users in < 7 Days
ESPC-XMIT-SD<7
WAN Relays SD to IDPS in < 6.8 Hours
WAN-RELAY-SD<7H
IDPS Rx SD from WAN in < 6.8 Hours
IDPS-RCV-SD<7H
IDPS Xmits SD to ESPC in < 6.8 Hours
IDPS-XMIT-SD<7H
ESPC Xmits SD to Users in < 6.8 Hours
ESPC-XMIT-SD<7H

#	End State (Phase - PH1)
1	DELIVERED-STORAGE
2	LOSS-OF-SCIENCE-DATA
3	LOSS-OF-SCIENCE-DATA
4	LOSS-OF-SCIENCE-DATA
5	LOSS-OF-SCIENCE-DATA
6	DELIVERED-NO-STORAGE
7	LOSS-OF-SCIENCE-DATA
8	LOSS-OF-SCIENCE-DATA
9	LOSS-OF-SCIENCE-DATA
10	LOSS-OF-SCIENCE-DATA
11	LOSS-OF-SCIENCE-DATA

Availability Fault Trees



MMC Generates Commands
MMC-GEN-CMD
Loss of NSOF Command Generation > 7 Days
MMC-GEN-CMD0 7.10E-03

MMC Transmits Commands to WAN
MMC-XMIT-CMD
Loss of NSOF Command Transmit > 7 Days
MMC-XMIT-CMD0 1.60E-05

WAN Relays Commands to GSs
WAN-RELAY-CMD
Loss of WAN > 7 Days
WAN-RELAY-CMD0 1.6000E-05

GSs Receive CMDs / Xmit to SC
GS-RCV&XMIT-CMD
Loss of Svalbard Command Transmit > 7 Days
GS-RCV&XMIT-CMD0 3.00E-04
Loss of Fairbanks Command Transmit > 7 Days
GS-RCV&XMIT-CMD1 6.40E-03
Loss of Troll Command Transmit > 7 Days
GS-RCV&XMIT-CMD2 9.04E-02
Loss of WSC/TDRS Command Transmit > 7 Days
GS-RCV&XMIT-CMD3 1.00E-04

Receptors Receive SD and Xmit to WAN
RCPTR-RCV-SD
Ground SGCN Fails to Collect/FWD SD
RCPTR-RCV-SD0
Space SGCN Fails to Collect/FWD SD
RCPTR-RCV-TDRS 2.82E-02
Northern GSs Fail to Collect/FWD SD
RCPTR-RCV-SD00
Southern GSs Fail to Collect/FWD SD
RCPTR-RCV-SD01
Svalbard Fails to Collect/FWD SD
RCPTR-RCV-SVAL 1.09E-02
Fairbanks Fails to Collect/FWD SD
RCPTR-RCV-FAIR 1.91E-01
McMurdo Fails to Collect/FWD SD
RCPTR-RCV-MCM 1.17E-01
Troll Fails to Collect/FWD SD
RCPTR-RCV-TROLL 2.39E-01

Receptors Store SD
RCPTR-STORE-SD
Ground SGCN Fails to Collect/Store SD
RCPTR-STORE-SD0
Space SGCN Fails to Collect/Store SD
RCPTR-STORE-TDRS 2.85E-02
Northern GSs Fail to Collect/Store SD
RCPTR-STORE-SD00
Southern GSs Fail to Collect/Store SD
RCPTR-STORE-SD01
Svalbard Fails to Collect/Store SD
RCPTR-STORE-SVAL 1.28E-02
Fairbanks Fails to Collect/Store SD
RCPTR-STORE-FAIR 1.83E-01
McMurdo Fails to Collect/Store SD
RCPTR-STORE-MCM 1.13E-01
Troll Fails to Collect/Store SD
RCPTR-STORE-TROLL 2.35E-01

WAN Relays SD to IDPS in < 7 Days
WAN-RELAY-SD<7D
WAN Relays SD to IDPS in < 7 Days
WAN-RELAY-SD7D0 1.60E-05

WAN Relays SD to IDPS in < 6.8 Hours
WAN-RELAY-SD<7H
WAN Relays SD to IDPS in < 6.8 Hours
WAN-RELAY-SD7H0 1.60E-05

IDPS Rx SD from WAN in < 7 Days
IDPS-RCV-SD<7D
IDPS NSOF Rx SD from WAN in < 7 Days
IDPS-RCV-SD7D0 1.60E-05

IDPS Rx SD from WAN in < 6.8 Hours
IDPS-RCV-SD<7H
IDPS NSOF Rx SD from WAN in < 6.8 Hours
IDPS-RCV-SD7H0 1.36E-02

IDPS Xmits SD to ESPC in < 7 Days
IDPS-XMIT-SD<7D
IDPS NSOF Xmits SD to ESPC in < 7 Days
IDPS-XMIT-SD7D0 1.60E-05

IDPS Xmits SD to ESPC in < 6.8 Hours
IDPS-XMIT-SD<7H
IDPS NSOF Xmits SD to ESPC in < 6.8 Hours
IDPS-XMIT-SD7H0 5.00E-04

ESPC Xmits SD to Users in < 7 Days
ESPC-XMIT-SD<7
ESPC Xmits SD to Users in < 7 Days
ESPC-XMIT-SD70 1.60E-05

ESPC Xmits SD to Users in < 6.8 Hours
ESPC-XMIT-SD<7H
ESPC Xmits SD to Users in < 6.8 Hours
ESPC-XMIT-SD7H0 1.60E-05

25 Monte Carlo Simulations

Event Description	Failure Probability	Basis
ESPC Xmits SD to Users in < 7 Days	0.0016%*	Model: 0 / 10K months failed
ESPC Xmits SD to Users in < 6.8 hours	0.0016%*	Model: 0 / 10K months failed
Loss of Svalbard Command Transmit > 7 Days	0.03%	Model: 3 / 10K months failed
Loss of Fairbanks Command Transmit > 7 Days	0.64%	Model: 64 / 10K months failed
Loss of Troll Command Transmit > 7 Days	9.0%	Model: 904 / 10K months failed
Loss of WSC/TDRS Command Transmit > 7 Days	0.01%	Model: 1 / 10K months failed
IDPS Rx SD from WAN in < 7 Days	0.0016%*	Model: 0 / 10K months failed
IDPS Rx SD from WAN in < 6.8 hours	1.36%	Model: 136 / 10K months failed
IDPS Xmits SD to ESPC in < 7 Days (NAB: no effect)	0.0016%*	Model: 0 / 10K months failed
IDPS Xmits SD to ESPC in < 6.8 hours (NAB: 0.055%)	0.05%	Model: 5 / 10K months failed
Loss of NSOF Command Generation > 7 Days	0.01%	Model: 1 / 10K months failed
Loss of NSOF Command Transmit > 7 Days	0.0016%*	Model: 0 / 10K months failed
Fairbanks Fails to Collect/FWD SD	19.08%	Model: 1908 / 10K months failed
McMurdo Fails to Collect/FWD SD	11.67%	Model: 1167 / 10K months failed
Svalbard Fails to Collect/FWD SD	1.09%	Model: 109 / 10K months failed
Space SGCN Fails to Collect/FWD SD	2.82%	Model: 282 / 10K months failed
Troll Fails to Collect/FWD SD	23.90%	Model: 2390 / 10K months failed
Fairbanks Fails to Collect/Store SD	18.29%	Model: 1829 / 10K months failed
McMurdo Fails to Collect/Store SD	11.33%	Model: 1133 / 10K months failed
Svalbard Fails to Collect/Store SD	1.28%	Model: 128 / 10K months failed
Space SGCN Fails to Collect/Store SD	2.85%	Model: 285 / 10K months failed
Troll Fails to Collect/Store SD	23.51%	Model: 2351 / 10K months failed
Loss of WAN > 7 Days	0.0016%*	Model: 0 / 10K months failed
WAN Relays SD to IDPS in < 7 Days	0.0016%*	Model: 0 / 10K months failed
WAN Relays SD to IDPS in < 6.8 hours	0.0016%*	Model: 0 / 10K months failed

This did not come easy!

*Models with no failures have a calculated probability of 0.0016% based on a 90% confidence interval.

Monte Carlo Simulation

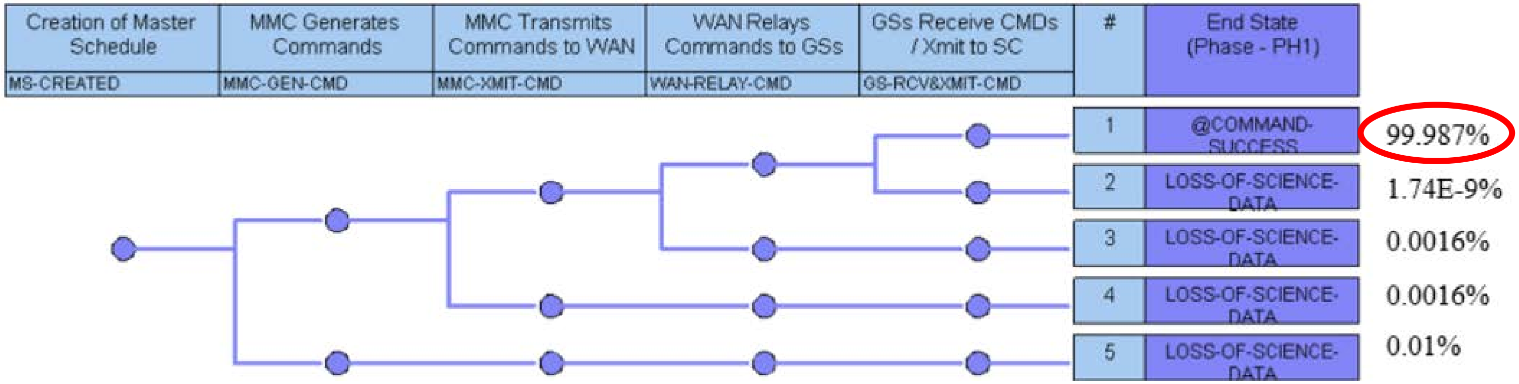
- 10,000 1-month runs per model
- Loss times can be analyzed using 2 Raptor report files
  - Failure Times (i.e., when they failed)
    - Often tens of thousands of failures
    - Not given by run
    - Occasionally missing failures
  - Key Parameters (hours)

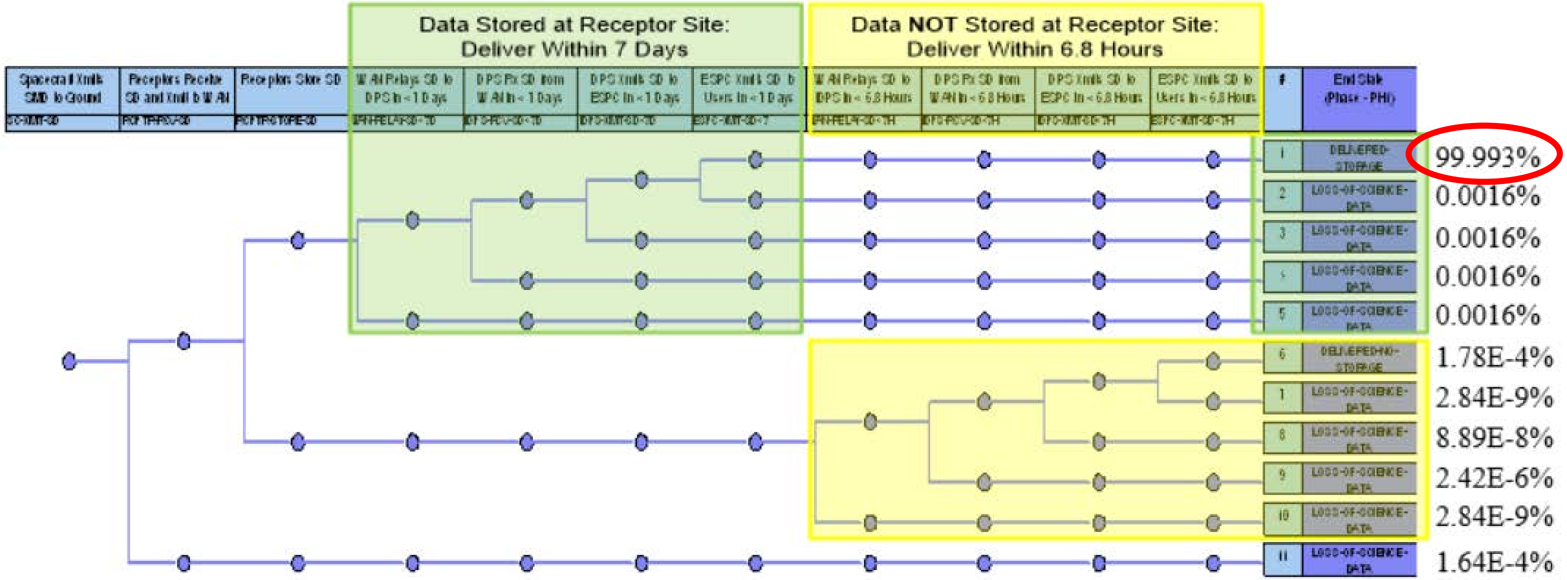
Run	MTBDE	MDT	MTBM
9912	316.8508	403.1492	3.911739
573	117.4191	62.58091	5.525604
2164	253.3123	106.6877	5.69241
5579	86.49955	33.50045	7.013477
6559	267.9833	92.01667	8.120707
7769	557.4377	162.5623	8.078807
6978	282.5626	77.43741	8.19022

Down Time	Events
403	1
250	4
213	2
201	6
184	2
163	1
155	2

- Results used to identify months with downtime exceeding memory capacity

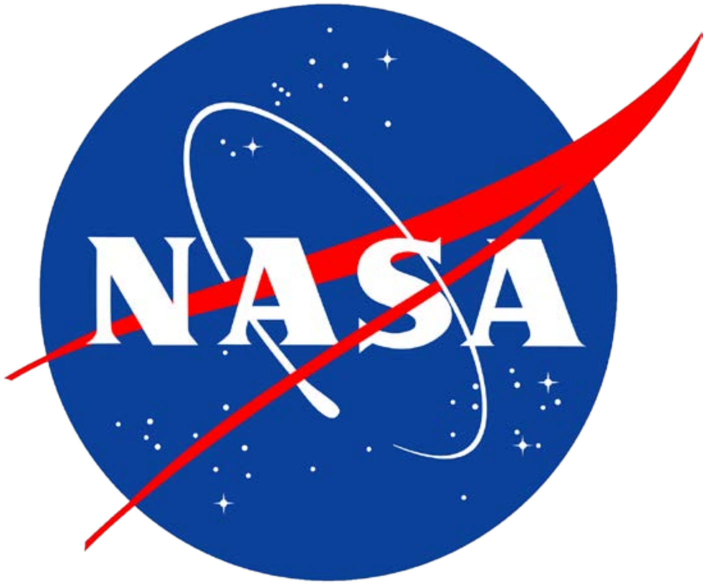
Data Availability Results





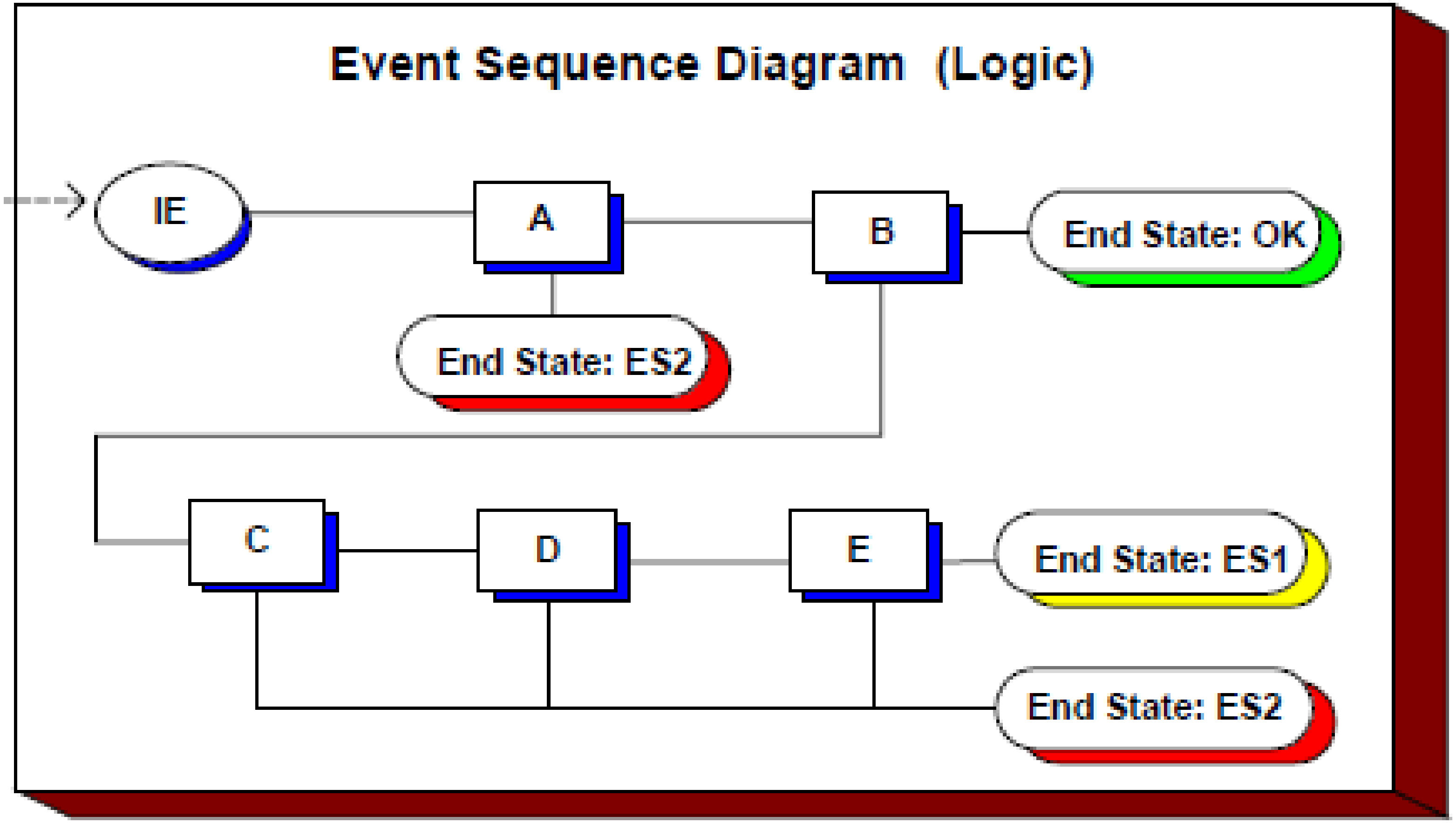
Lessons Learned

- Data Availability can be calculated using PRA.
- Monte Carlo results can be incorporated into Fault Tree / PRA.
- Raptor
  - Not designed to model storage.
  - Not designed to provide downing event durations by run.
- Use the right methodology for the analysis.
  - PRA may not be the best fit for every data availability calculation.
  - Monte Carlo simulation alone may be better.
  - Recharacterize requirements to not drive methodology choices.


NASA

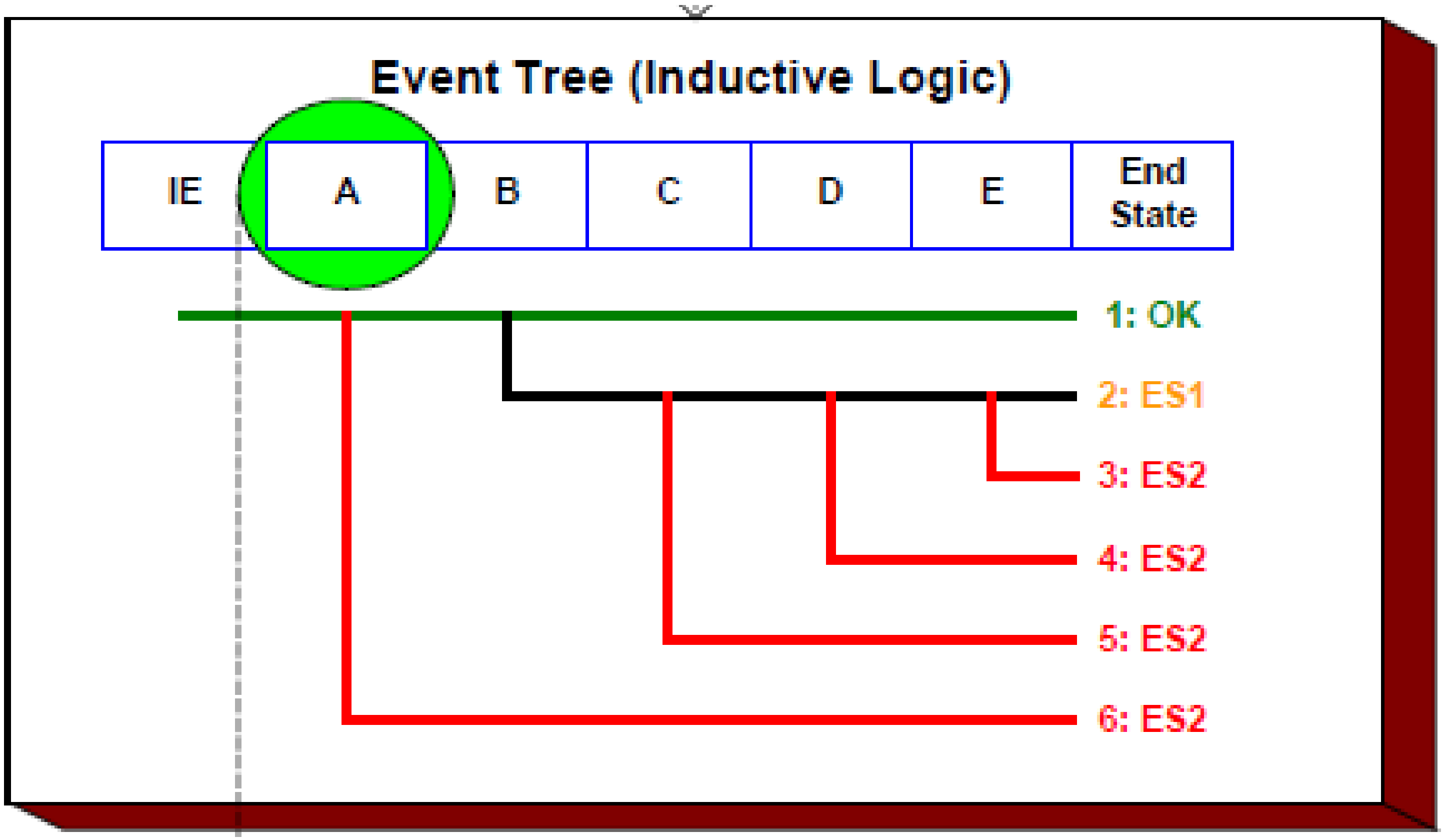
PRA Process

Event Sequence Diagram

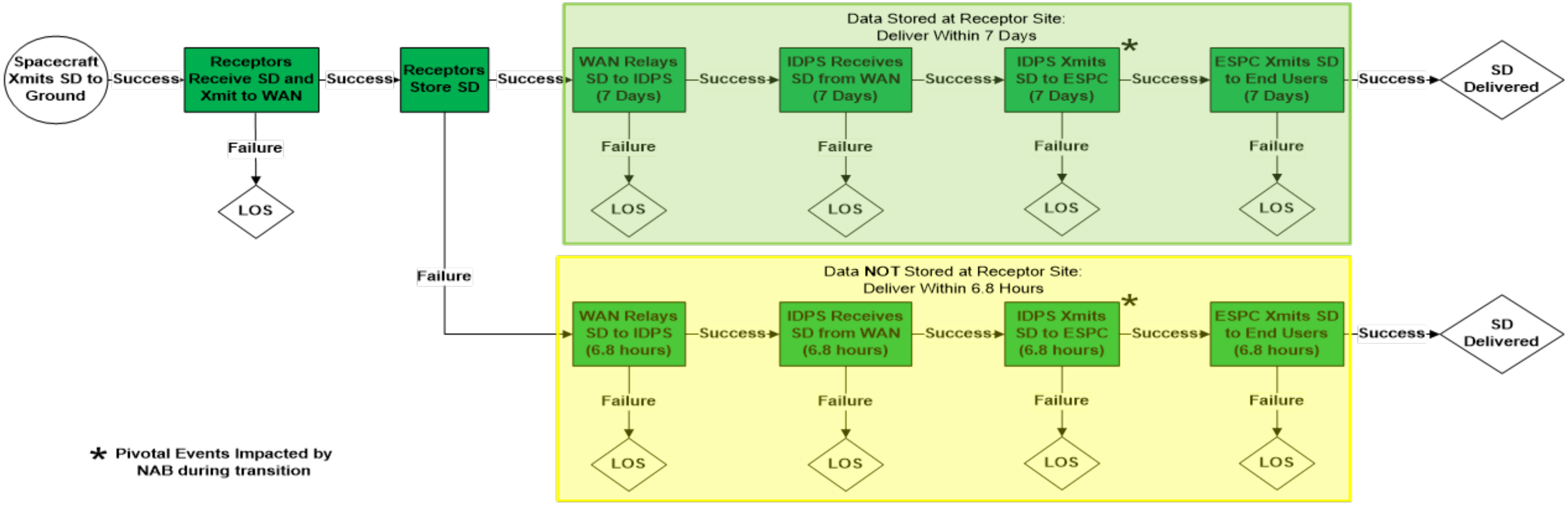


PRA Process

Event Tree

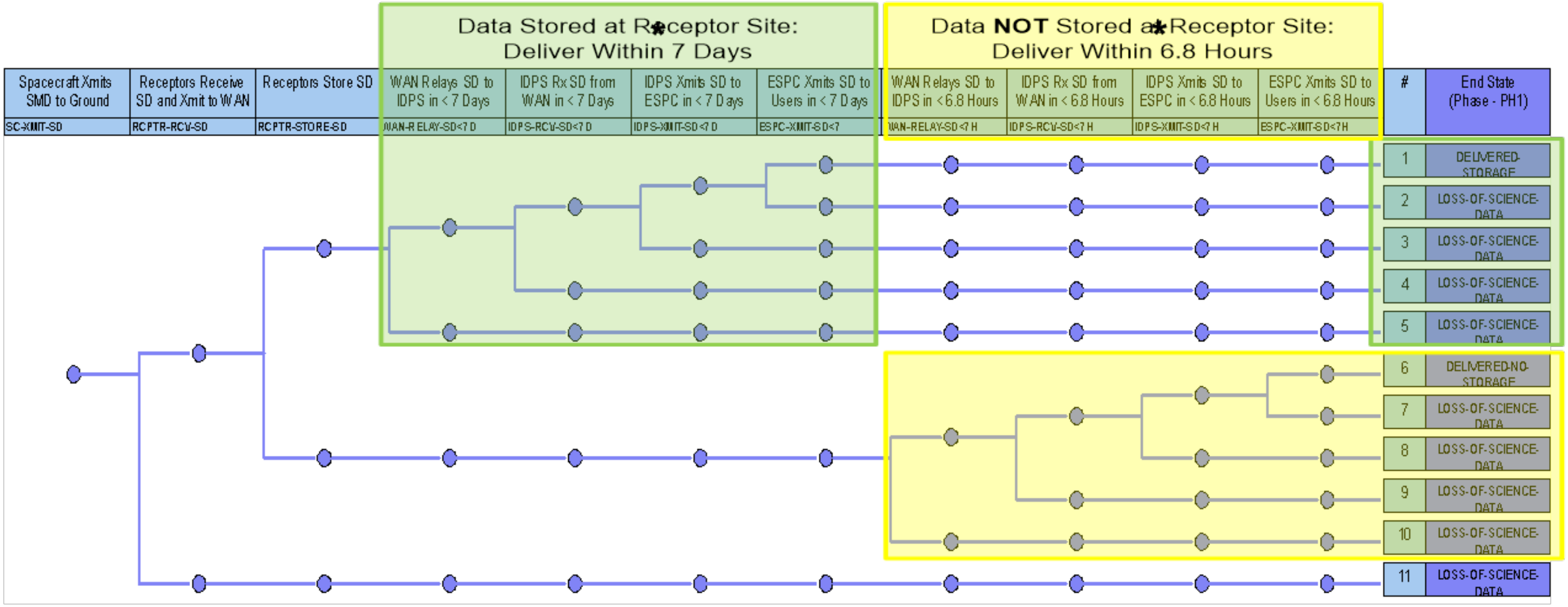


Event Sequence Diagram - Data


Spacecraft Xmits SD to Ground
Success
Receptors Receive SD and Xmit to WAN
Success
Receptors Store SD
Success
Failure
LOS
Failure
Data Stored at Receptor Site: Deliver Within 7 Days
WAN Relays SD to IDPS (7 Days)
Success
IDPS Receives SD from WAN (7 Days)
Success
IDPS Xmits SD to ESPC (7 Days)
*
Success
ESPC Xmits SD to End Users (7 Days)
Success
SD Delivered
Failure
LOS
Data NOT Stored at Receptor Site: Deliver Within 6.8 Hours
WAN Relays SD to IDPS (6.8 hours)
Success
IDPS Receives SD from WAN (6.8 hours)
Success
IDPS Xmits SD to ESPC (6.8 hours)
*
Success
ESPC Xmits SD to End Users (6.8 hours)
Success
SD Delivered
Failure
LOS
* Pivotal Events Impacted by NAB during transition

- Receptors Receive SD and Xmit
- Receptors Store SD [If successful, 7 Days to deliver; if not, 6.8 hours]
  - WAN Relays SD to IDPS (2)
  - IDPS Receives SD from WAN (2)
  - IDPS Xmits SD to ESPC (2)
  - ESPC Xmits SD to End Users (2)

Event Tree - Data



Data Stored at Receptor Site:
Deliver Within 7 Days

Data **NOT** Stored at Receptor Site:
Deliver Within 6.8 Hours

Spacecraft Xmits SMD to Ground	Receptors Receive SD and Xmit to WAN	Receptors Store SD	WAN Relays SD to IDPS in < 7 Days	IDPS Rx SD from WAN in < 7 Days	IDPS Xmits SD to ESPC in < 7 Days	ESPC Xmits SD to Users in < 7 Days	WAN Relays SD to IDPS in < 6.8 Hours	IDPS Rx SD from WAN in < 6.8 Hours	IDPS Xmits SD to ESPC in < 6.8 Hours	ESPC Xmits SD to Users in < 6.8 Hours	#	End State (Phase - PH1)
SC-XMIT-SD	RCPTR-RCV-SD	RCPTR-STORE-SD	WAN-RELAY-SD<7 D	IDPS-RCV-SD<7 D	IDPS-XMIT-SD<7 D	ESPC-XMIT-SD<7	WAN-RELAY-SD<7 H	IDPS-RCV-SD<7 H	IDPS-XMIT-SD<7 H	ESPC-XMIT-SD<7H		
											1	DELIVERED-STORAGE
											2	LOSS-OF-SCIENCE-DATA
											3	LOSS-OF-SCIENCE-DATA
											4	LOSS-OF-SCIENCE-DATA
											5	LOSS-OF-SCIENCE-DATA
											6	DELIVERED-NO-STORAGE
											7	LOSS-OF-SCIENCE-DATA
											8	LOSS-OF-SCIENCE-DATA
											9	LOSS-OF-SCIENCE-DATA
											10	LOSS-OF-SCIENCE-DATA
											11	LOSS-OF-SCIENCE-DATA

Monte Carlo Results

- Top Fault Tree Events

Event Description	Failure Probability	Basis
Troll Fails to Collect/FWD SD	23.90%	Model: 2390 / 10K months failed
Troll Fails to Collect/Store SD	23.51%	Model: 2351 / 10K months failed
Fairbanks Fails to Collect/FWD SD	19.08%	Model: 1908 / 10K months failed
Fairbanks Fails to Collect/Store SD	18.29%	Model: 1829 / 10K months failed
McMurdo Fails to Collect/FWD SD	11.67%	Model: 1167 / 10K months failed

- Top Event Tree Events

Event Description	Failure Probability	Basis
IDPS Rx SD from WAN in < 6.8 hours	1.36%	Model: 136 / 10K months failed
IDPS Xmits SD to ESPC in < 6.8 hours	0.05%	Model: 5 / 10K months failed
Loss of Command Generation > 7 Days	0.01%	Model: 1 / 10K months failed