PURDUE UNIVERSITY

Extra-terrestrial Habitat Systems: Safety, Reliability, and Resilience

Jory Lyons[1],
Dr. Amin Maghareh[2], Audai Theinat[2],
Dr. Shirley Dyke[2,3], Dr. Antonio Bobet[2]

[1] School of Aeronautics and Astronautics, Purdue University
[2] Lyles School of Civil Engineering, Purdue University
[3] School of Mechanical Engineering, Purdue University

RETH

SURF SUMMER UNDERGRADUATE RESEARCH FELLOWSHIPS

Purdue RETH Team

Faculty Members





Postdoctoral and Graduate Researchers




Undergraduate Researchers









purdue.edu/reth

Overview

- Introduction
  - Background and Motivation
  - Environmental Hazards
  - Design Approaches
- Methodology
  - Safety, Reliability, and Resilience
- Case Study
  - Model Rocket
  - Strengths, Weaknesses, Opportunities, Threats (SWOT) Analysis
- Conclusion

“Can you imagine living on the moon?”

Purdue RETH

Background & Motivation

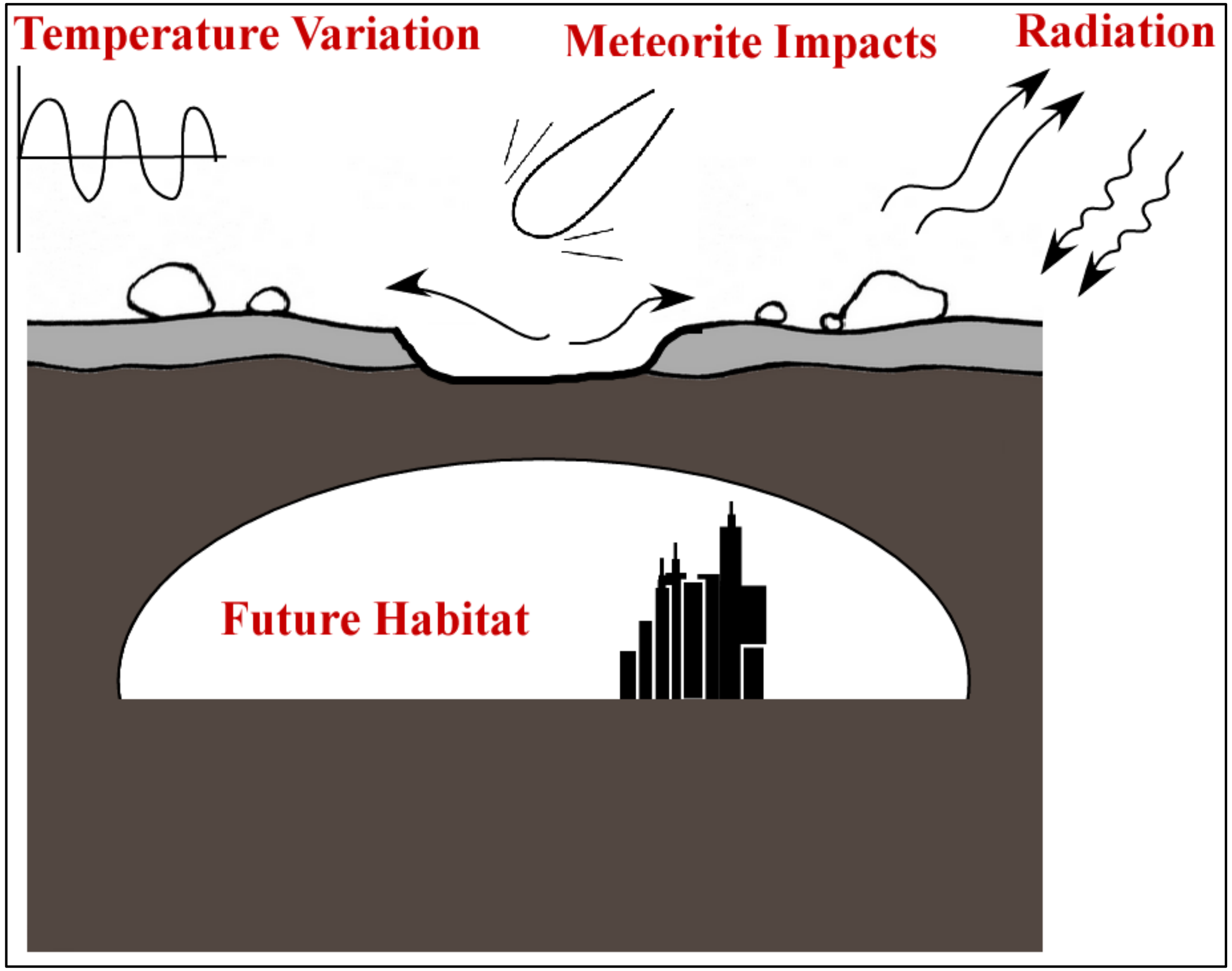
- Grand challenge to design resilient extraterrestrial habitats
  - Envision first Earth-independent human settlement
- Current risk-based techniques lack resilience
- Critiquing conventional reliability-based design
- Avoid catastrophic disasters
  - Apollo 1 fire
  - Space Shuttle failures

European Space Agency

PURDUE
UNIVERSITY

Environmental Hazards

- Temperature extremes
- Hypervelocity Meteoroids
- Radiation
- Moon-quakes
- Atmospheric Vacuum

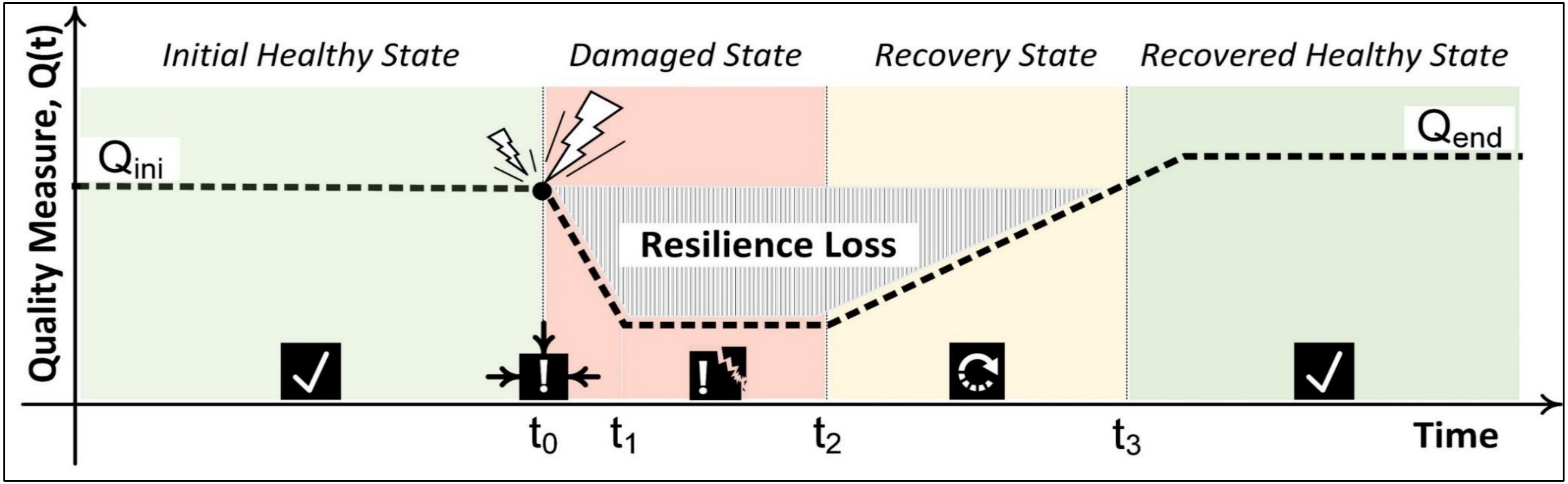


Purdue RETH

RETH

Proposed Approach: Resilience-based Design

- ability for system to absorb, recover, and adapt quickly from disruption without fundamental changes in function or sacrifices in safety



Purdue RETH

PURDUE UNIVERSITY

Current Approach: Reliability-based Design

*Simplified but lacks resilience

Severity		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Likelihood

Catastrophic	STOP
Unacceptable	URGENT ACTION
Undesirable	ACTION
Acceptable	MONITOR
Desirable	NO ACTION

http://blog.mindgenius.com/2011/04/risk-management-with-gordon-wyllie.html

RETH

Reliability-based vs Resilience-based

	Anticipation	Resistance	Adaptation	Recovery	Recovery Time
Resilience	✓	✓	✓	✓	✓
Reliability	✓	✓			
Redundancy	✓		✓	✓	
Robustness	✓	✓			
Reconfigurability			✓	✓	
Recoverability				✓	✓
Rapidity			✓		✓

Purdue RETH

Reliability-Based Approaches

- Failure Modes, Effects, and Criticality Analysis (FMECA)
  - Occurrence (O), Severity (S), Detection (D)
  - Risk Priority Number (RPN = O*S*D)
  - Criticality Number
- Probabilistic Risk Assessment (PRA)
  - Includes FMECA or FMEA
  - Fault Tree Analysis (FTA)
  - Event-sequence Diagram (ESD)

Stamatelatos, M. et al. (2011). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 10.13140/RG.2.2.18206.13122.

Reliability-Based Approaches – Differences

- Failure Modes, Effects, and Criticality Analysis (FMECA)
  - Helps tell which failures to fix and data to acquire

- Probabilistic Risk Assessment (PRA)
  - Uses FMECA and determines more failures and combinations
  - May include *partial* or full FMECA
  - Quantitative and qualitative

Stamatelatos, M. et al. (2011). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 10.13140/RG.2.2.18206.13122.

Criticality – FMECA

Identify and rank importance of component to system

Basic failure rate, λ_p

Failure mode ratio, α

Conditional probability of failure, β

Conditional probability of detection, υ

Mission phase duration, t

U.S. Department of Defense. (1980). MIL-STD-1629A, Procedures For Performing A Failure Mode, Effects and Criticality Analysis.

Model Rocket Case Study

Model Rocket Case Study – FMECA

Identification Number	Component Name	Component Function	Failure Mode(s)	Mission Stage	Failure Cause(s)	Failure Effects	Failure Detection Method	Occurrence Index (O)	Severity Index (S)	Detection Index (D)	Risk Priority Number (O)*(S)*(D)
1	Parachute	Landing	Deployment failure	Landing	Stuck / jammed	Unrecoverable rocket	**None**	**4**	**5**	**5**	**100**

Model Rocket Case Study – FMECA

Identification Number	Component Name	Component Function	Failure Mode(s)	Mission Stage	Failure Cause(s)	Failure Effects	Failure Detection Method	Occurrence Index (O)	Severity Index (S)	Detection Index (D)	Risk Priority Number (O)*(S)*(D)
1	Parachute	Landing	Deployment failure	Landing	Stuck / jammed	Unrecoverable rocket	**None**	**4**	**5**	**5**	**100**

Identification Number	Data Source	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ_p)	Conditional Probability of Detection	Operating Time (t) (sec)	Criticality Number	Total Item Criticality	Damage Mode	Damage Effects	Remarks
1	**Estimate**	1.000	0.900	**0.01**	1.00	1	0.009	0.024	Use	More probable	Need backup

PURDUE
UNIVERSITY

Model Rocket Case Study – FMECA

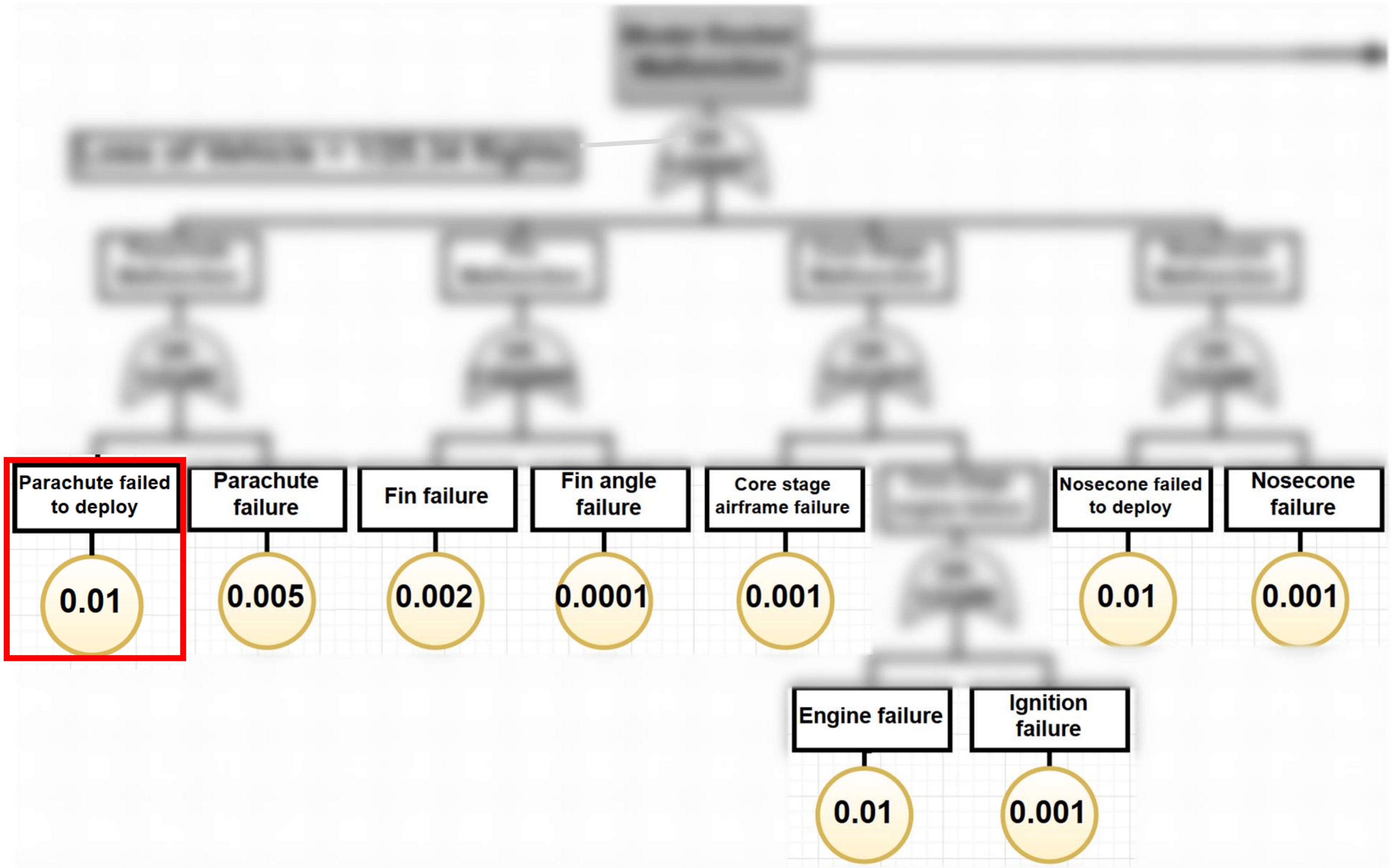
Identification Number	Component Name	Component Function	Failure Mode(s)	Mission Stage	Failure Cause(s)	Failure Effects	Failure Detection Method	Occurrence Index (O)	Severity Index (S)	Detection Index (D)	Risk Priority Number (O)*(S)*(D)
1	Parachute	Landing	Deployment failure	Landing	Stuck / jammed	Unrecoverable rocket	None	4	5	5	100

Identification Number	Data Source	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ_p)	Conditional Probability of Detection	Operating Time (t) (sec)	Criticality Number	Total Item Criticality	Damage Mode	Damage Effects	Remarks
1	Estimate	1.000	0.900	**0.01**	1.00	1	0.009	0.024	Use	More probable	Need backup

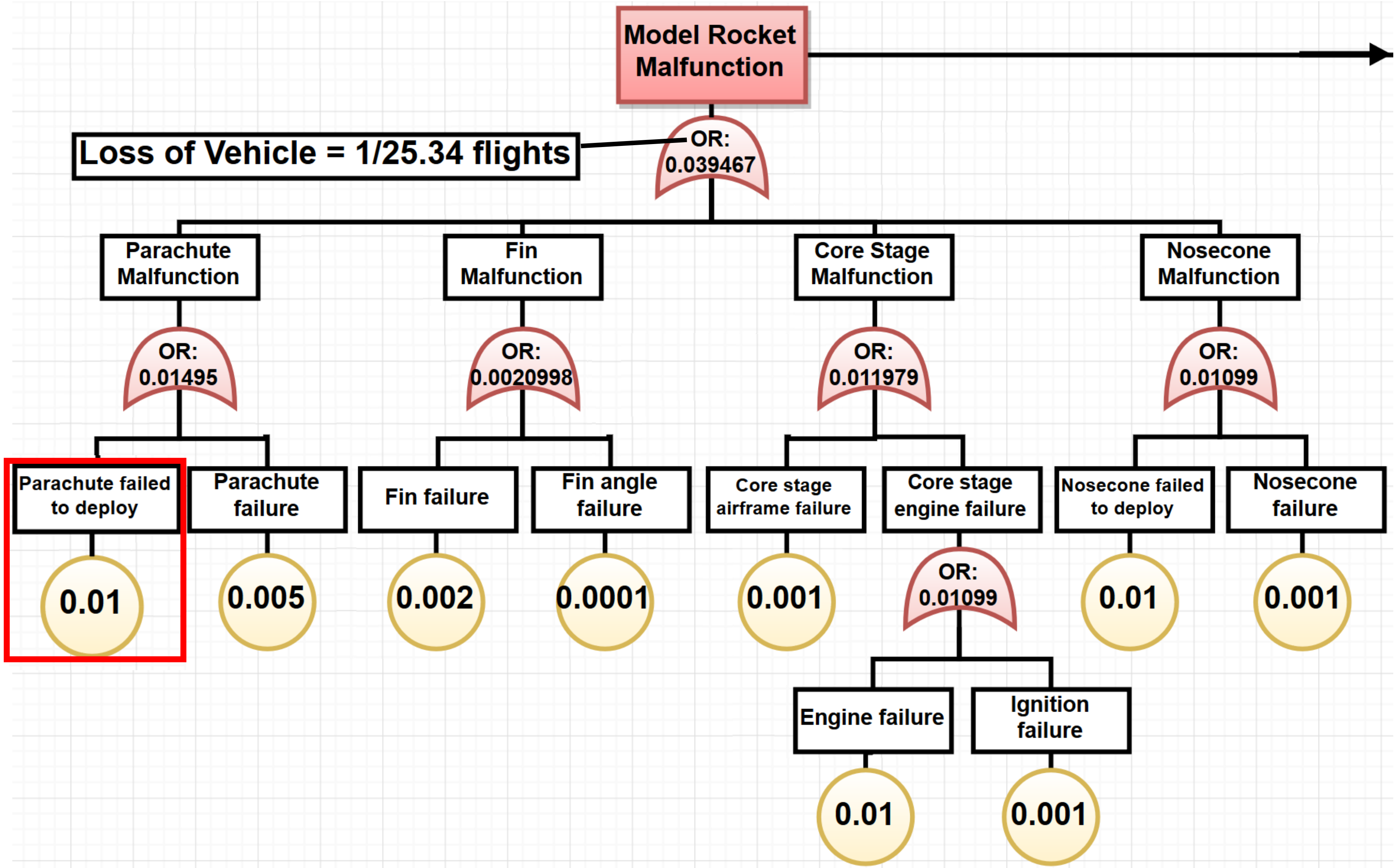
RETH

Model Rocket Fault Tree Analysis (FTA)

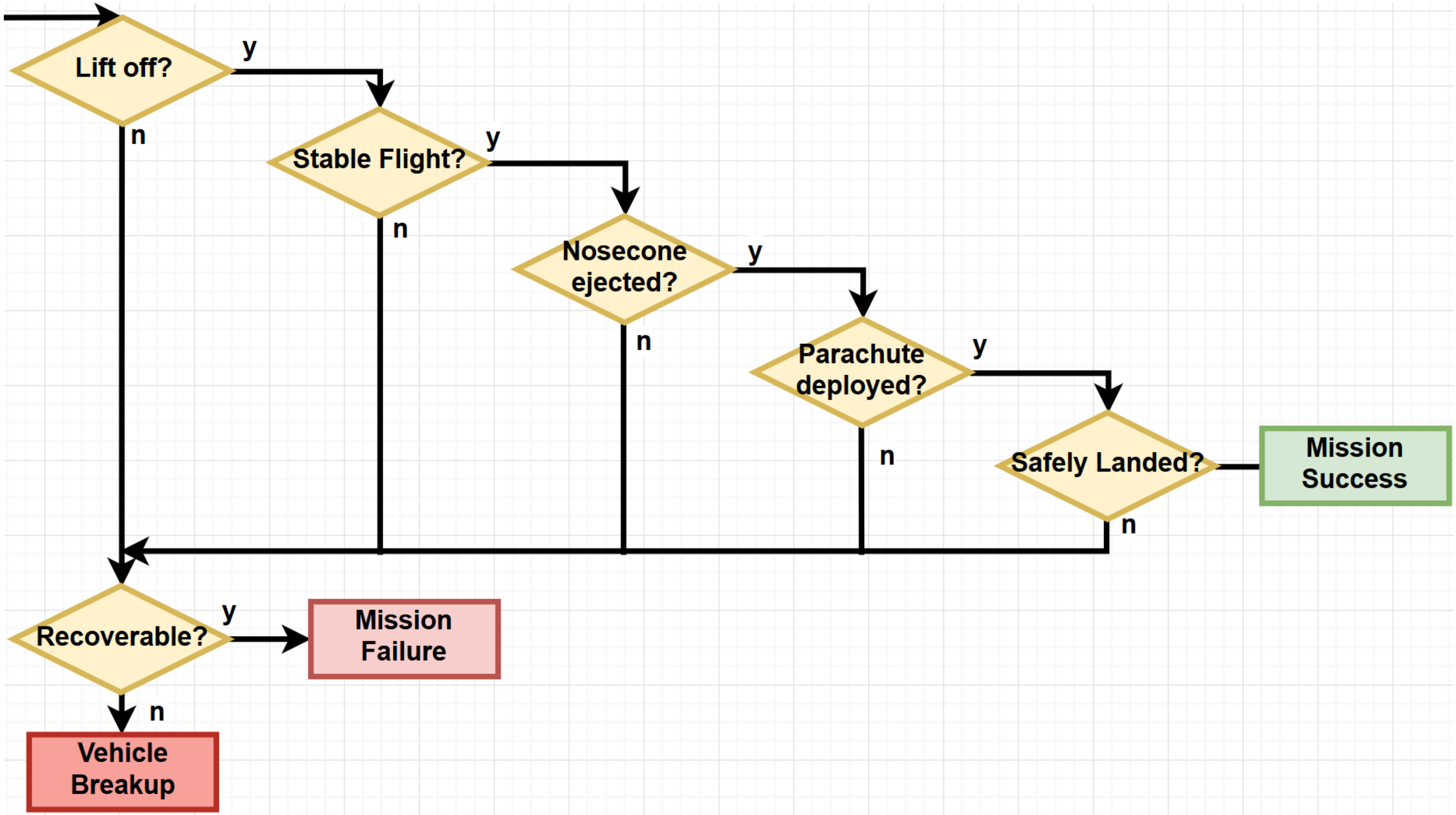
Model Rocket Fault Tree Analysis (FTA)



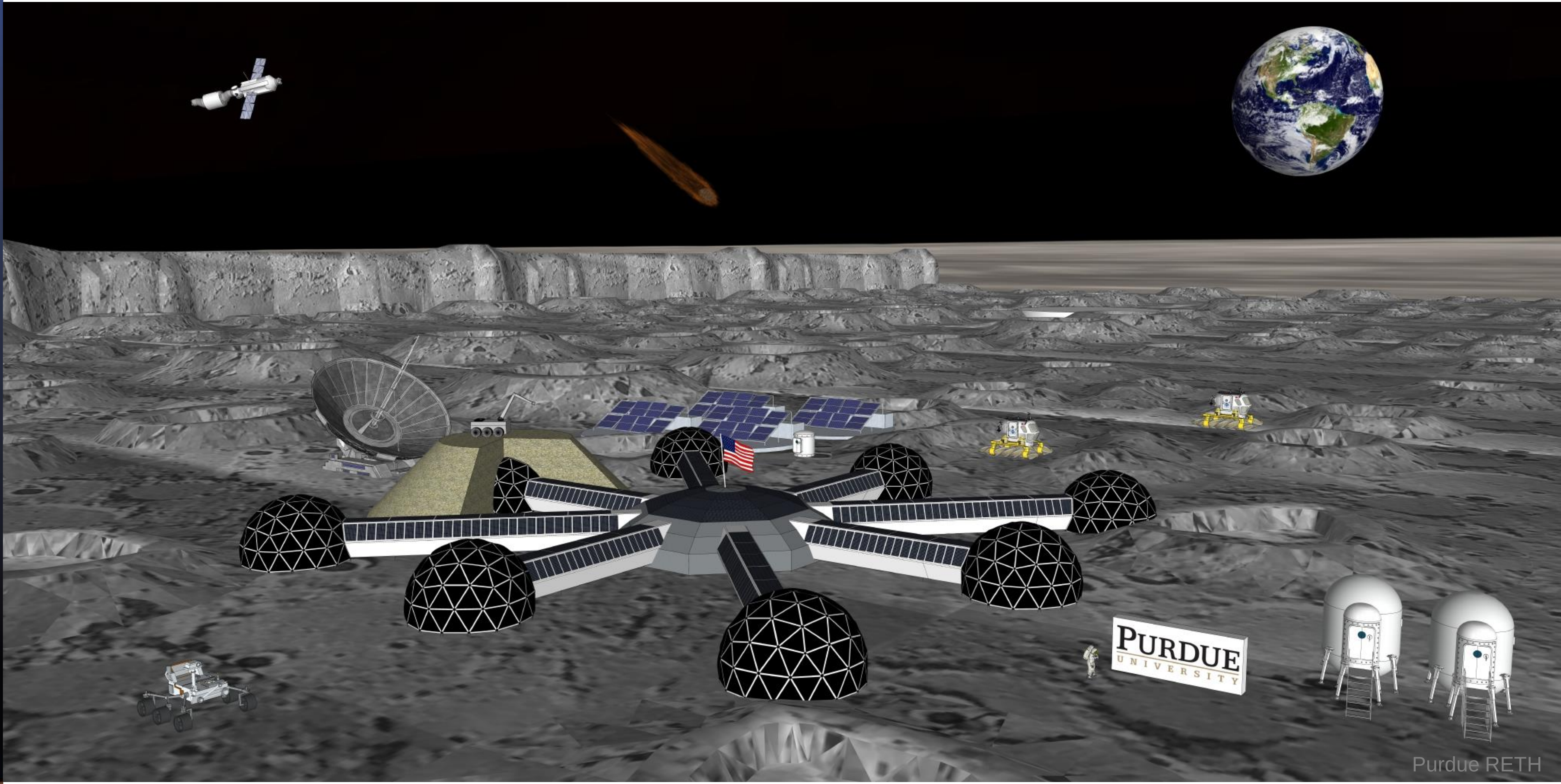
Model Rocket Fault Tree Analysis (FTA)



Event-sequence Diagram (ESD)



Resilient Extra-terrestrial Habitat



Reliability-based Design (FMECA/PRA) Analysis

Strengths

- Proven to be effective to determine quantitative and qualitative risks
- Accounts for catastrophic failure and hazards

Weaknesses

- Lacks adaptability and recoverability
- Inapplicable to cope with unknown hazards
- May require experts and require identification of rare hazards mixtures

Opportunities

- Can determine system interdependencies
- Can be improved/incorporated in resilience framework

Threats

- May ignore some system failure modes
- May not be feasible for complex systems

Conclusions

- Investigated reliability and resilience-based design
- FMECA and PRA
  - Create partial system resilience
  - Can be incorporated in RETH resilience-based framework
- Make living safer and more sustainable
  - Resilience is the key to have safe permanent habitats

INTERNATIONAL RETH WORKSHOP

OCTOBER 22nd - 23rd 2018

Thank You

Purdue.edu/reth

lyons41@purdue.edu

References

Stamatelatos, Michael & Dezfuli, Homayoon & Apostolakis, G & Everline, Chester & Guarro, Sergio & Mathias, Donovan & Mosleh, Ali & Paulos, Todd & Riha, David & Smith, Curtis & Vessely, William & Youngblood, Robert. (2011). Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 10.13140/RG.2.2.18206.13122.

Stamatis, D. H. (2003). Failure Mode and Effect Analysis, 2nd edition. ASQ Quality Press, Milwaukee, WI, ISBN 0-87389-598-3. Retrieved May 25, 2018, from http://www.qualitypress.asq.org

U.S. Department of Defense. (1980). MIL-STD-1629A, Procedures For Performing A Failure Mode, Effects and Criticality Analysis.

Back-Up Slides

Purdue.edu/reth
lyons41@purdue.edu

FMECA – MIL-STD-1629A

FAILURE MODE EFFECTS AND CRITICALIN ANALYSIS - MAINTAINABILITY INFORMATION

SYSTEM/SUBSYSTEM NOMENCLATURE	SYSTEM IDENTIFICATION NUMBER		DATE:	PREPARED BY:
INDENTURE LEVEL	REFERENCE DRAWING	MISSION	SHEET ___ OF ___	APPROVED BY:
SYSTEM/SUBSYSTEM DESCRIPTION			COMPENSATING PROVISIONS	

ITEM IDWT NO.	ITEM NOMENCLATURE	FUNCTION		FUNCTIONAL FAILURE		ENGINEERING FAILURE MODE		MISSION PHASE	FAILURE EFFECTS			FAILURE DETECTION METHOD	SEVERITY CLASS	MINIMUM EQUIPMENT LIST	ENGINEERING FAILURE MODE MTBF AND REMARKS
		NO.		LTR		NO.			LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

DAMAGE MODE AND EFFECTS ANALYSIS

SYSTEM ____________

INDENTURE LEVEL ____________

REFERENCE DRAWING ____________

MISSION ____________

DATE ____________

SHEET ______ OF ______

COMPILED BY ____________

APPROVED BY ____________

U.S. Department of Defense. (1980). MIL-STD-1629A, Procedures For Performing A Failure Mode, Effects and Criticality Analysis.

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS.	DAMAGE MODE	DAMAGE EFFECTS			REMARKS
							LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS	

RETH

Model Rocket Case Study – FMECA

Identification Number	Component Name	Component Function	Failure Mode(s)	Mission Stage	Failure Cause(s)	Failure Effects	Failure Detection Method	Occurrence Index (O)	Severity Index (S)	Detection Index (D)	Risk Priority Number (O)*(S)*(D)
1	Parachute	Landing	Deployment failure	Landing	Stuck/jammed	Unrecoverable rocket	None	4	5	5	100
2			Break	Landing	Low strength, loose	Unrecoverable rocket	None	3	5	5	75
3	Fin	Stability	Angle/position misalignment	Mission	Loose, bad manufacturing	Off-course, unrecoverable rocket	Before launch inspection	3	3	2	18
4			Break	Flight	Low strength, loose	Off-course, unrecoverable rocket	None	1	4	5	20
5	Core Stage	Structure	Break	Mission	Low strength, loose	Unrecoverable rocket	None	1	5	5	25
6	Engine	Propulsion	Ignition failure	Flight	Faulty, wet	None, unrecov-erable rocket	Before launch inspection	3	2	2	12
7			Explode	Flight	Faulty, broken	Unrecoverable rocket	None	2	5	5	50
8	Nosecone	Aerodynamics	Deployment failure	Landing	Stuck/jammed	Unrecoverable rocket	None	4	5	5	100
9			Break	Mission	Low strength	Unrecoverable rocket	None	2	5	5	50

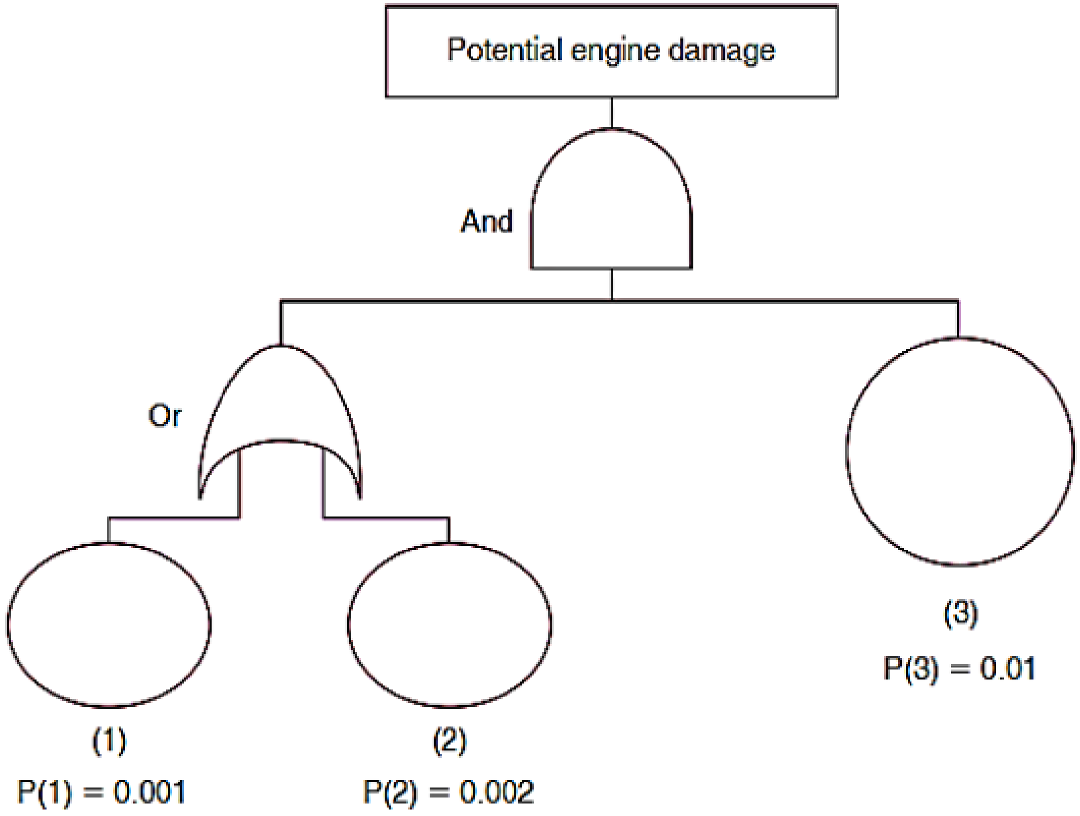
Model Rocket Case Study – FMECA

Identification Number	Data Source	Failure Effect Probability (β)	Failure Mode Ratio (α)	Failure Rate (λ_p)	Conditional Probability of Detection	Operating Time (t) (sec)	Criticality Number	Total Item Criticality	Damage Mode	Damage Effects	Remarks
1	Estimate	1.000	0.900	0.01	1.00	1	0.009	0.024	Use	More probable	Need backup
2	Estimate	1.000	0.100	0.005	1.00	30	0.015		Use/age	More probable	
3	Estimate	0.500	0.200	0.002	1.00	40	0.008	0.0084	Use	More probable	
4	Estimate	0.500	0.800	0.0001	1.00	10	0.0004		Use	More probable	
5	Estimate	1.000	1.000	0.001	1.00	40	0.04	0.04	Use	More probable	
6	Estimate	0.200	0.300	0.01	1.00	1	0.0006	0.0076	Use/age	More probable	Need better detection
7	Estimate	1.000	0.700	0.001	1.00	10	0.007		Use/age	More probable	
8	Estimate	1.000	0.700	0.01	1.00	1	0.007	0.019	Use	More probable	Lubricate or loosen
9	Estimate	1.000	0.300	0.001	1.00	40	0.012		Use	More probable	

$$C_m = (v)\lambda_p \alpha \beta t$$

$$C_r = \sum_{n=1}^{n} (C_m)_n$$

Fault Tree Analysis (FTA)



Using the formula for reliability of a parallel system,

$$R_{sys} = 1 - [(1-R3)(1-R1 \times R2)]$$

where $R_{1\&2}$ = Reliability of Elements 1 and 2 in series.

Therefore,

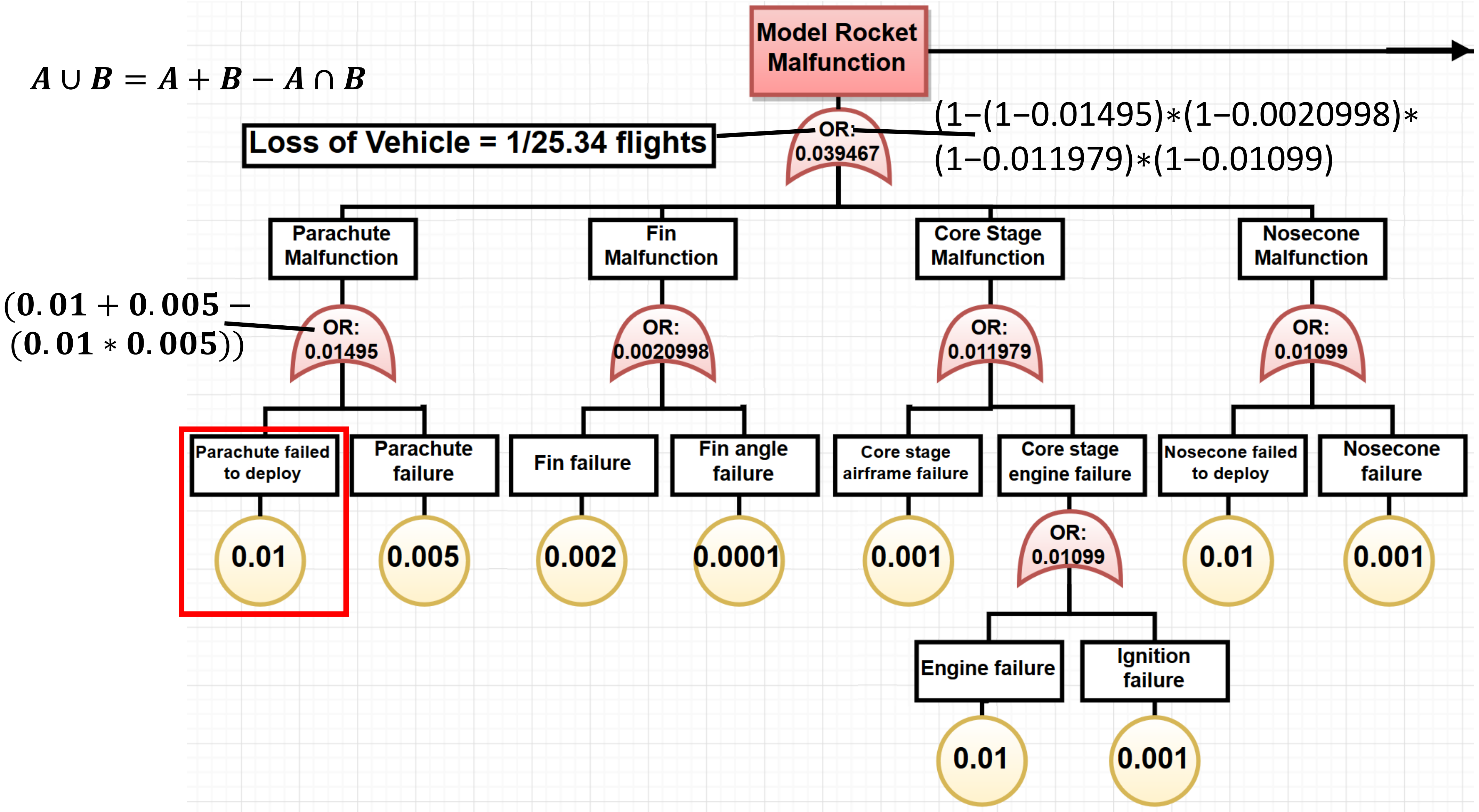
$$\begin{aligned} R_{sys} &= 1 - [(1-R3)\,(1-R1 \times R2)] \\ &= 1 - [(1-.99)\{1-(.999)(.998)\}] \\ &= 1 - [(.01)(1-.997002)] \\ &= 1 - [(.01)(.002998)] \\ &= 1 - .00002998 \\ &= 0.99997002 \end{aligned}$$

Probability of damage, $P(D) = 1 - R_{sys} = .00002998$ or approximately .0003.

Stamatis, D. H. (2003). Failure Mode and Effect Analysis, 2nd edition. ASQ Quality Press, Milwaukee, WI, ISBN 0-87389-598-3. Retrieved May 25, 2018, from http://www.qualitypress.asq.org

Model Rocket Fault Tree Analysis (FTA)

$A \cup B = A + B - A \cap B$



RETH Risk Analysis (FMECA and PRA) Results

Strengths

Proven to be effective to determine quantitative and qualitative risks

- Probabilistic
- Determines required data
- Significantly developed
- Capable of utilizing all data
- Past use allows less effort and brainstorming

Accounts for catastrophic failure and hazards

- Determines single-points failures
- Determines small failures and cascading effects
- Helps improve systems (of systems)

Weaknesses

Lacks adaptability and recoverability

Inapplicable to cope with unknown hazards

- Not deterministic

May require experts and requires identification of rare hazards mixtures

- Simplifications ignore combined failures
- Takes great effort and time
- FMECA necessitates team to brainstorm

Opportunities

Can determine system interdependencies

- Can use criticality more within FTA
- Can use nonbinary logic and fragility curves
- Conditional probability of detection
- Determine more cascading effects

Can be improved/incorporated in resilience framework

- Can consider modularity to be resilient
- Efficiency in decision matrix/FMECA
- Can be easily changeable with advanced analysis

Threats

May ignore some system failure modes

Scrutiny if unexpected catastrophic failure

- May not determine particular cascading effects

May not be feasible for complex systems

- May prove expensive
- Requires instrumentation and time