



33rd Annual **INCOSE**
international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023



Paper #220

Complex System Reliability Analysis using a Model-Based Shared Systems Simulation

Jeremy Ross

Research Engineer, Ford Motor Company

Adjunct Professor, University of Detroit Mercy

17 July - 2023

www.incose.org/symp2023 #INCOSEIS

Blast from the Past Space Shuttle

Reliability Target

97% Probability of Success for **100 flights** per Orbiter ^[1]

99.9% per Launch Success Rate

Resources

\$ 209 Billion in 2010 dollars ^[2]

 **12 Years** RFP to Launch ^[1]



Observed per Launch Reliability: 98.5%



Lessons

Wicked problems require more than just resources to solve.

The beginning is the most important part of the work.

– *Plato*



Today's System Landscape

Complexity + Interdependency + Responsibility



Image: University of Sterling [5]



Image: B. Marr & Co. [6]

Reliability Analysis Goals

- ▶ Supplement detailed reliability analysis approaches
- ▶ Support early program tradeoff decisions
- ▶ Characterize and simulate emergent system attributes
- ▶ Leverage and reuse existing model-based resources

Agenda

- ▶ Reliability Definition
- ▶ Current Approaches
- ▶ Shared Systems Simulation Methodology
- ▶ Case Study: Mars Exploration Ice Mapper Orbiter
 - Simulation Development
 - Reliability Analysis
- ▶ Modeling the Complexity Resilience Tradeoff

Reliability Definition

“ ... the proper functioning of a system during its expected life under the full range of conditions experienced in the field. ”

— *INCOSE Systems Engineering Handbook* ^[7]

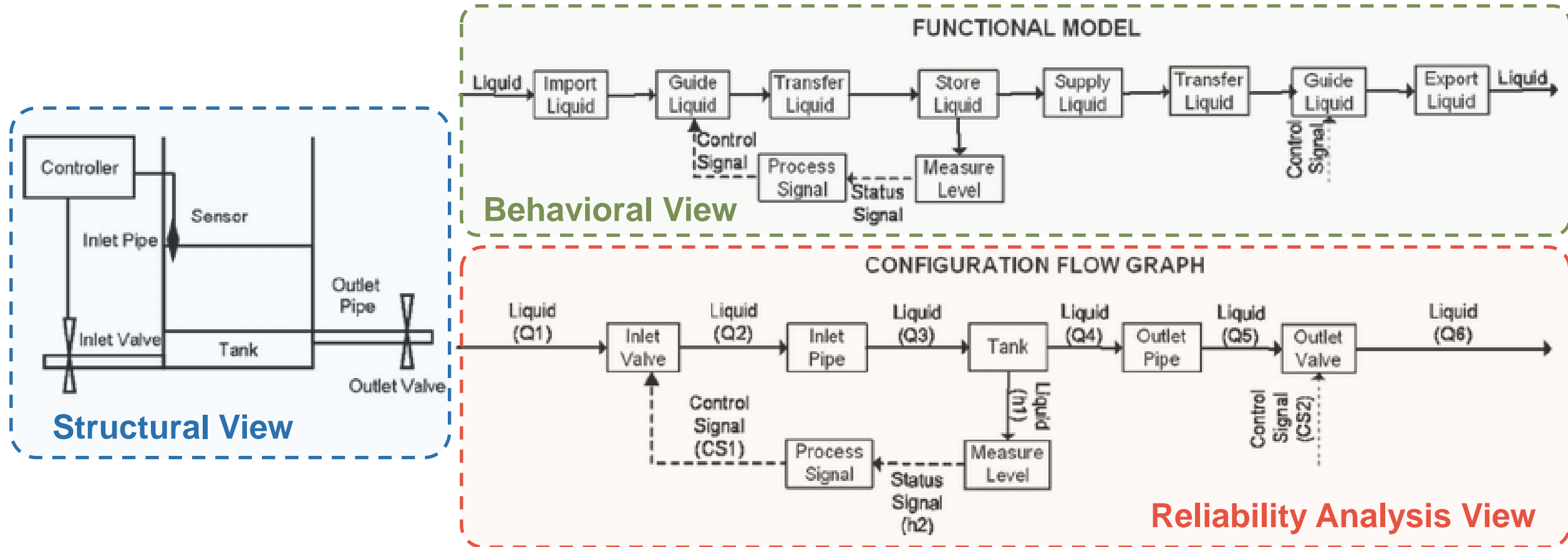
“ The probability a system will perform a required function for a given period of time. ”

— *Practical Reliability Engineering*, O'Connor and Kleyner ^[8]

Current Reliability Assessment Methods

- ▶ Three main assessment and fault management methods
 - FMEA, Fault Tree Analysis, Probability Risk Assessment ^{[9],[10]}
- ▶ Utilize a **Failure-Based Perspective**
 - Requires detailed element definition ^[10]
- ▶ **Function-Based Methods** offer an alternative
 - Reliability assessed based on element behavior
 - Enables analysis prior to detailed system element definition
 - Current approaches favor graph-based models

Configuration Flow Graph (CFG)



Configuration Flow Graph example for a notional "hold-up tank" system.

From "A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems", T. Kortoglu and I. Tumer, 2008. ^[10]

How the Coupled Reliability Analysis Differs

- ▶ Leverages existing model-based architecture definition
- ▶ Maintains a single ASOT for function and reliability definition

Note:

- ▶ This paper assessed reliability performance but did not consider other attributes like Cost and Timing

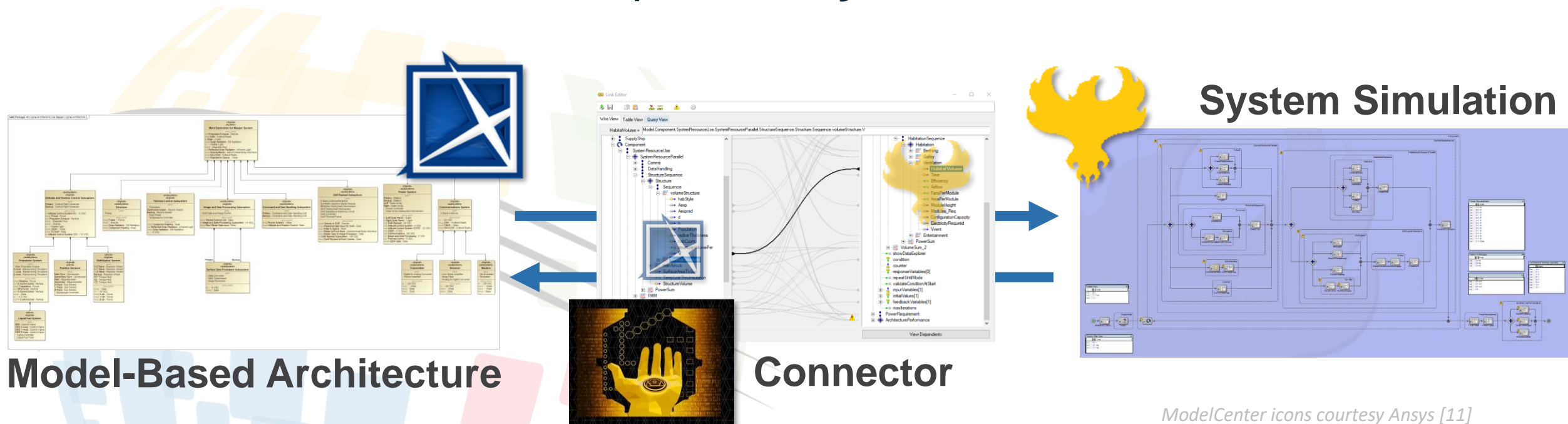
Shared Systems Simulation Methodology

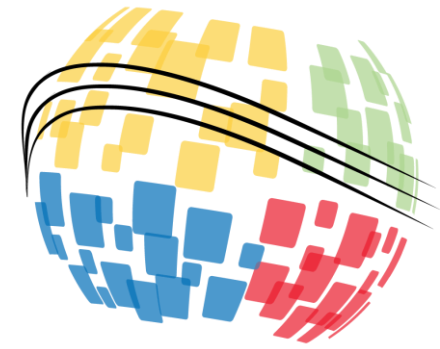
Step 1: **Architecture Definition**

↳ Step 2: **Simulation Development**

↳ Step 3: **Architecture to Simulation Coupling**

↳ Step 4: **Analysis**





Architecture Definition

System of Interest Mars Exploration Ice Mapper

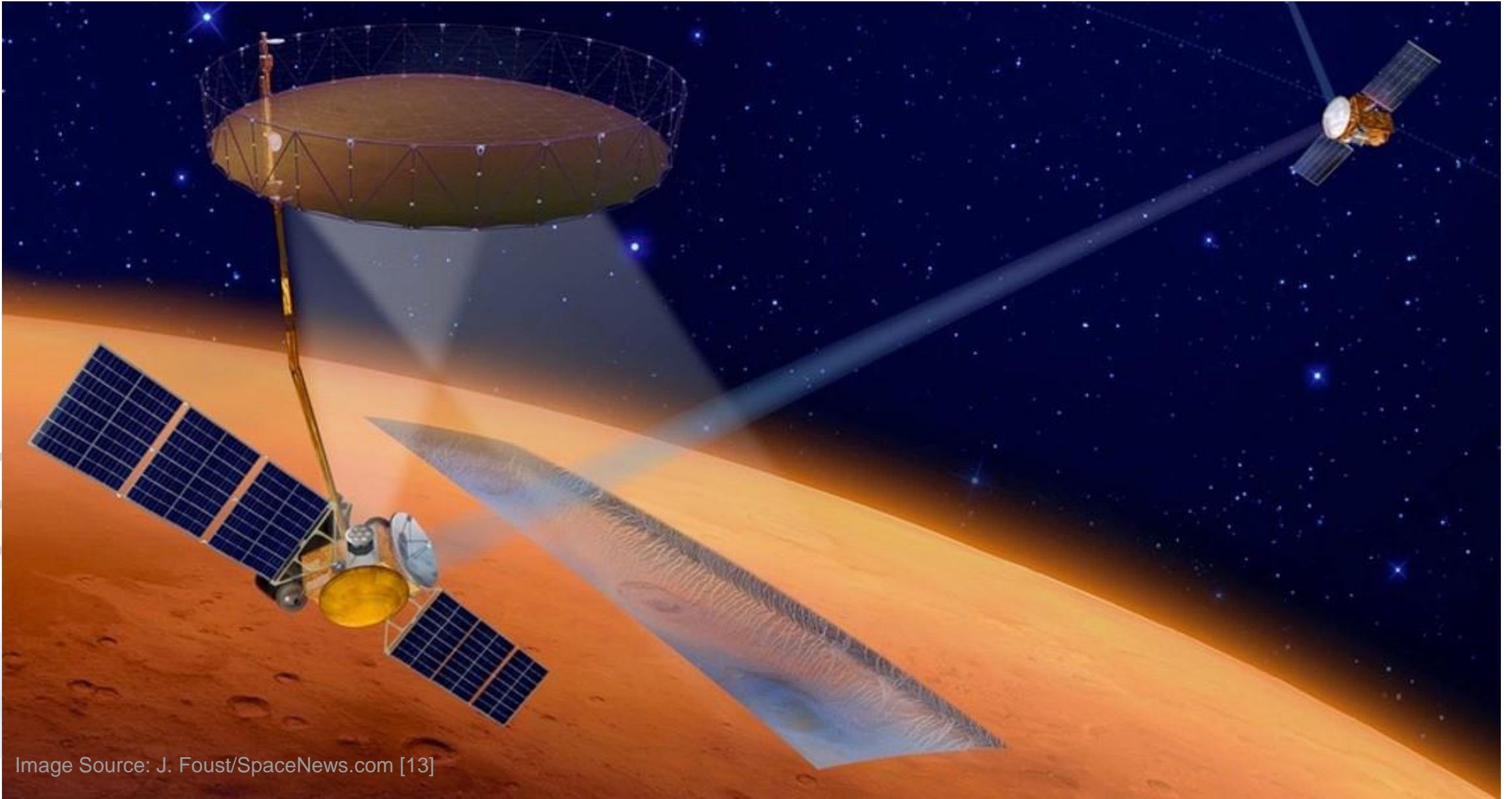
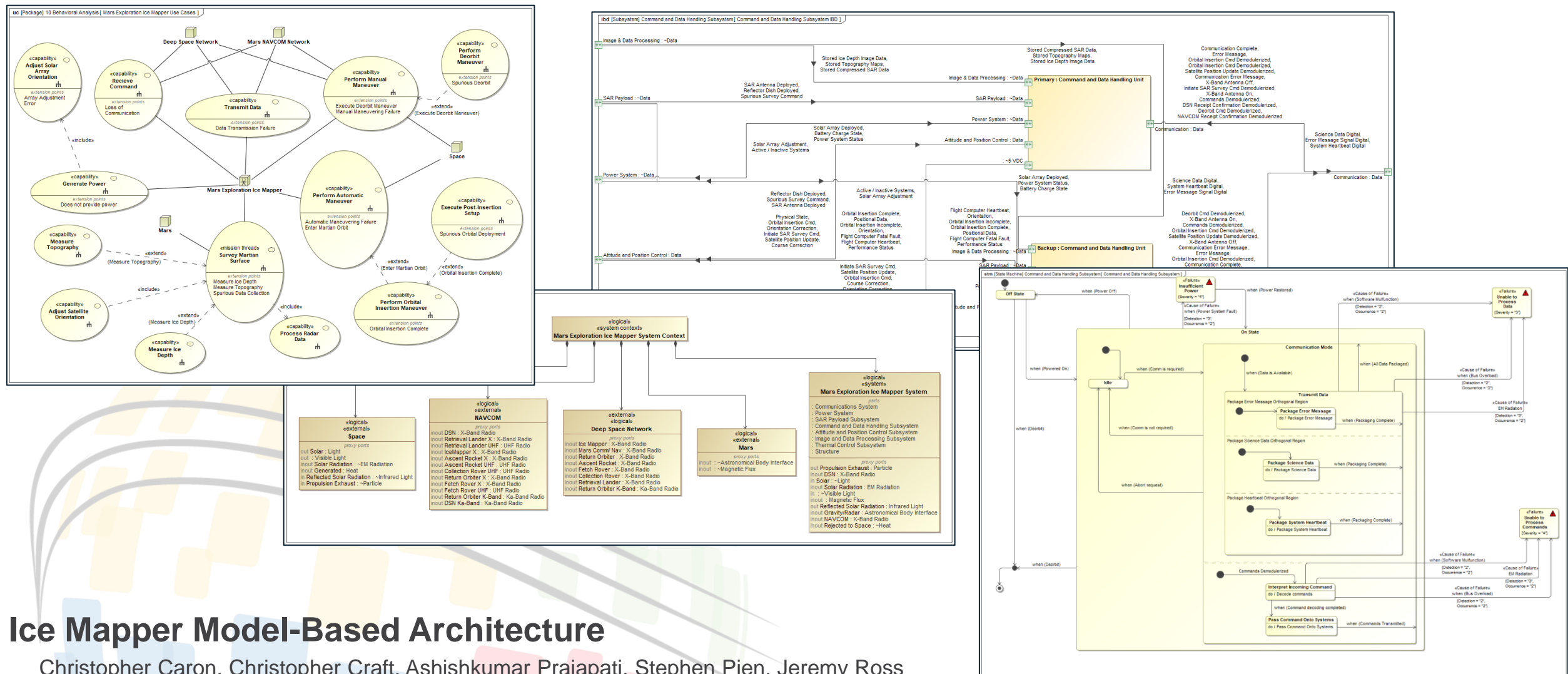
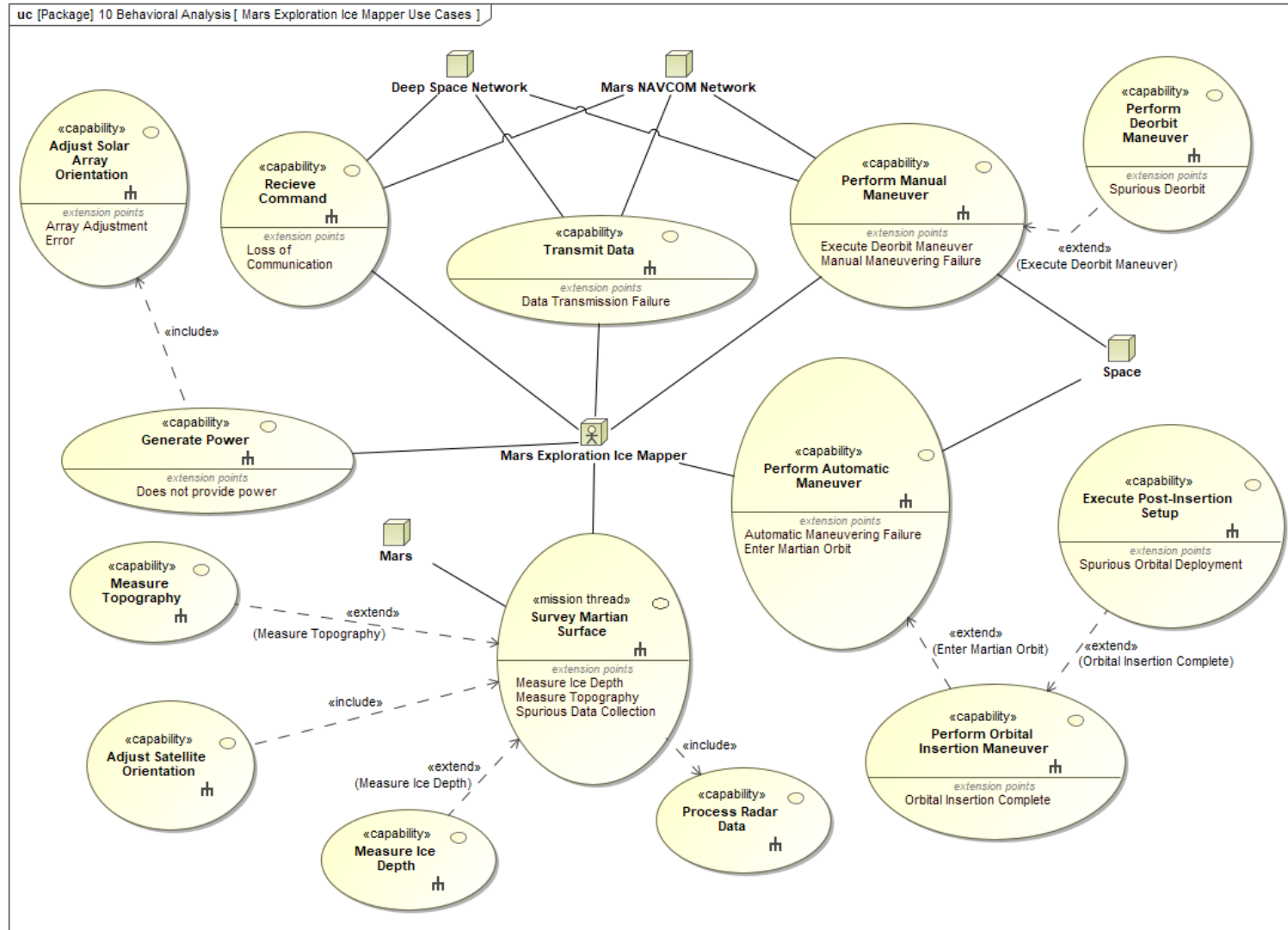


Image Source: J. Foust/SpaceNews.com [13]

Architecture Model Development



Simulation Scoping Subsystem of Interest

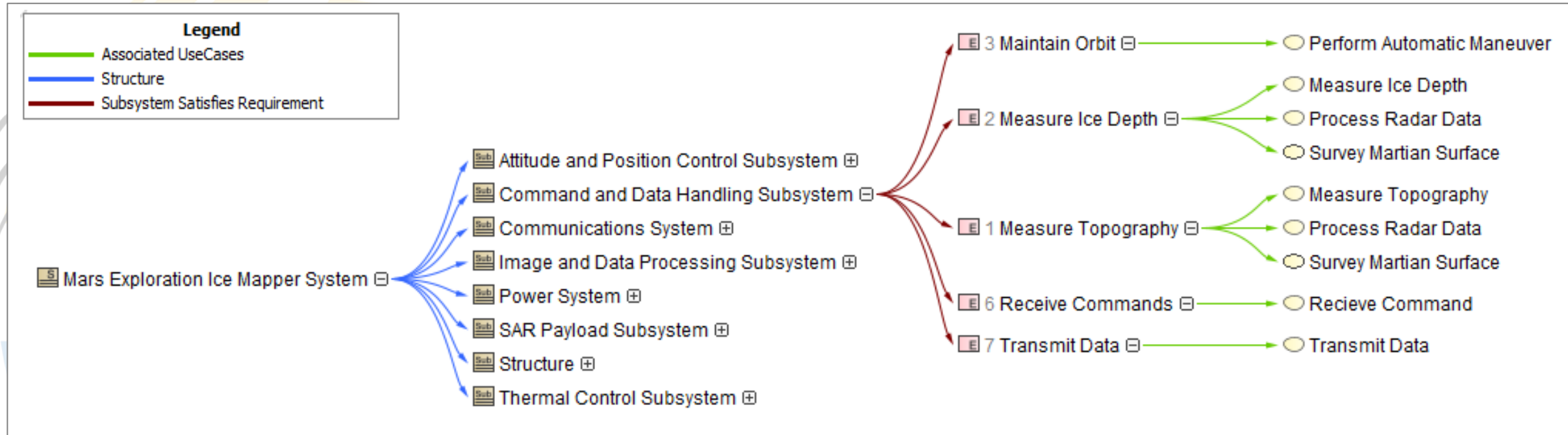
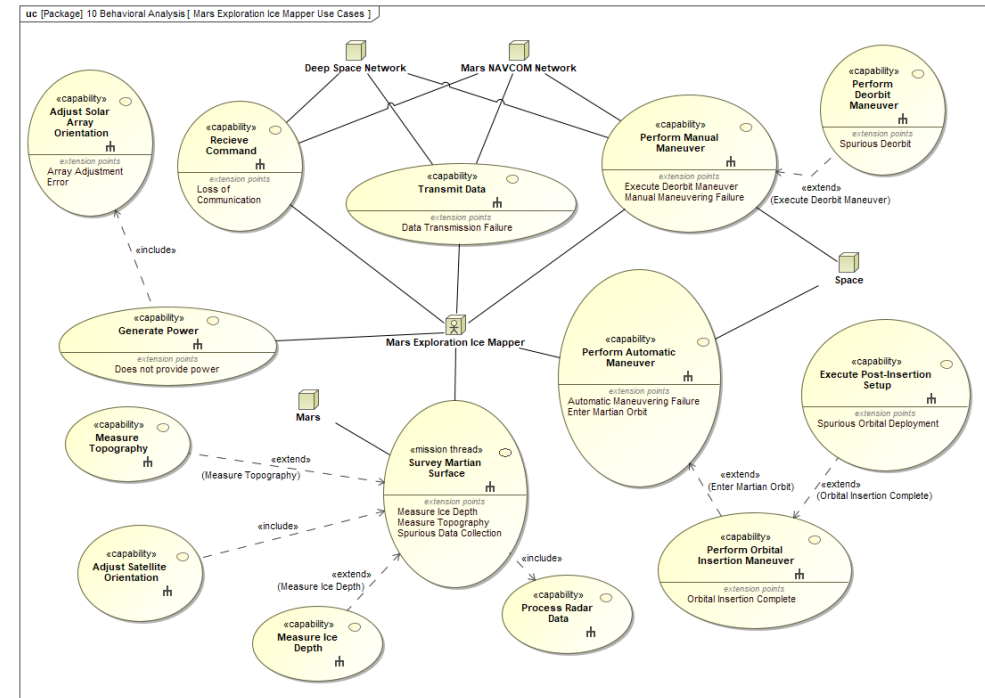


CTX: *Critical to X* Subsystem

- Reliability assessment focused on one subsystem
- Model-based architecture analyzed to determine highest-impact subsystem

Simulation Scoping

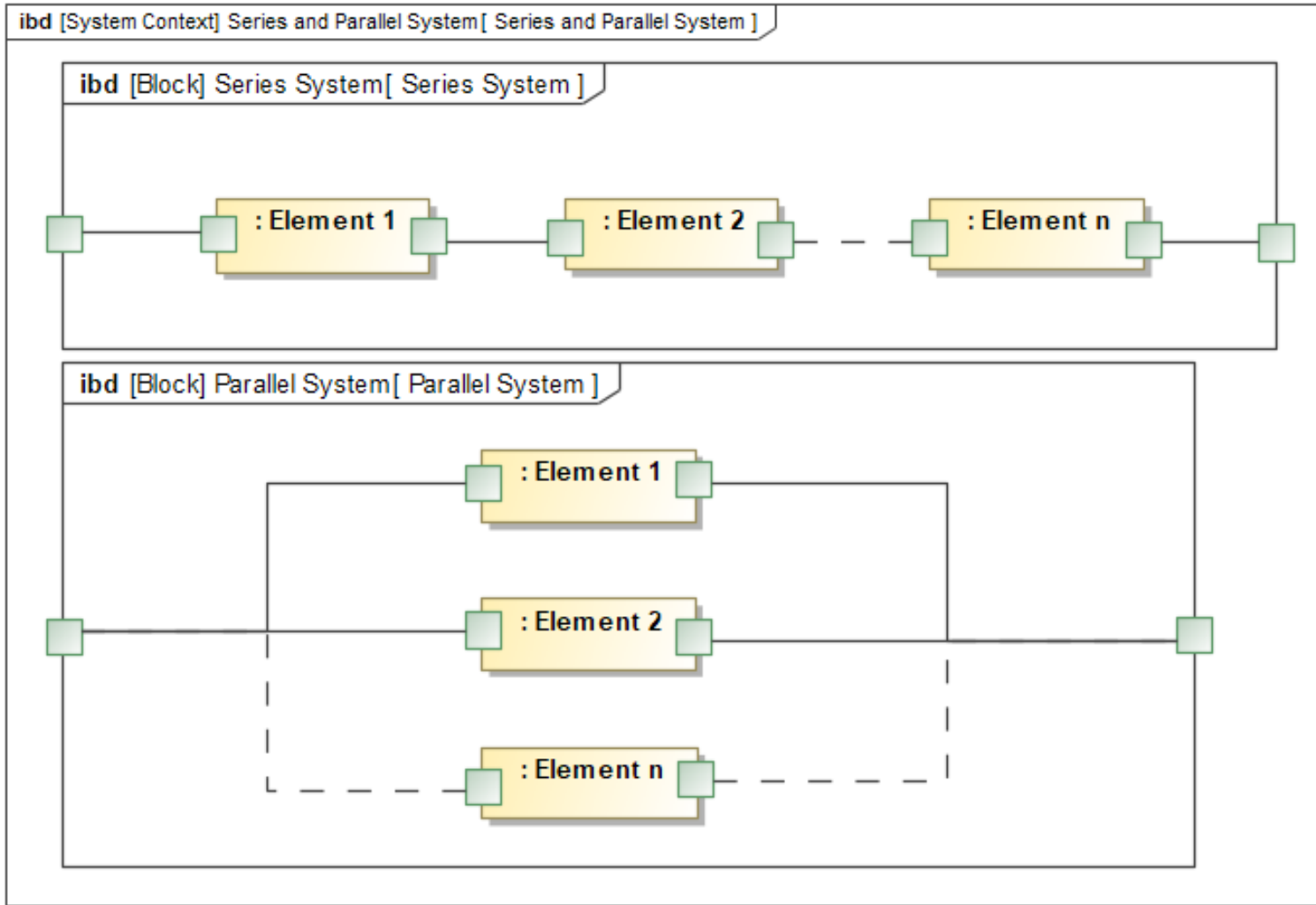
- ▶ Mission capability impact
- ▶ CTX Subsystem: **Command & Data Handling**





Simulation Development & Coupling

Architecture Variants

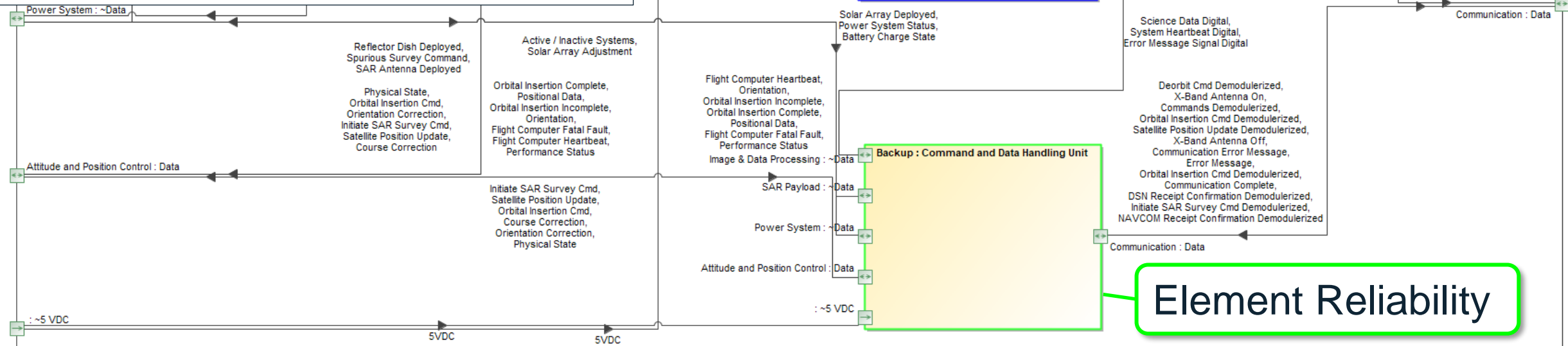
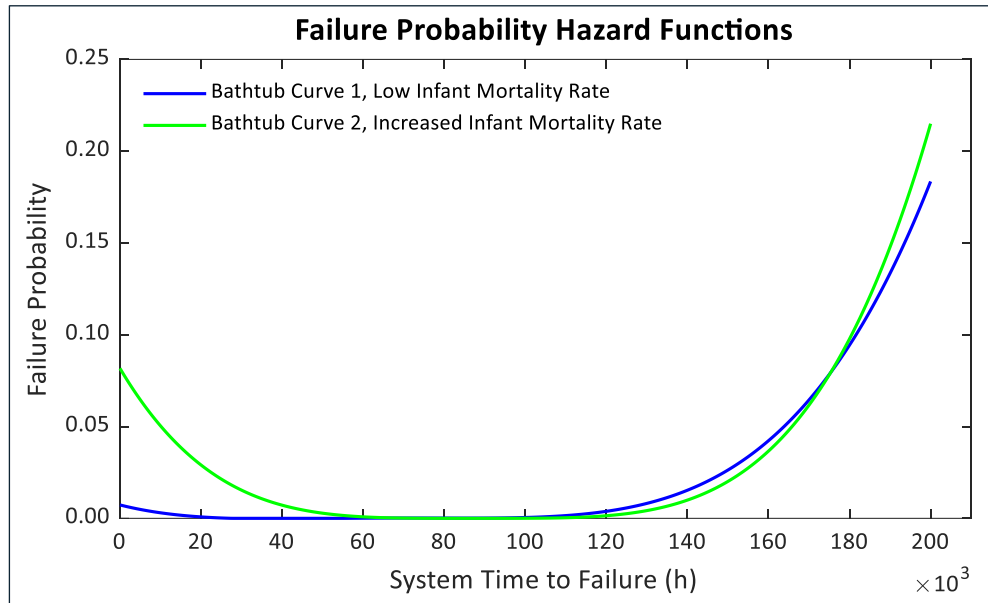


RELIABILITY RELATIONSHIP ^[15]

$$R_{series}(t) = \prod_{i=1}^n R_i(t)$$

$$R_{Parallel}(t) = 1 - \prod_{i=1}^n [1 - R_i(t)]$$

Architecture to Simulation Mapping

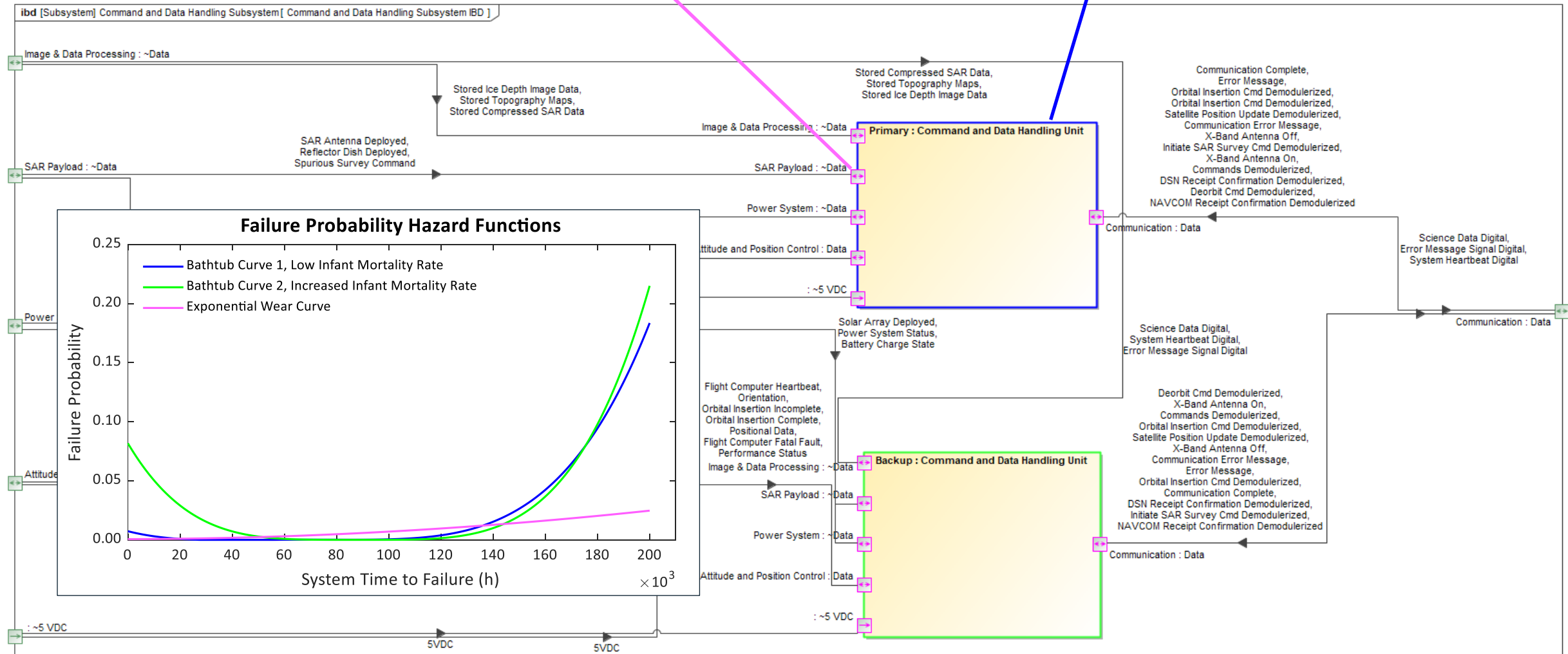


Element Reliability

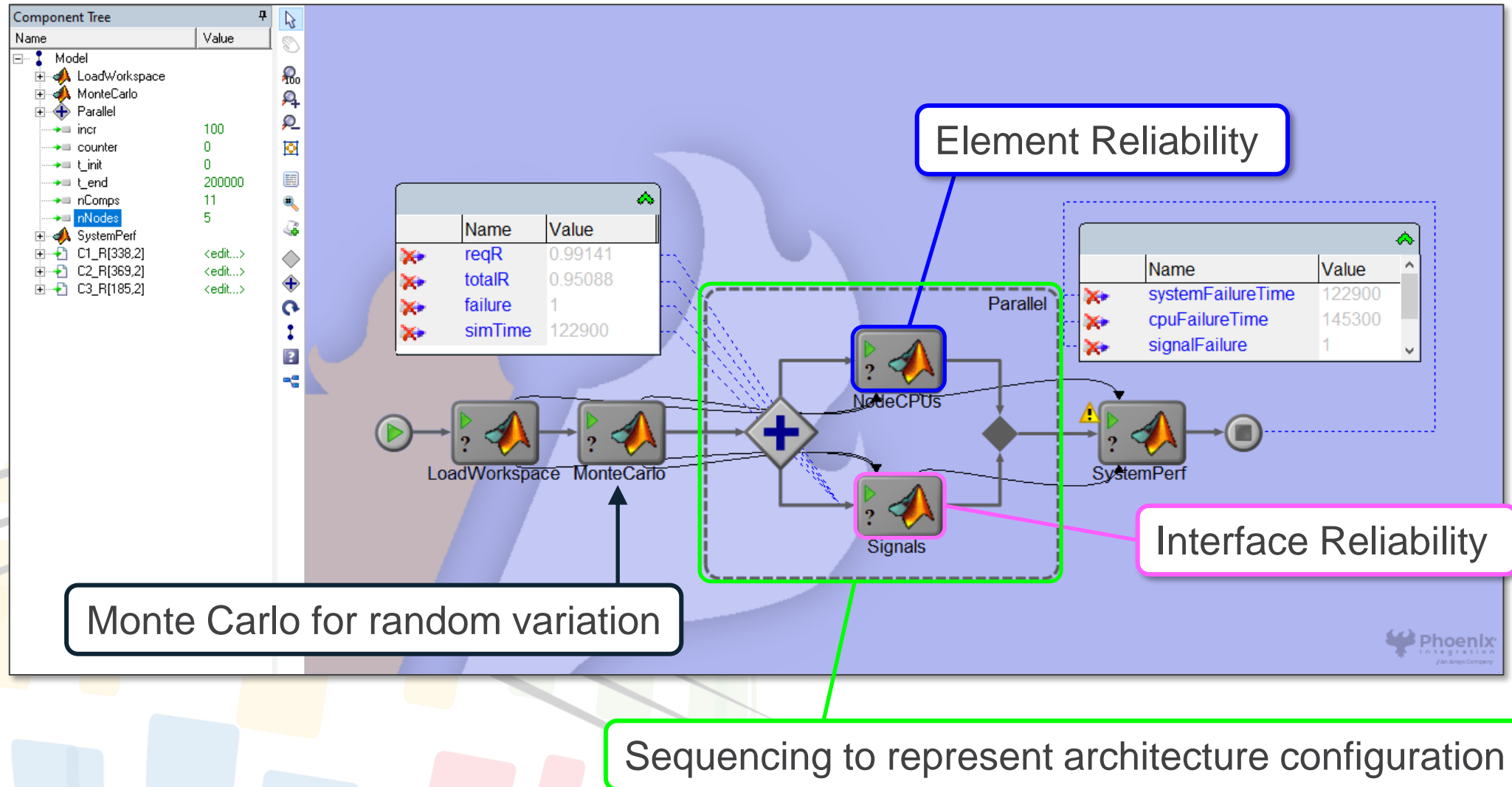
Architecture to Simulation Mapping

Interface Reliability

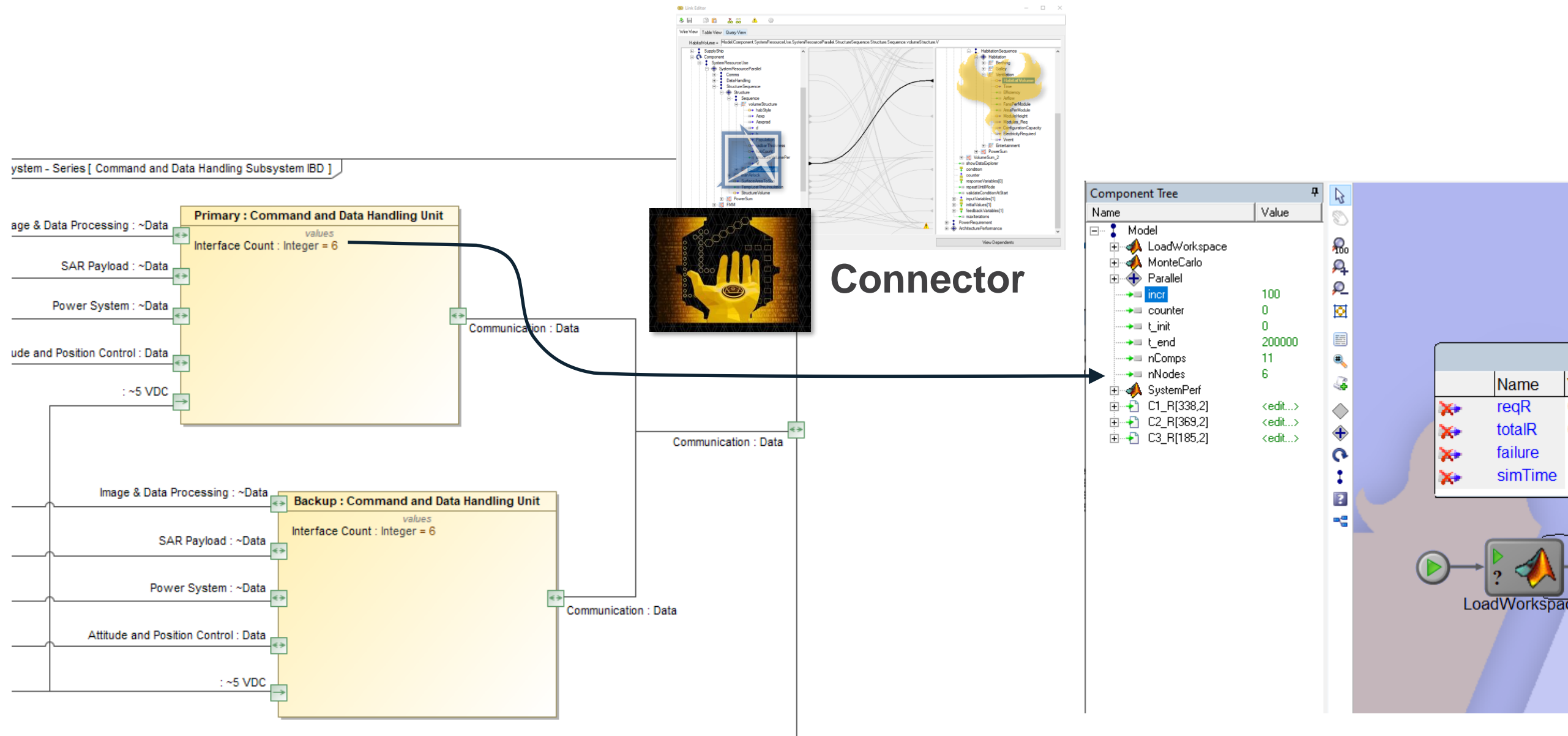
Element Reliability



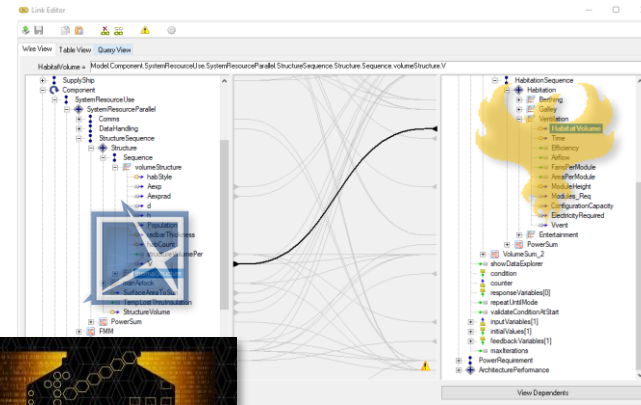
Architecture to Simulation Mapping



Link Architecture to Simulation



Link Architecture to Simulation



Connector

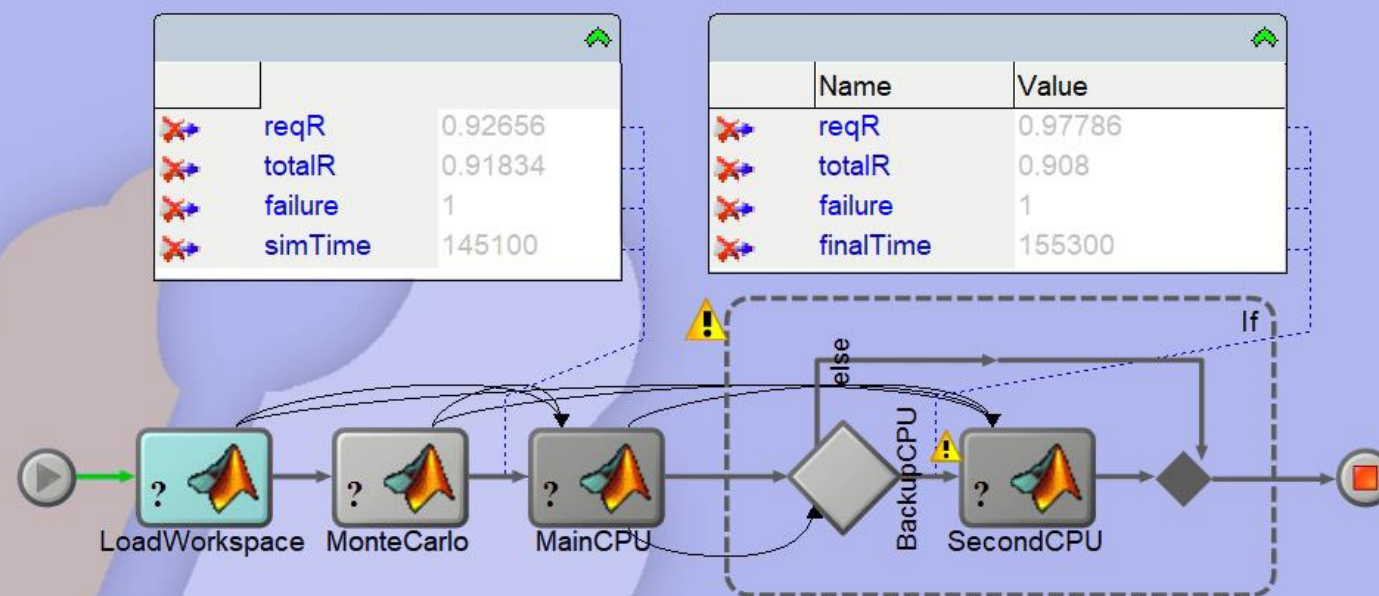
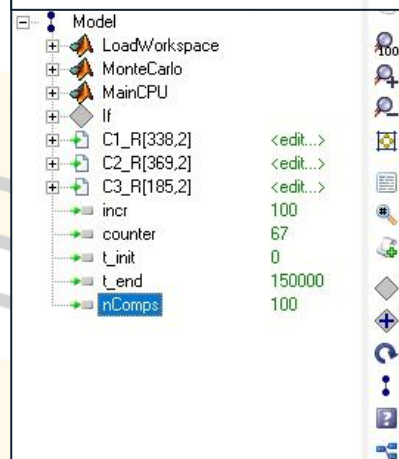
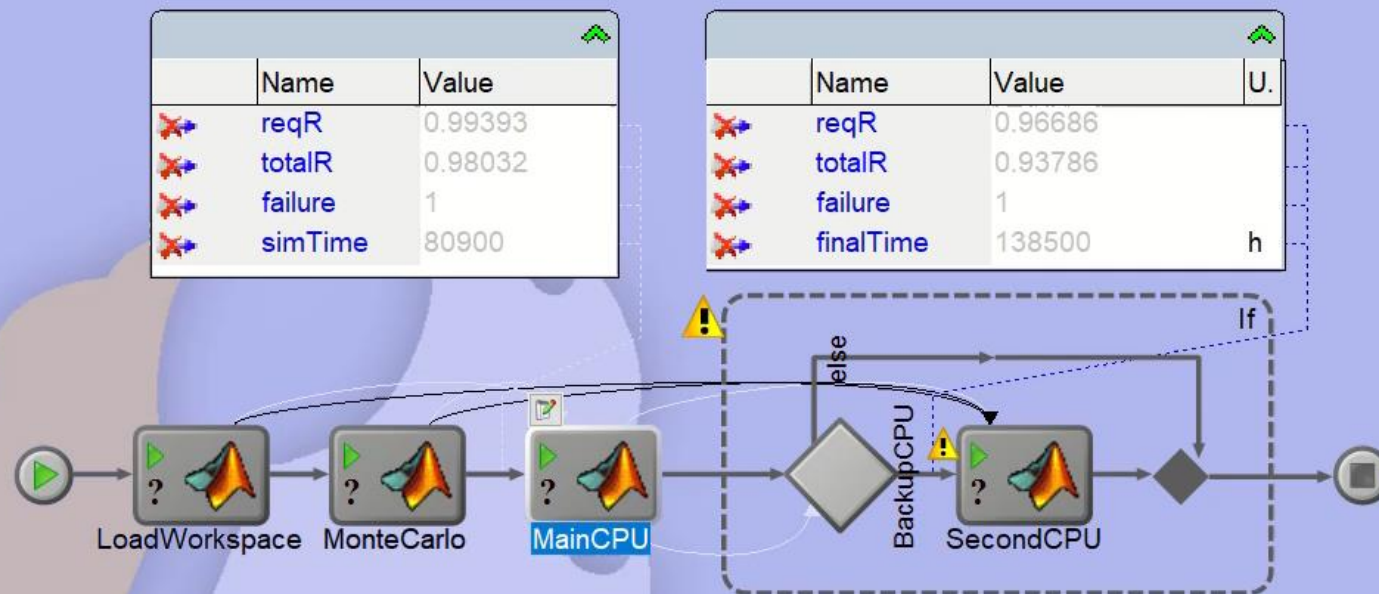
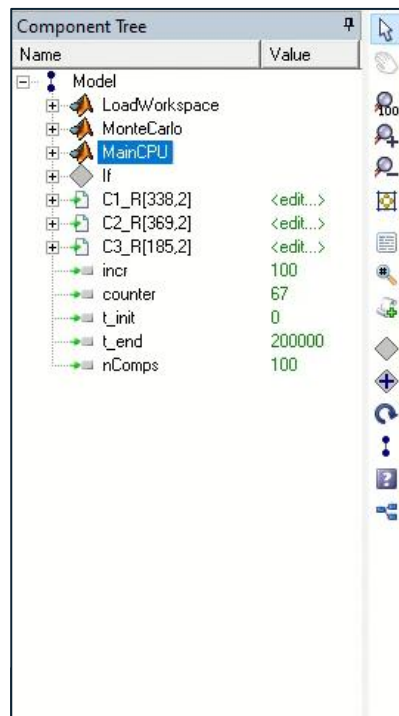
Component Tree

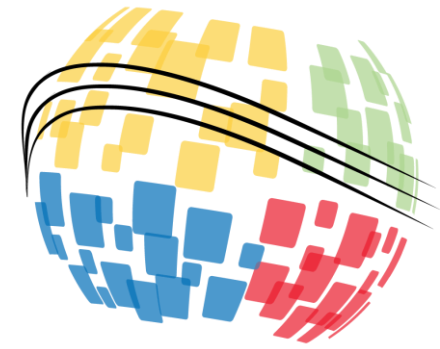
Name	Value
Model	
LoadWorkspace	
MonteCarlo	
Parallel	
incr	100
counter	0
t_init	0
t_end	200000
nComps	11
nNodes	7
SystemPerf	
C1_R[338.2]	<edit...>
C2_R[369.2]	<edit...>
C3_R[185.2]	<edit...>

LoadWorkspace

	Name
	reqR
	totalIR
	failure
	simTime

Demo





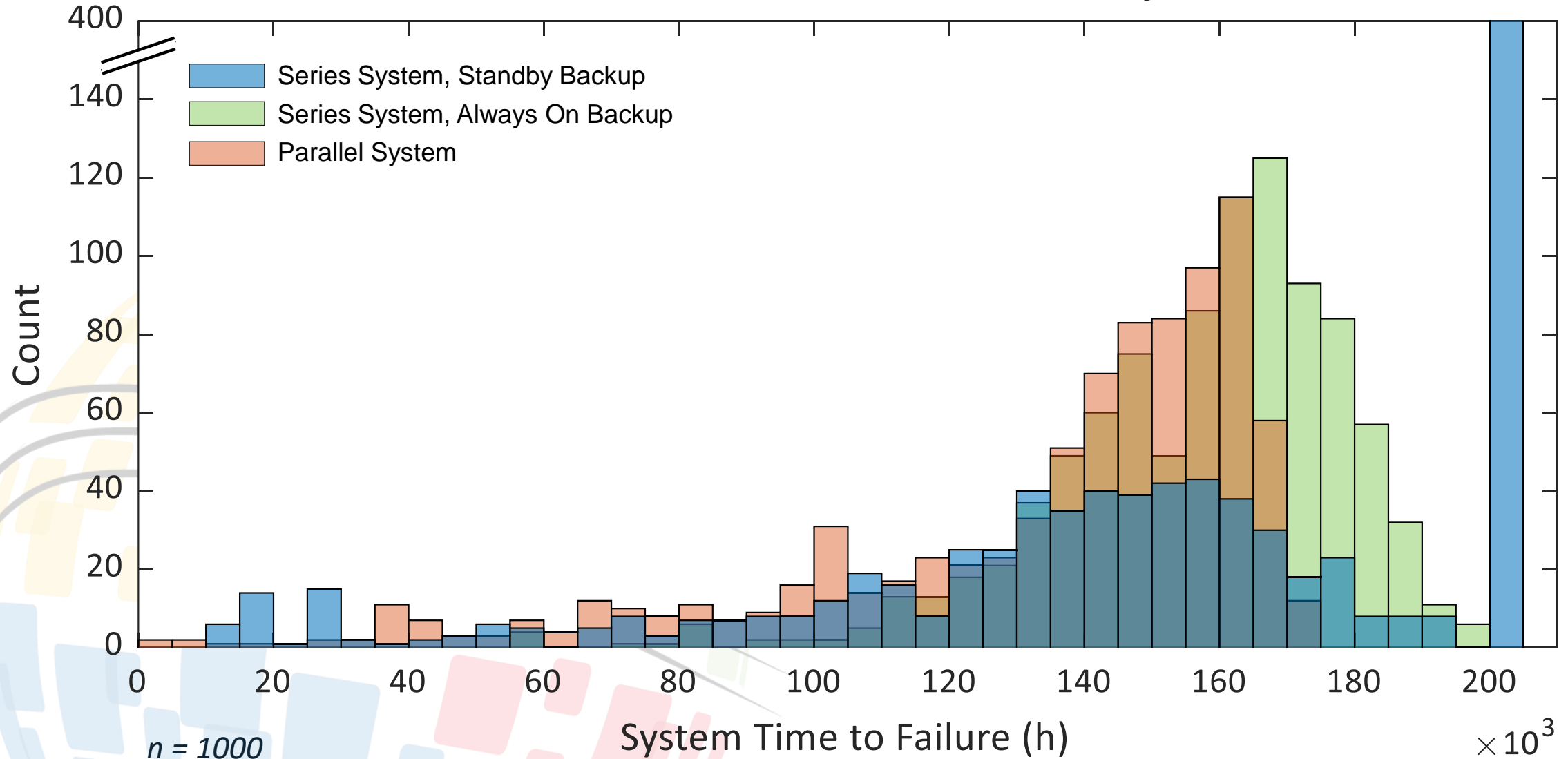
Reliability Analysis

Simulation Configuration

- ▶ Three architecture configurations:
 1. Series System with Standby Backup
 2. Series System with Always on Backup
 3. Parallel System with 3 Distributed Computing Nodes
- ▶ Target operational lifespan of 100,000 hours
- ▶ Simulated with 1,000 runs

Simulation Results Time to Failure for 1,000 Simulations

Time to Failure: Series and Parallel Systems



Simulation Results

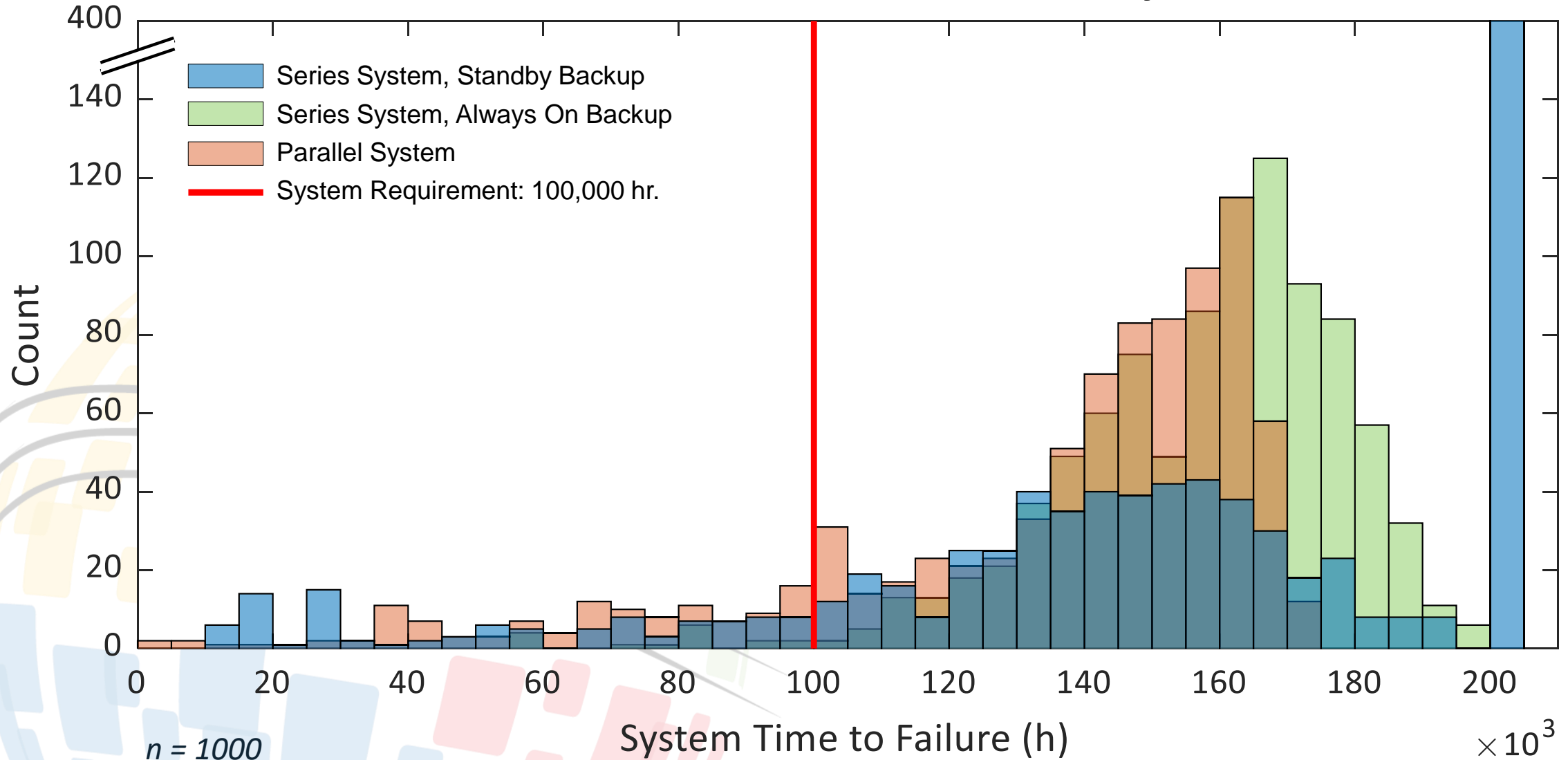
«performanceRequirement»

Operational Lifespan

Id = "P-01"

Text = "The system shall remain in operation for a minimum of 100,000 hours."

Time to Failure: Series and Parallel Systems

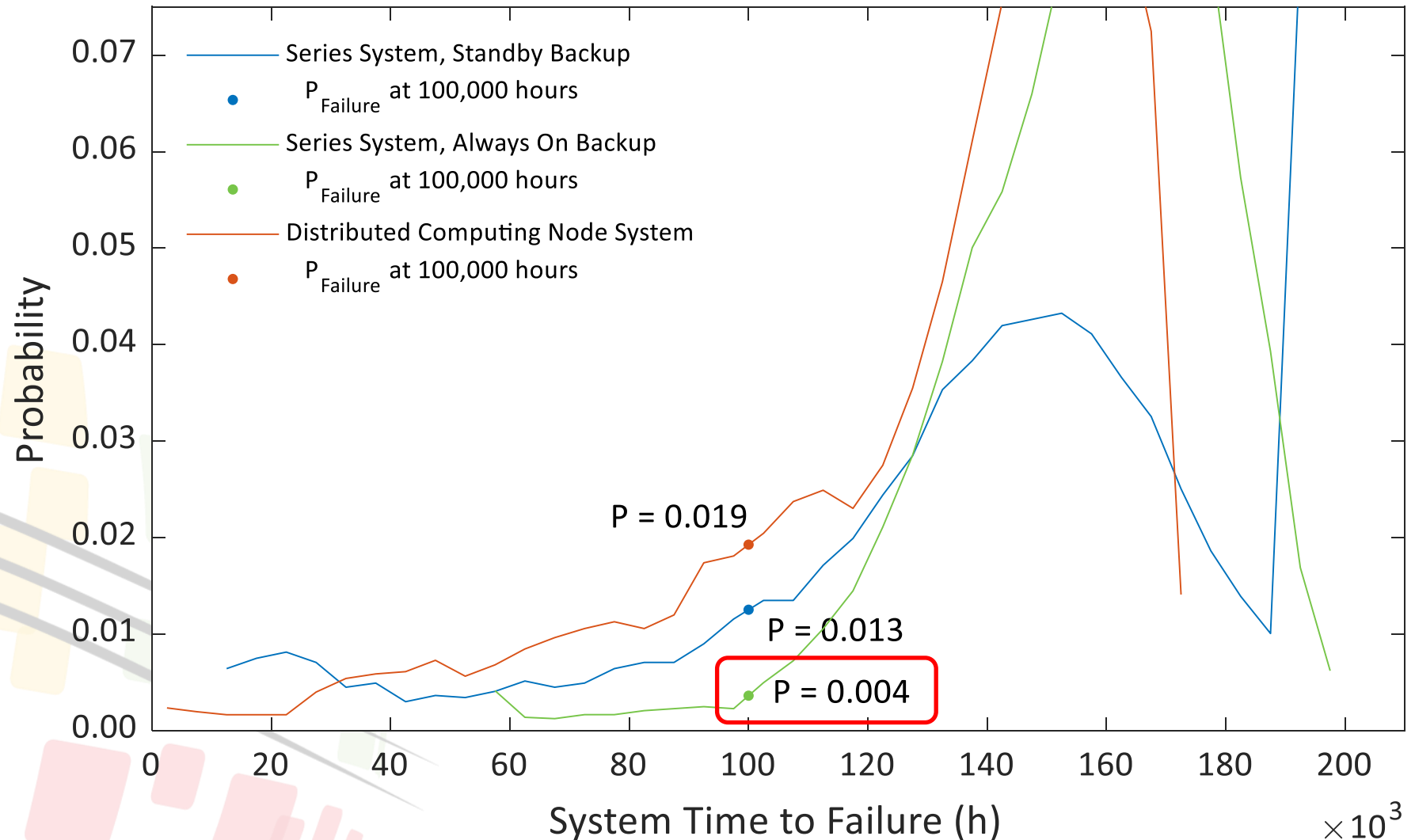


Failure Probability Distribution

Failure-Reliability Relationship

$$F_i(t) = 1 - R_i(t)$$

Failure Probability Distribution





Complexity Resilience Tradeoff

Complexity Resilience Tradeoff

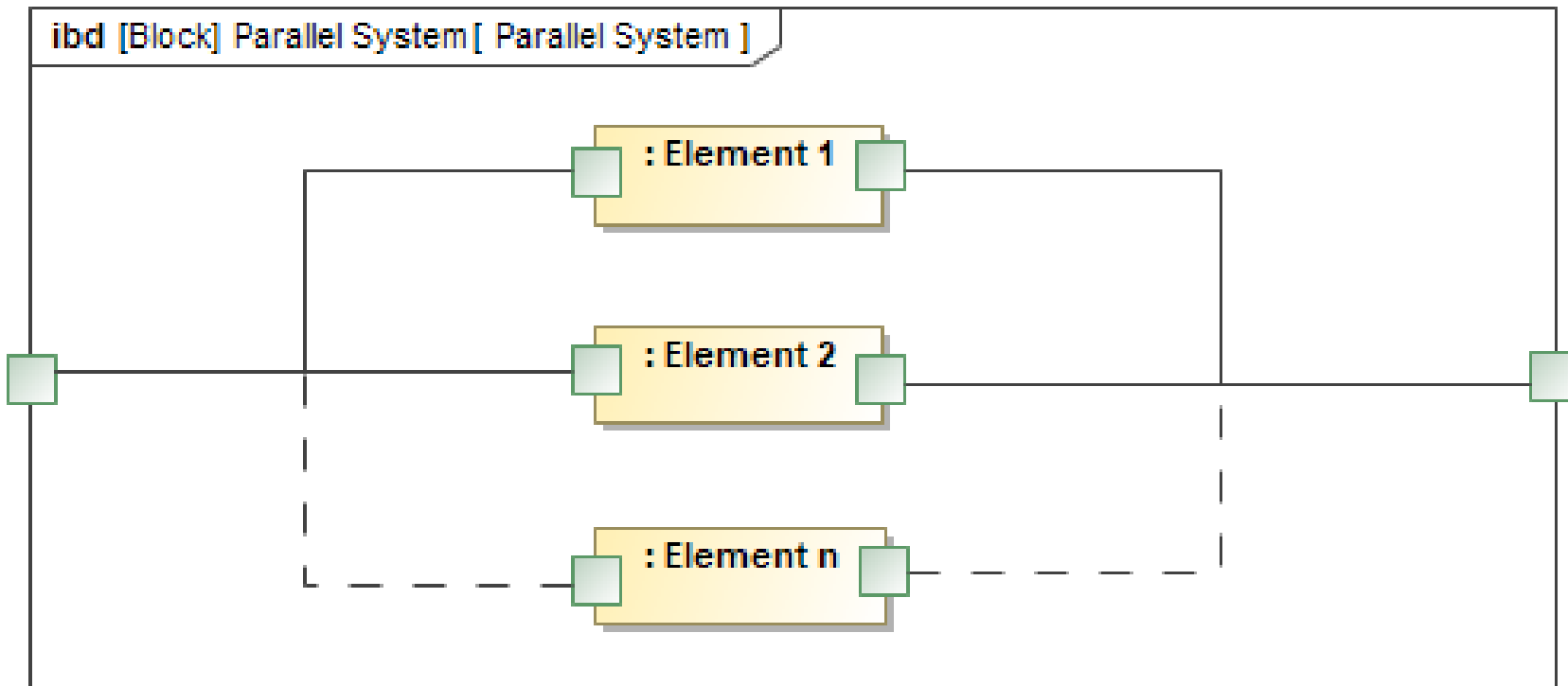


Adapted from R. Cook, *How Complex Systems Fail*. Cognitive Technologies Laboratory, University of Chicago, 2000. ^[16]

- ▶ Adding **new system elements, which are often intended to prevent system failure or aid in recovery from failure**, does not inherently yield a more robust system.
- ▶ These new elements introduce **additional system complexity, new forms of failure, and new pathways to failures** previously avoided by the less-complex system design.

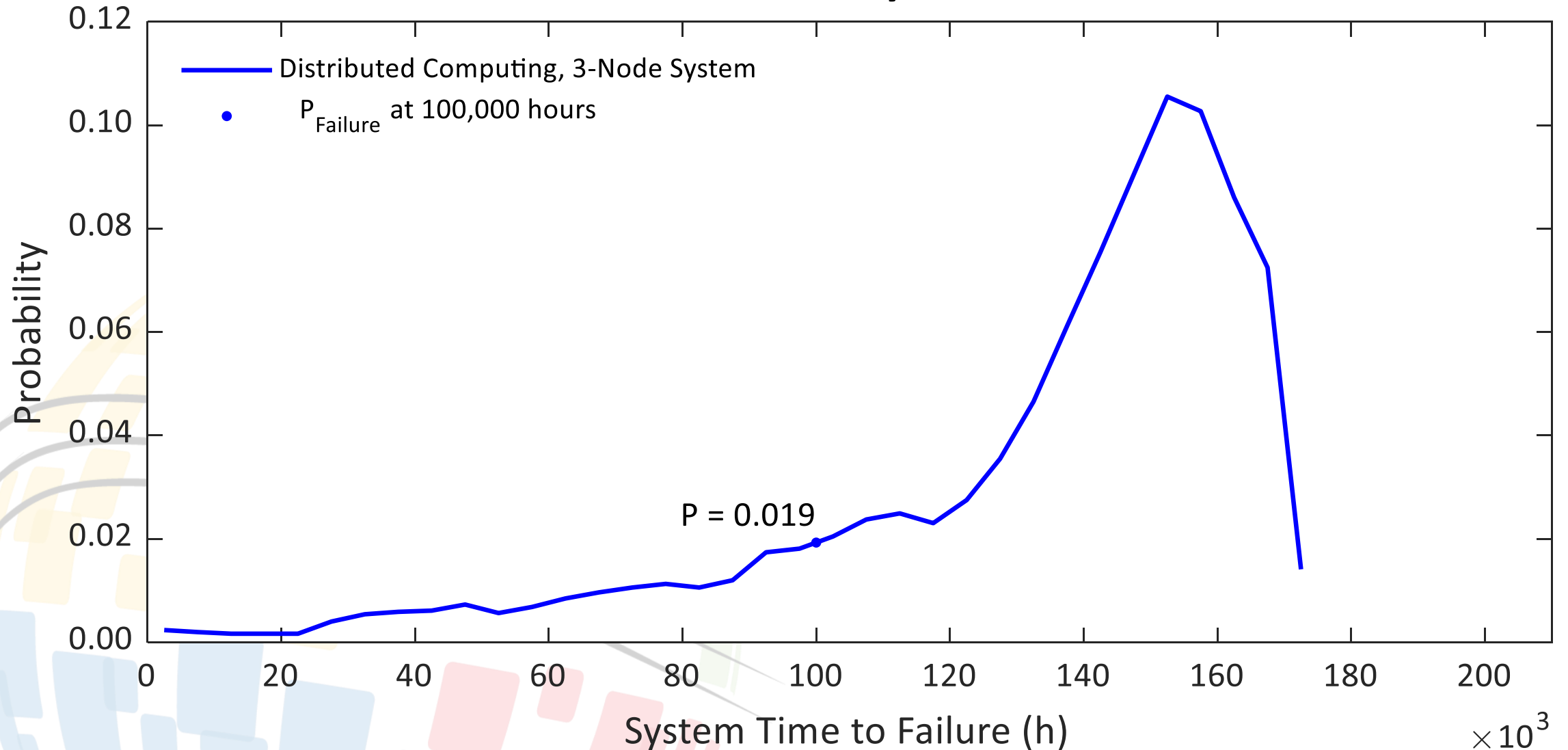
Complexity Resilience Tradeoff

Analyzed 3-, 4-, and 5- Node Parallel Systems



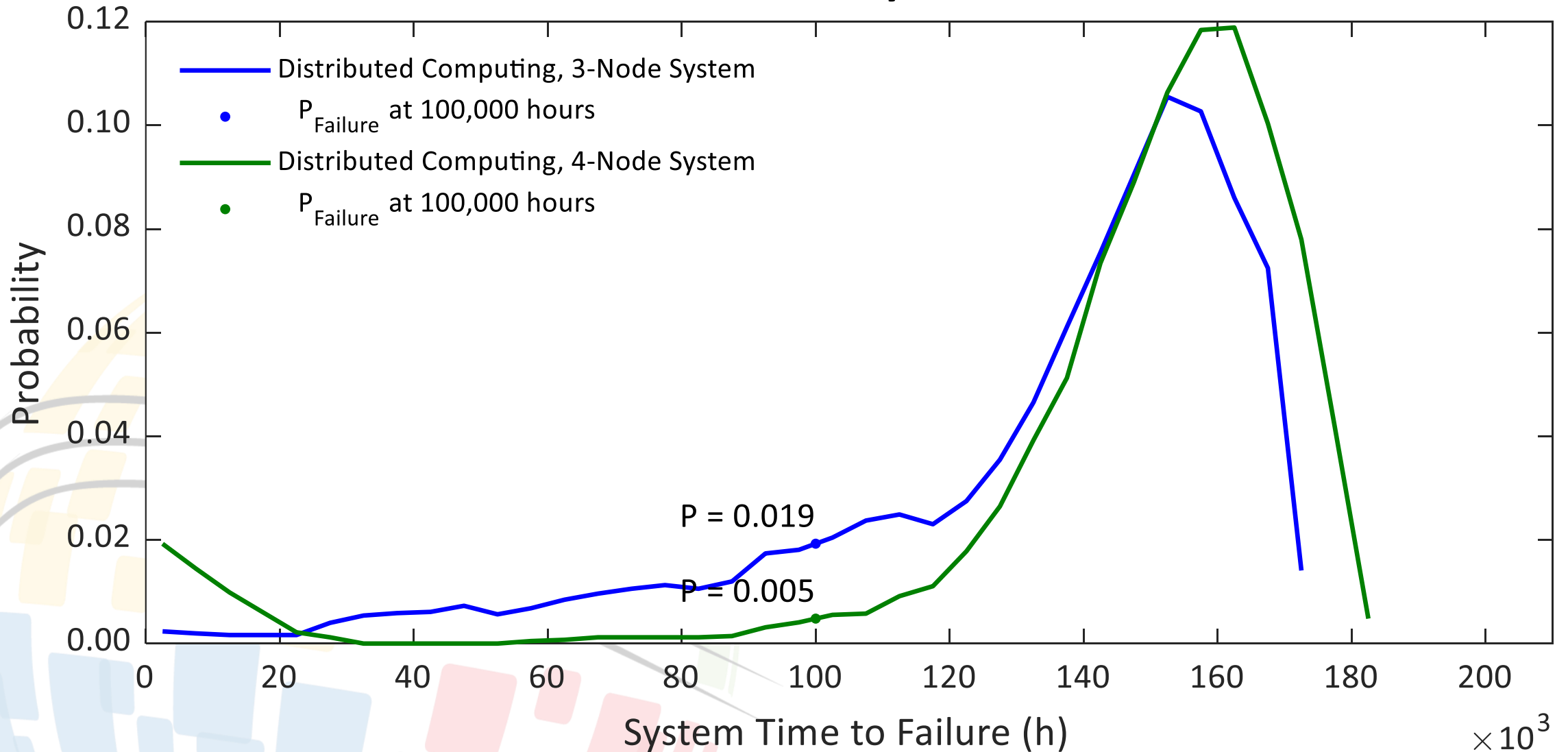
Simulation Results Multi-Node Parallel Systems

Failure Probability Distribution



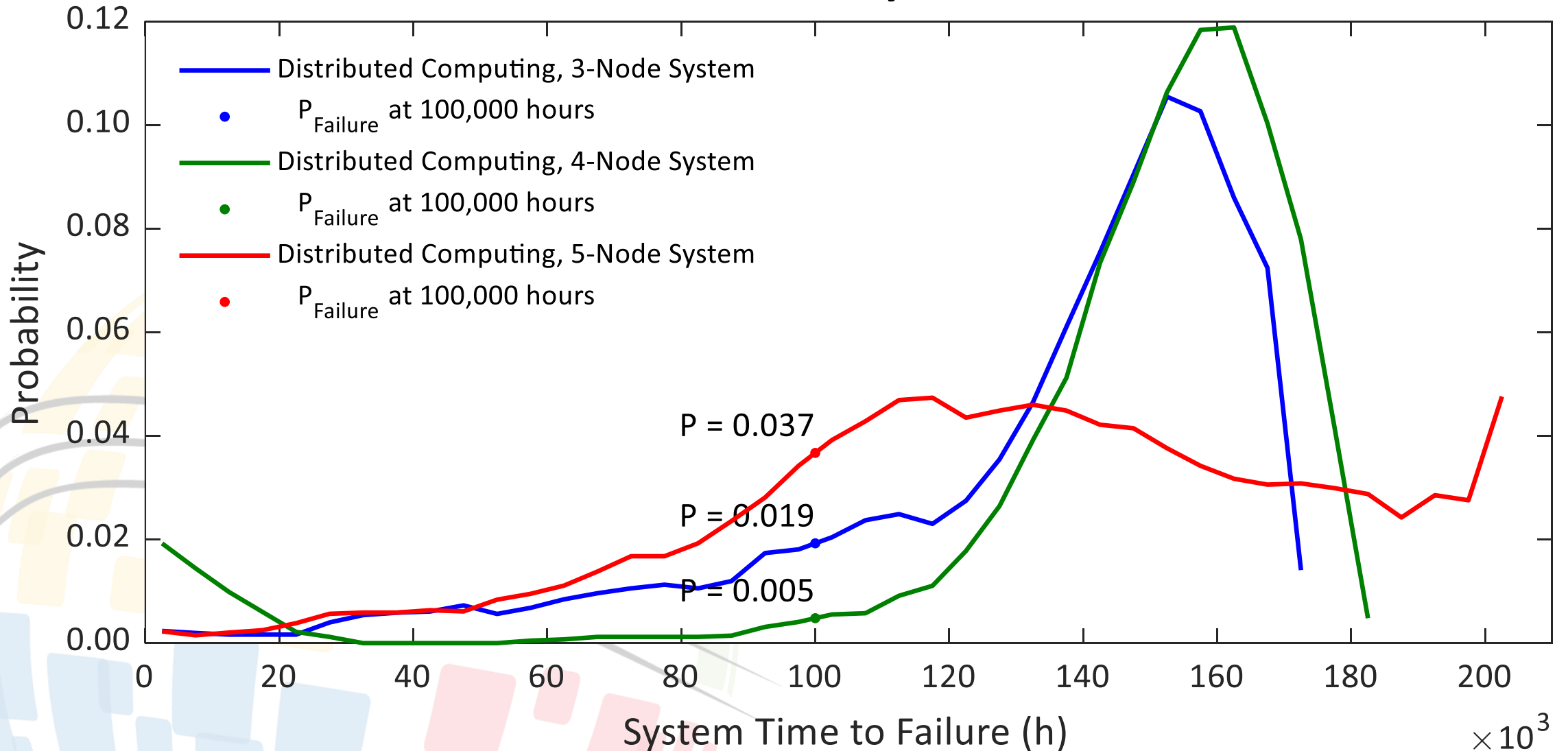
Simulation Results Multi-Node Parallel Systems

Failure Probability Distribution

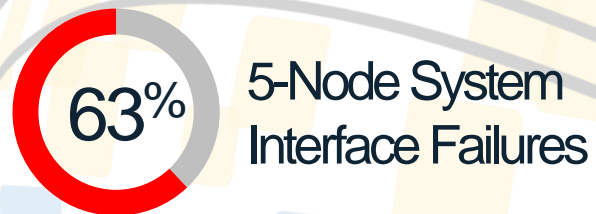
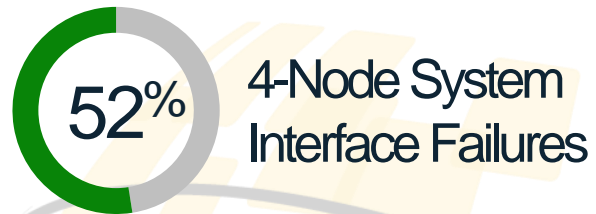


Simulation Results Multi-Node Parallel Systems

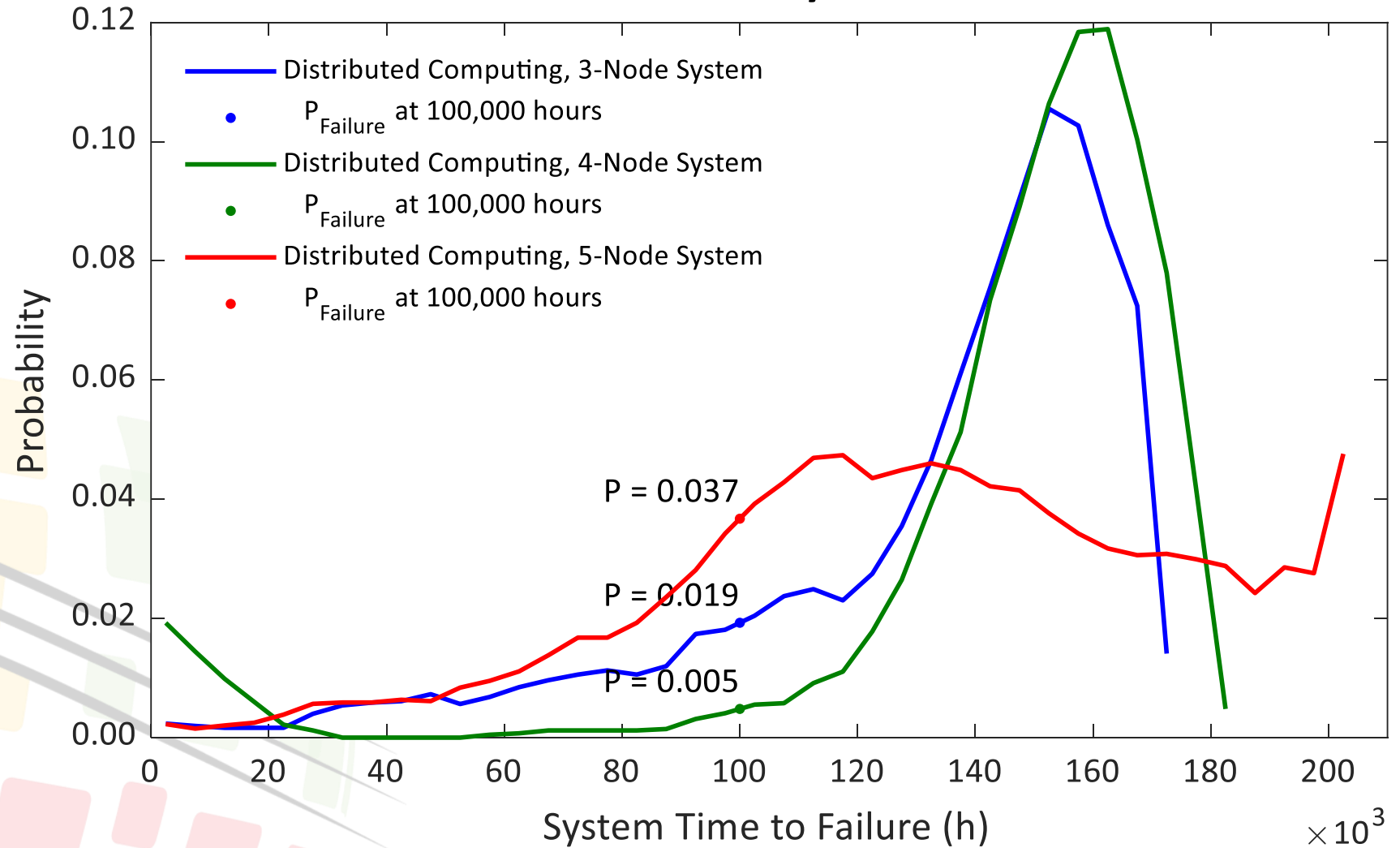
Failure Probability Distribution



Simulation Results Multi-Node Parallel Systems



Failure Probability Distribution





Summary

Evaluation Coupled Simulation Application to Reliability

- ▶ Efficiently created different architecture configurations and coupled to a system reliability simulation
- ▶ Enabled high reuse of model-based content
- ▶ Characterized architecture reliability to aid stakeholder decision-making
- ▶ Documented assumptions via the architecture and simulation configuration
- ▶ Created an extensible simulation infrastructure

Why go through the effort of coupling?

“I can manage the changes manually.”

A: **Immediate** and **automatic** architecture to simulation cascade

“My architecture is static; I don’t need to create concrete simulation links.”

A: Coupled simulation creates an **end-to-end** architecture-configuration-simulation-result traceability thread

“The analysis over-simplifies complex relationships.”

A: Simulation workflow is **continuously updatable** as ambiguity decreases

“There are too many assumptions in the methodology.”

A: Many of the assumptions are **implicit** in current qualitative approaches ... the coupled simulation approach **adds rigor and clarity**

References

- [1] R. A. Williamson, *Exploring the Unknown*, Washington, D.C.: National Aeronautics and Space Administration, 1999.
- [2] M. Wall, "NASA's Shuttle Program Cost \$209 Billion – Was it Worth It?", 11 July 2011. [Online]. Available: <https://spacenews.com/nasas-shuttle-program-cost-209-billion-was-it-worth-it/>. [Accessed 7 July 2023].
- [3] (Image Source) NASA, "STS-135: The Final Voyage", 27 July 2011. [Online]. Available: https://www.nasa.gov/mission_pages/shuttle/shuttlemissions/sts135/launch/sts-135_mission-overview.html. [Accessed 6 July 2023].
- [4] (Image Source) NASA, "Kennedy Space Center Image Gallery", 21 July 2011. [Online]. Available: <https://www.nasa.gov/centers/kennedy/multimedia/images/index.html>. [Accessed 5 July 2023].
- [5] (Image Source) University of Sterling, "Seven Good Reasons to Study MSc Big Data Course". [Online]. Available: <https://www.stir.ac.uk/blog/7-good-reasons-to-study-msc-big-data-course/>. [Accessed 13 July 2023].
- [6] (Image Source) B. Marr & Co., "How Tesla Is Using Artificial Intelligence to Create The Autonomous Cars Of The Future", 2021. [Online]. Available: <https://bernardmarr.com/how-tesla-is-using-artificial-intelligence-to-create-the-autonomous-cars-of-the-future/>. [Accessed 13 July 2023].
- [7] INCOSE, *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 4th edn, 2015. John Wiley & Sons, Hoboken, NJ. (p. 226)
- [8] P.D.T. O'Connor & A. Kleyner, *Practical Reliability Engineering*, Version 5, 2012. John Wiley & Sons, Hoboken, NJ.
- [9] M. Augustine, O.P. Yadav, R. Jain, A. Rathore, "Cognitive Map-Based System Modeling for Identifying Interaction Failure Modes", 2012. *Research in Engineering Design*, vol. 23, pp. 105 – 124.
- [10] T Kurtoglu & IY Tumer, "A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems", 2008. *Journal of Mechanical Design*, vol. 130, no. 5.
- [11] Dassault Systèmes, *MagicDraw*, 2021. [Online]. Available: <https://www.3ds.com/products-services/catia/products/no-magic/magicdraw/>. [Accessed 18 October 2021].
- [12] Ansys, *Ansys ModelCenter | MBSE Software*, 2022. [Online]. Available: <https://www.ansys.com/products/connect/ansys-modelcenter>. [Accessed 10 December 2022].
- [13] J. Foust, *Mars scientists look to less expensive missions*, 2022. [Online]. Available: <https://spacenews.com/mars-scientists-look-to-less-expensive-missions/>. [Accessed 4 July 2023].
- [14] C. Caron, C. Craft, A. Prajapati, S. Pien, J. Ross, *Applying Model-Based Systems Engineering (MBSE) Methods to a Novel Shared Systems Simulation Methodology*, 12 December 2021. University of Detroit Mercy, College of Engineering and Science
- [15] J. Menčík, *Concise Reliability for Engineers*, 2016. IntechOpen, London (UK).
- [16] R. Cook, *How Complex Systems Fail*, 2000. Cognitive Technologies Laboratory, University of Chicago, Chicago, IL.
- [17] (Image Source) System Failure image. [Online]. Available: <https://squatiniversity.com/2016/02/19/system-failure/>. [Accessed 7 July 2023].



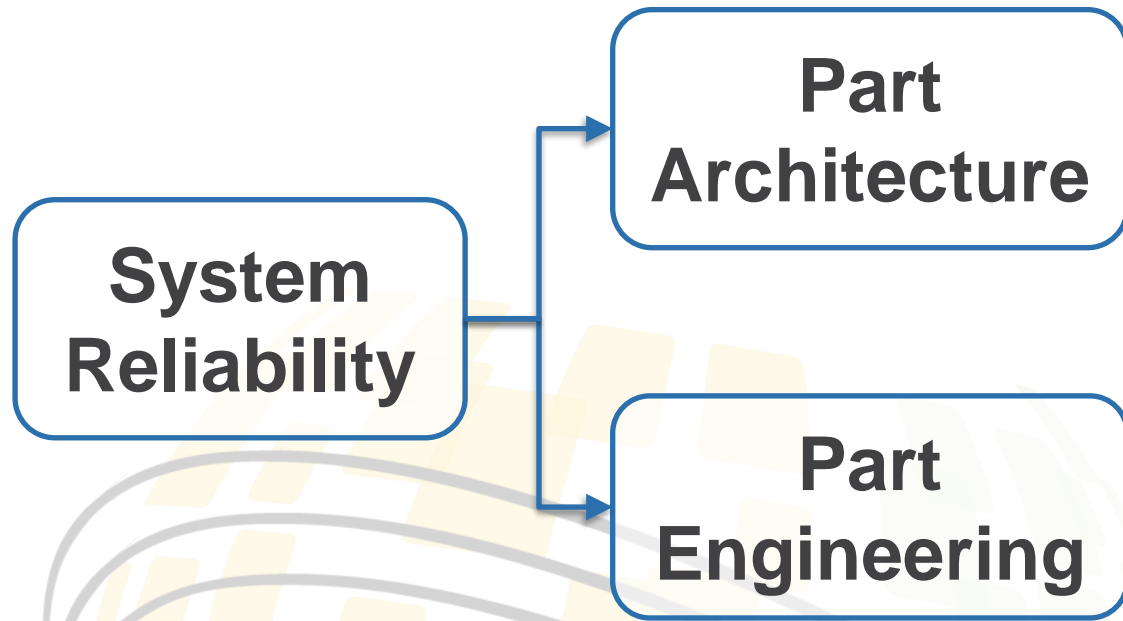
33rd Annual **INCOSE**
international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS

System Success Increasingly Relies on Emergent System Attributes



SYSTEM EMERGENCE

- ▶ Product of the architecture
- ▶ Results from interactions and relationships between elements
- ▶ Established early in the system development lifecycle

SYSTEMS ARCHITECTING

- ▶ An inductive method to address system ambiguity
- ▶ Qualitative, heuristic-based
- ▶ Traditionally part of a sequential Systems Architecting → Systems Engineering process