33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

The Safety Aspect of Measuring System Trust

Kate Kovalovsky
Strategic Technology Consulting

Agenda

- Introduction
- Model-Based Analysis for Defense Safety
- Safety Analysis Metrics
- System Trust Metric
- Conclusion

Introduction

Can system safety be summarized with meaningful and comprehensive metrics?

What metrics are useful in analyzing system safety?

How can Model-Based Systems Engineering facilitate capturing safety metrics?

Safety data in a digital engineering environment is the first step toward an overall system trust metric as described in the INCOSE 2035 Systems Engineering Vision

INCOSE 2035 SE Vision: Trust Metric

Engineering Trusted Systems

FROM

Systems trust is a loosely defined concept that includes many properties including cyber-security, data privacy, systems safety and overall reputation. The legal landscape governing how systems must address these properties is evolving quickly and inconsistently, but the properties that comprise "trust" are routinely "secondary" considerations in overall system designs. But the increasing level of interconnectedness in systems and the increasingly routine nature of data collection to power new systems, is resulting in a risk surface for organizations that is rising exponentially.

TO

Systems engineering routinely incorporates a range of new perspectives including security, privacy, and explainability with traditional perspectives such as systems safety to define and track a metric of "systems trust". This includes designing with data minimization and defense in depth principles to protect the systems from cyber- threats and minimize the impact to users if a system is breached.

As autonomous systems become mainstream, principles of explainability and provable safety will allow system providers to build confidence in these systems and will allow those system developers to differentiate themselves in the marketplace.

source: https://violin-strawberry-9kms.squarespace.com/model-based-practices

Purpose

- Demonstrate how a model-based Systems Modeling Language (SysML) safety profile can **provide insight into a system's safety posture** by leveraging metric suites in Cameo Systems Modeler to **summarize safety characteristics** on a fictitious system

Model-Based Analysis for Defense Safety

Model-Based Profile for MIL-STD-882

- Users enter information and model automatically returns results
- Safety information evolves with system model
- Captures key information about safety analysis to inform design
- Enables metrics to be tracked throughout system lifecycle
- Aligns with Risk Assessment and Software Safety Criticality Matrices from MIL-STD-882

System Application Example

- For presentation purposes, the profile and metrics were applied to a fictitious system
- Can be applied to any MBSE / SysML effort

Hazard & Risk Analysis

- Hazards can be rated according to the Risk Assessment Matrix directly in the model

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risk Assessment Code (RAC): High Serious Medium Low Eliminated

Safety ID	Name	Severity	Safety Result	Probability Level Initial	Initial Risk Level	Probability Level Current	Current Risk Level	Probability Level Final	Final Risk Level
SC-50	Delete Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-51	Download Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-52	Initialize the System	Level II: Critical	Safety Critical	Level C: Occasional	Serious	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-53	Initiate Built-In Test	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated
SC-54	Initiate System Shutdown	Level II: Critical	Safety Critical	Level B: Probable	High	Level C: Occasional	Serious	Level E: Improbable	Medium
SC-55	Load Cryptographic Keys	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-56	Initiate INS Alignment	Level II: Critical	Safety Critical	Level D: Remote	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated

Software Analysis

- Software functions are rated according to the SwCI table which determines LoR

SOFTWARE SAFETY CRITICALITY MATRIX				
	SEVERITY CATEGORY			
SOFTWARE CONTROL CATEGORY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

SwCI	Level of Rigor Tasks
SwCI 1	Program shall perform analysis of requirements, architecture, design, and code; and conduct in-depth safety-specific testing.
SwCI 2	Program shall perform analysis of requirements, architecture, and design; and conduct in-depth safety-specific testing.
SwCI 3	Program shall perform analysis of requirements and architecture; and conduct in-depth safety-specific testing.
SwCI 4	Program shall conduct safety-specific testing.
SwCI 5	Once assessed by safety engineering as Not Safety, then no safety specific analysis or verification is required.

Name	Severity	SW Safety Result	SWControlCategory	Sw CI Calc	Partitioned	Partitioned Status	Status
Execute Periodic Built-In Test	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Partially Met
Generate and Route Precision Time Outputs	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Partially Met
Generate Download Status	Level IV: Negligible	Not Safety Significant	4Influential	SwCI4	false	N/A	Not Met
Generate IBIT Options Message	Level IV: Negligible	Not Safety Significant	2SemiAutonomous	SwCI4	false	N/A	Partially Met
Generate Sensor Capability Status Request	Level II: Critical	Safety Critical	3RedundantFaultTolerant	SwCI3	true	Yes	Partially Met
Generate software status	Level II: Critical	Safety Critical	2SemiAutonomous	SwCI2	true	Yes	Partially Met
GPS Signal Acquisition	Level II: Critical	Safety Critical	1Autonomous	SwCI1	true	Yes	Not Met
Initialize Periodic Built-in Test	Level III: Marginal	Safety Related	1Autonomous	SwCI3	false	N/A	Not Met

Safety Analysis Metrics

Validation-Based Metric Suites

- Validation suites in Cameo Systems Modeler provide a way of evaluating a set of data (model) against a specific expression
  - Helpful for consistency and quality checks
- Metric suites can summarize the counts and percentages of the validation results
- In this application, metric suites provide insight into the safety posture of a system
- Metric suites output to tables in Cameo
- Further visualization is done using Microsoft Excel

Distribution of Safety-Critical Functionality

Name	Safety Critical System Count	Safety Critical System Percentage	Safety Related System Count	Safety Related System Percentage	NSS System Count	NSS System Percentage
System Alpha	15	53.5714	8	28.5714	5	17.8571

Name	Safety Critical Software Count	Safety Critical Software Percentage	Safety Related Software Count	Safety Related Software Percentage	NSS Software Count	NSS Software Percentage
System Alpha	22	61.1111	10	27.7778	4	11

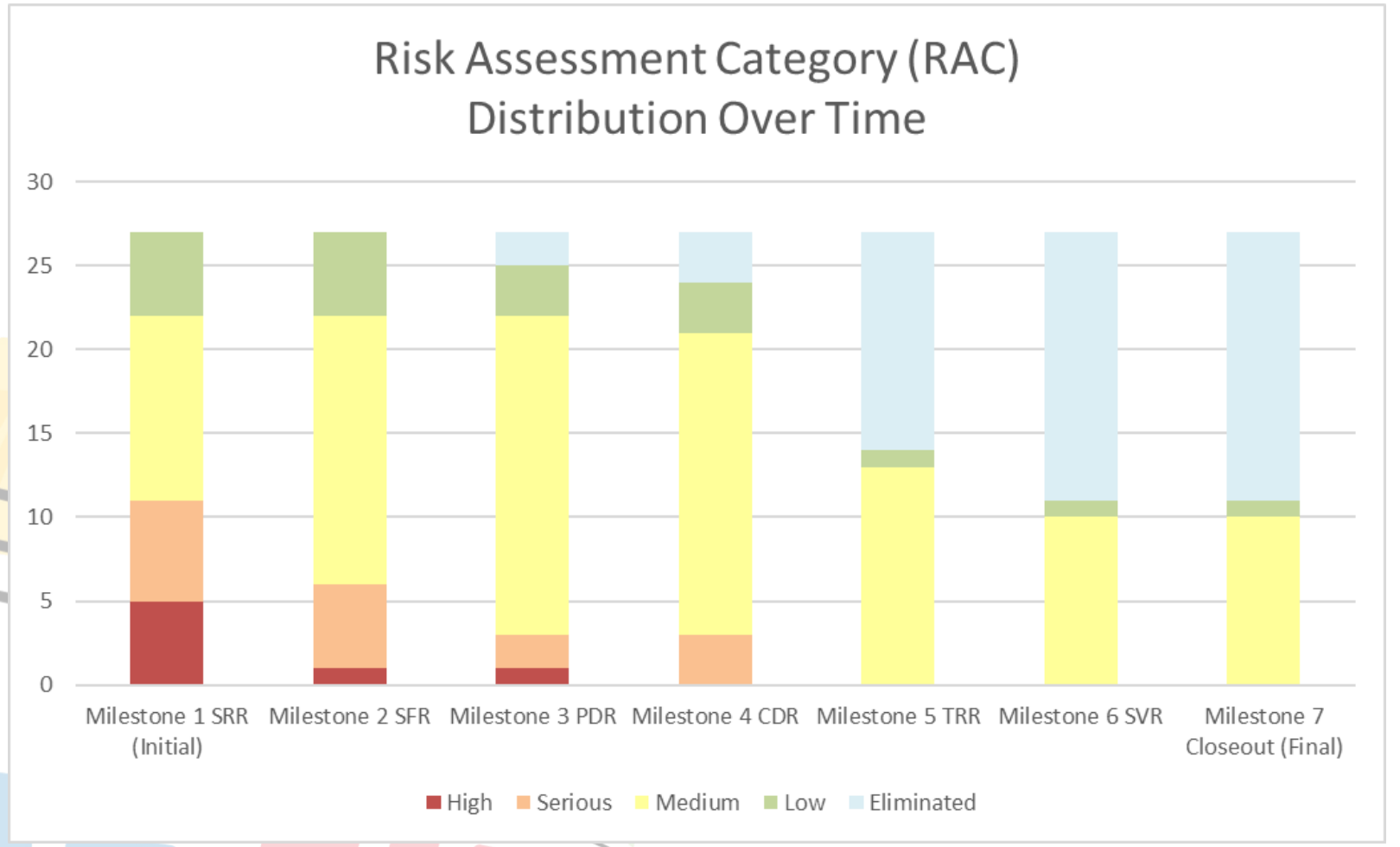
Risk Mitigation Across Lifecycle

Risk Assessment Code (RAC): High Serious Medium Low Eliminated

Safety ID	Name	Severity	Safety Result	Probability Level Initial	Initial Risk Level	Probability Level Current	Current Risk Level	Probability Level Final	Final Risk Level
SC-50	Delete Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-51	Download Recorded Data	Level IV: Negligible	Not Safety Significant	Level D: Remote	Low	Level E: Improbable	Low	Level F: Eliminated	Eliminated
SC-52	Initialize the System	Level II: Critical	Safety Critical	Level C: Occasional	Serious	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-53	Initiate Built-In Test	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated
SC-54	Initiate System Shutdown	Level II: Critical	Safety Critical	Level B: Probable	High	Level C: Occasional	Serious	Level E: Improbable	Medium
SC-55	Load Cryptographic Keys	Level III: Marginal	Safety Related	Level C: Occasional	Medium	Level E: Improbable	Medium	Level F: Eliminated	Eliminated
SC-56	Initiate INS Alignment	Level II: Critical	Safety Critical	L emote	Medium	Level D: Remote	Medium	Level F: Eliminated	Eliminated

Name	Initial High Count	Current High Count	Final High Count	Initial Serious Count	Current Serious Count	Final Serious Count	Initial Medium Count	Current Medium Count	Final Medium Count	Initial Low Count	Current Low Count	Final Low Count	Initial Eliminate Count	Current Eliminated Count	Final Eliminated Count
Milestone 1 SRR	5	5	0	6	6	0	11	11	11	5	5	1	0	0	15
Milestone 2 SFR	5	1	0	6	5	0	11	16	11	5	5	1	0	0	15
Milestone 3 PDR	5	1	0	6	2	0	11	19	11	5	3	1	0	2	15
Milestone 4 CDR	5	0	0	6	3	0	11	18	11	5	3	1	0	3	15
Milestone 5 TRR	5	0	0	6	0	0	11	13	10	5	1	1	0	13	16
Milestone 6 SVR	5	0	0	6	0	0	11	10	10	5	1	1	0	16	16
Milestone 7 Closeout	5	0	0	6	0	0	11	10	10	5	1	1	0	16	16

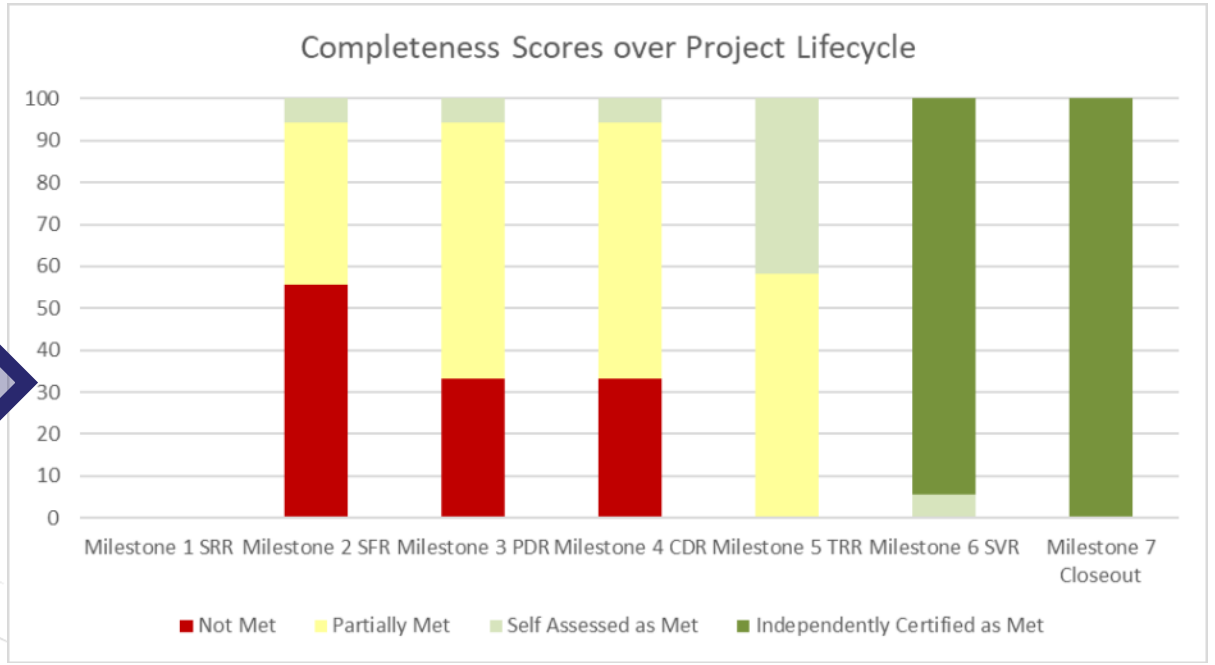
Risk Mitigation Across Lifecycle



Software Level of Rigor Completeness

- Shows progress toward meeting Level of Rigor requirements

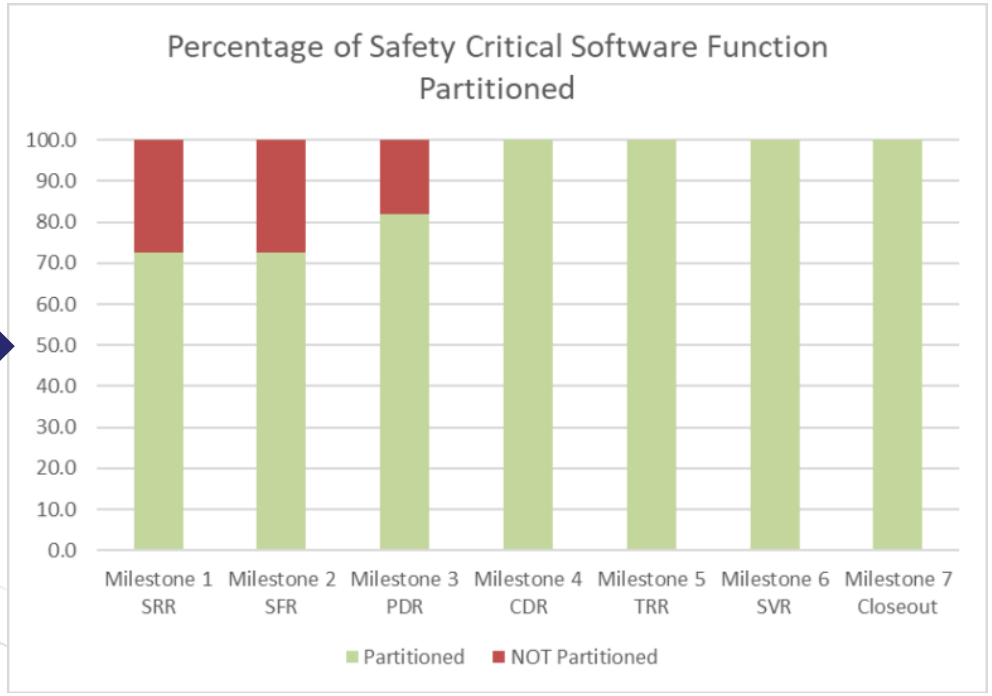
#	Name	Completeness Not Met Percentage	Completeness Partially Met Percentage	Completeness Self Assessed As Met Percentage	Completeness Independently Certified As Met Percentage
1	Milestone 1 SRR	0	0	0	0
2	Milestone 2 SFR	55.5556	38.8889	5.5556	0
3	Milestone 3 PDR	33.3333	61.1111	5.5556	0
4	Milestone 4 CDR	33.3333	61.1111	5.5556	0
5	Milestone 5 TRR	0	58.3333	41.6667	0
6	Milestone 6 SVR	0	0	5.5556	94.4444
7	Milestone 7 Closeout	0	0	0	100



Safety-Critical Partitioning Percentage

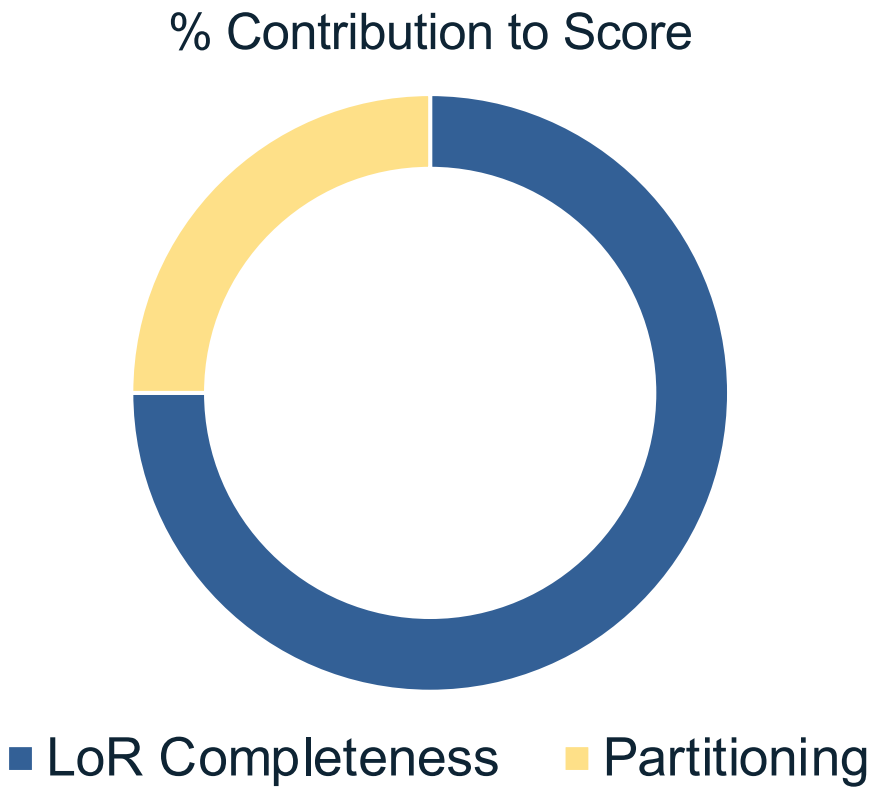
- Safety-critical software should be partitioned away from non-safety-critical software

Name	Safety Critical Software Partitioned Percentage	Safety Critical Software NOT Partitioned Percentage
Milestone 1 SRR	72.7273	27.2727
Milestone 2 SFR	72.7273	27.2727
Milestone 3 PDR	81.8182	18.1818
Milestone 4 CDR	100	0
Milestone 5 TRR	100	0
Milestone 6 SVR	100	0
Milestone 7 Closeout	100	0



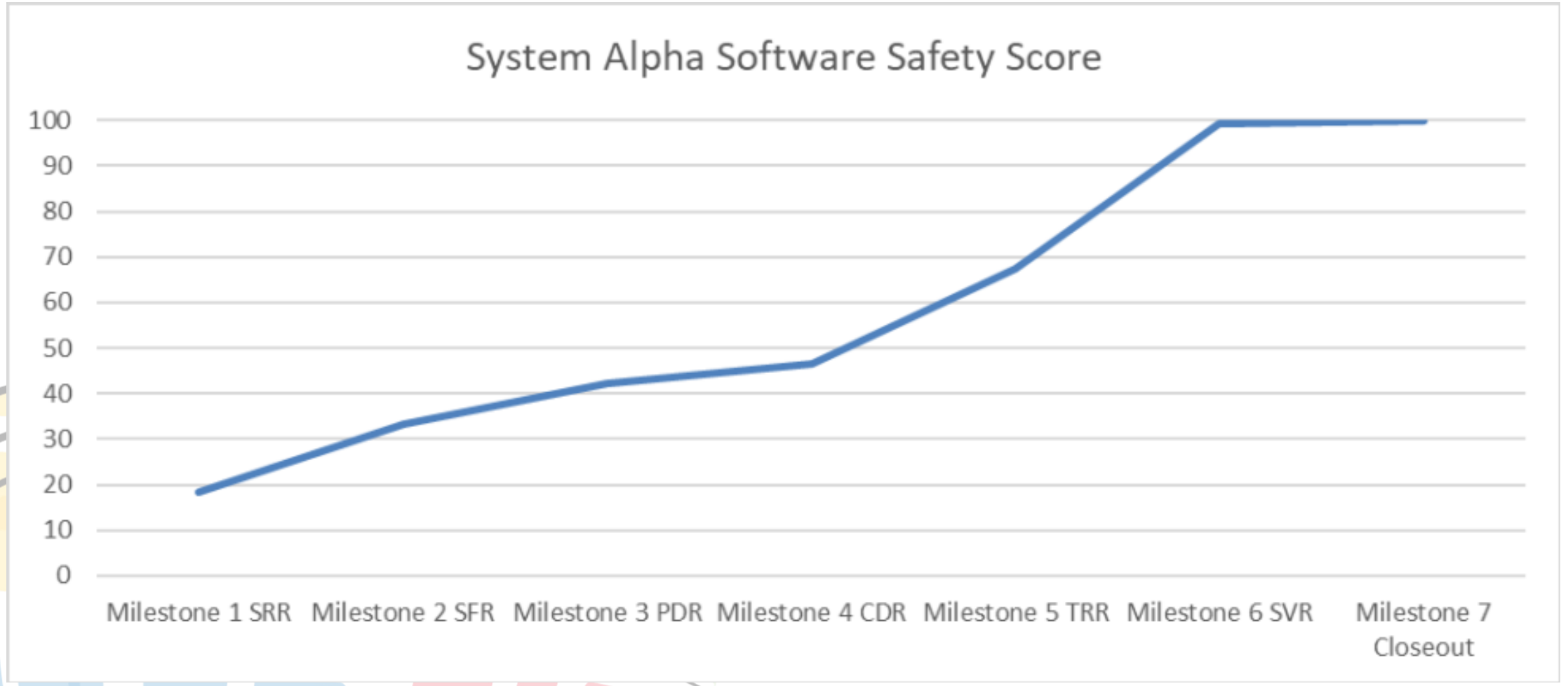
System Trust Metric

Software Safety Trustworthiness



- A quick-glance score (0-100)
- Calculated from LoR completeness and partitioning scores

Software Safety Trustworthiness Example



Comprehensive System Trust

- Expand to cyber, AI/Explainability, data privacy, reliability
- Could use Analytic Hierarchy Process (AHP) or other weighting to prioritize among elements

Conclusion

Future Research Opportunities

- Refine software safety metric based on real-world applications
- Create MBSE profiles for other safety standards
- Research how to measure other trust aspects
  - Calculate from an Integrated Digital Environment
  - Optimized weighting

Conclusion

- SysML can be extended to integrating safety analyses with systems engineering models and provide meaningful information to stakeholders
- Software Safety Trustworthiness score is comprised of Level of Rigor Completeness Score and Partitioning Score
- Safety is one component of the INCOSE's Systems Engineering Vision 2035's System Trust Metric
- A holistic System Trust Metric would also contain cybersecurity, reliability, data privacy, artificial intelligence explainability, and organizational transparency scores

Thank you for your time - Q&A

Kate Kovalovsky
Director of MBSE Services, STC

kkovalovsky@strattechnologies.com

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS