9th UCAAT User Conference on Advanced Automated Testing

Interim Report, IEEE Working Group 982.1, Measures of the Software Aspects of Dependability

Robert V. Binder

Chair, IEEE 982.1 Working Group

09/14/2022

Overview

982.1-202x Measures of the Software Aspects of Dependability

IEEE – Institute of Electrical and Electronics Engineers https://ieee.org

Background

- Motivation
- Goals
- Work to date
- Changes and improvements

Key questions

- What is Dependability?
- How is it different than …
- Can it be measured?
- Pre- versus post-release?

This presentation is snapshot of work in progress.

All concepts, terms, etc. are subject to change.

IEEE 982.1 Working Group

Gül Boztok Algin

Christie Bahn

Trac Bannon

Pieter Botman

Lynn Robert Carter

Sigrid Eldh

Lance Fiondella

Michael Grottke

Lou Gullo

Jon Hagar

Pratap Lakshman

Rajesh Murthy

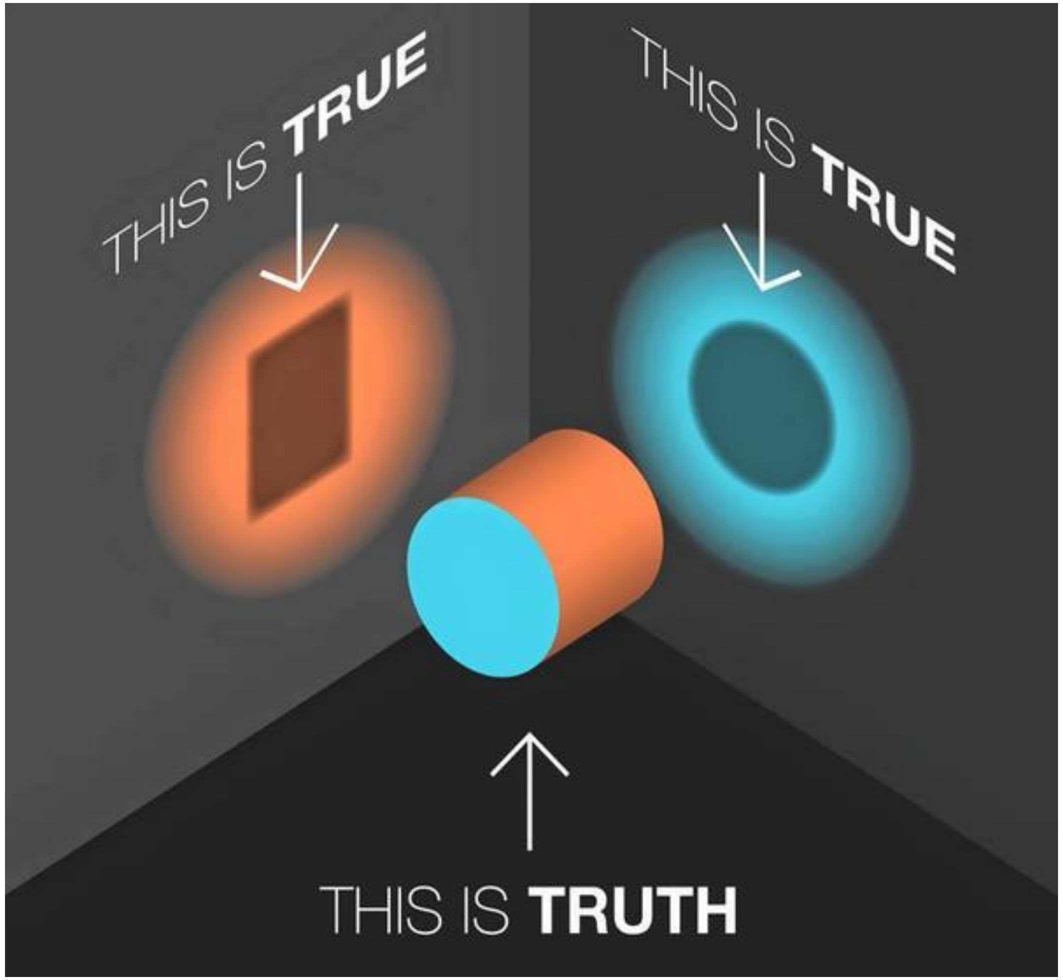
Joanna Olszewska

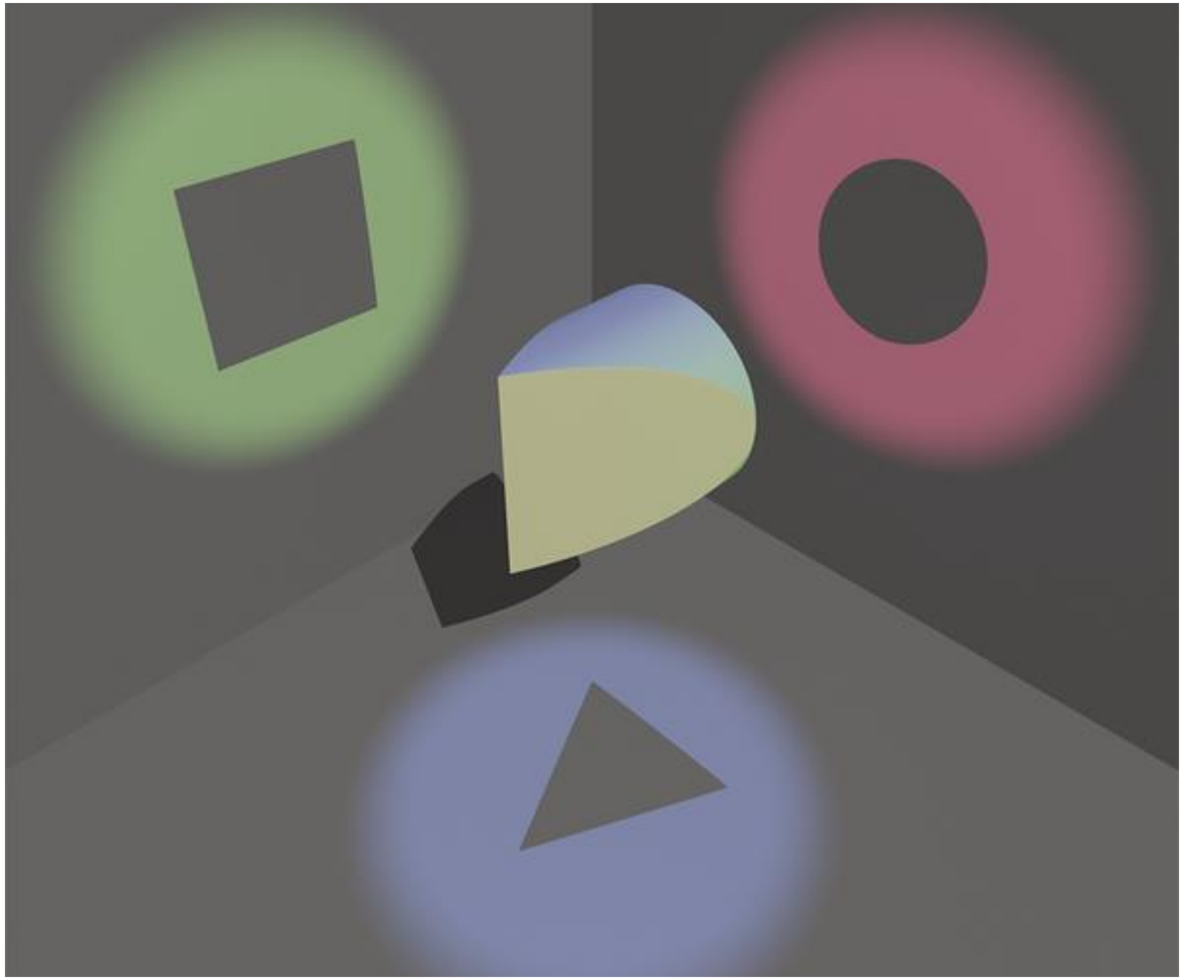
Annette Reilly

Rob Schaaf

Sinem Getir Yaman

What the process seemed like to me





What is Software Dependability?

An ideal definition would make it possible to answer questions like

- Is system *X* more dependable than system *Y*?
- How has system *X*'s dependability changed over time?
- What can we do to make system *X* more (less) dependable?
- How do we know system *X* is dependable?

Such a definition should make clear how dependability is different from:

- Trustworthiness
- Safety
- Security

What is Software Dependability?

IEEE 982.1-2005 defines *Dependability* as

> [The] trustworthiness of a computer system such that reliance can be justifiably placed on the service it delivers. Reliability, availability, and maintainability are aspects of dependability. (adapted from Lyu [B12])

982.1-2005, IEEE Standard Dictionary of Measures of the Software Aspects of Dependability

- Owing to ambiguities and the circularity of this definition, and to support international harmonization, the 982.1 working group is considering adopting the IEC definition.

What is Software Dependability?

dependability, <of an item>: ability to perform as and when required

Note 1 to entry: Dependability includes availability (192-01-23), reliability (192-01-24), recoverability (192-01-25), maintainability (192-01-27), and maintenance support performance (192-01-29), and, in some cases, other characteristics such as durability (192-01-21), safety and security.

Note 2 to entry: *Dependability is used as a collective term for the time-related quality characteristics of an item (emphasis added)*

IEC 60050-192:2015, International Electrotechnical Vocabulary (IEV) - Part 192: Dependability

What is Software Dependability?

Recall the key questions:

1) Is system *X* more dependable than system *Y*?
2) How has system *X*’s dependability changed over time?
3) What can we do to make system *X* more (less) dependable?
4) How do we know system *X* is dependable?

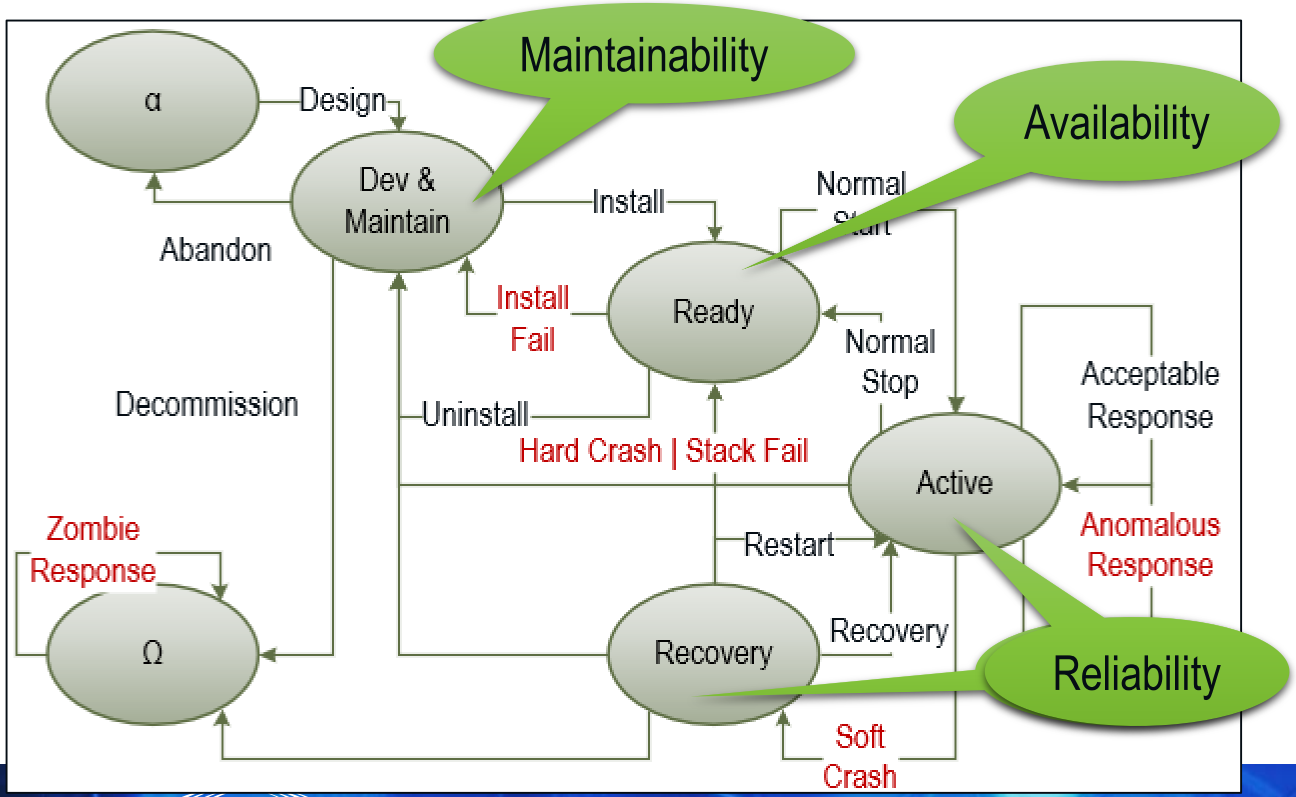
Neither definition of Dependability can provide a concise answer

- Both definitions are *rubrics* – neither defines Dependability as a measureable quality attribute.
- Why can’t we quantify Dependability?

Can Dependability be Quantified?

A Duty Cycle model was developed to experiment with quantification

Basic idea: set a budget for total cycle time and time to spend in each mode. Use the ratio of mode time to total cycle time as the weight for the corresponding quality attribute.



		OFFLINE	READY	ACTIVE	Total
Interval (1 year)	hrs				8760.0
Operational Budget	hrs	120	7688	952	8760.0
Dependability Threshold		0.90000	0.99999	0.99000	
Anti-D Tolerance		0.1	0.00001	0.01	
Dependability Threshold,	hrs	108.0	7687.9	942.5	8738.4
Dependability Budget		1.233%	87.762%	10.759%	
D-Factor Weight		1.370%	87.763%	10.868%	100.000%
Actual Hours	hrs	300	7570	890	8760
Actual MAR Metric		?	0.98466	0.94432	

Can Dependability be Quantified?

*In a word, **No.***

Problems

- Variability and scale of development ("big" *M*) confounds results
- Use "small" ***m,*** limited to file refresh without upstream effort?
- Restrict model to availability and reliability?

> *...a weighted average approach lacks statistical meaning. Specifically, there is no textbook method by which one can compute variance, confidence intervals, or related statistical inferences for these metrics.* - WG member comment

Dependability is a *Quality Outcome*

A ***Quality Attribute*** is a property of a tangible object that may be measured using an *Operational Definition.*

- Availability and Reliability are measurable quality attributes.

A ***Quality Outcome*** is a result defined with one or more quality attributes.

- It is an abstract category for characterizing related system effects that have practical importance to interested parties.
- Typically not quantifiable.

When, As, and Operating Conditions

> *"Dependability is the ability to perform* ***as and when required****"*

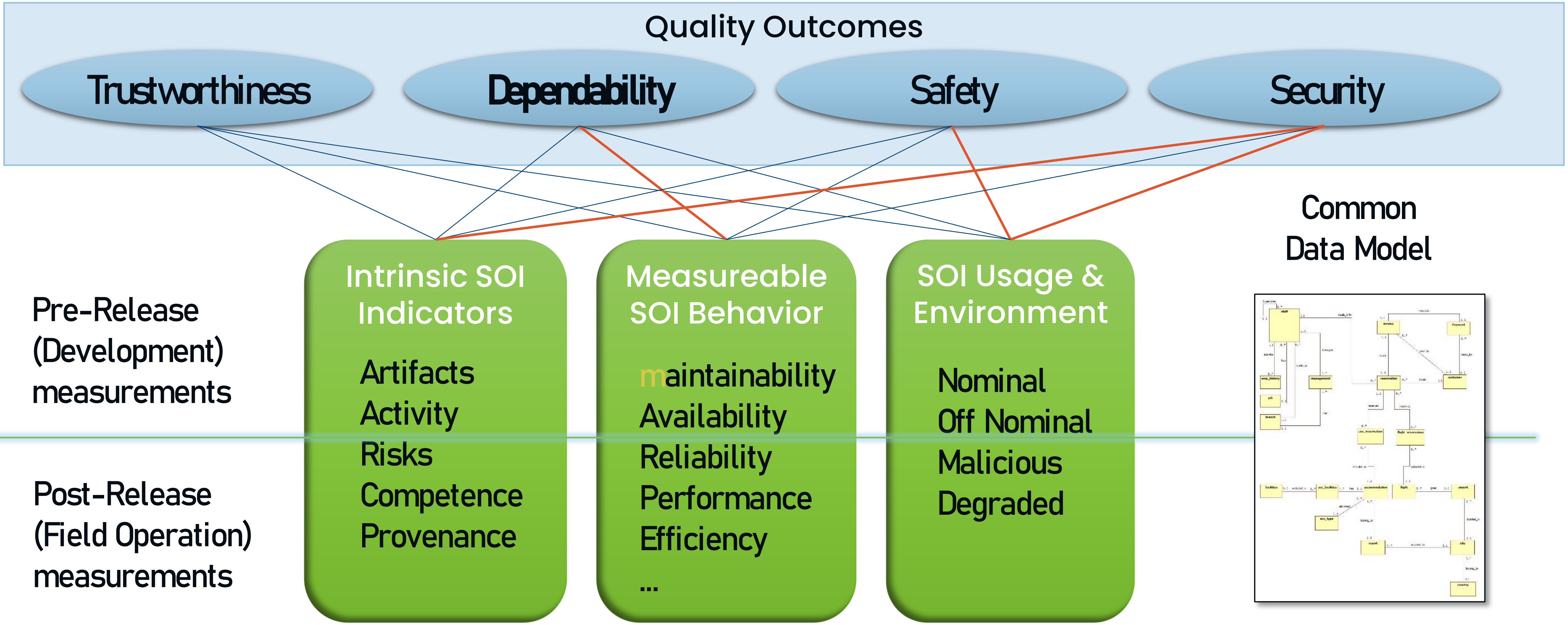
	Functionality	Safety	Security
	maintainable Available Correct, Timely Resilient …	Intended use does not harm interested parties …	No data spills Hack resistant Tamper resistant …
Nominal	✱	✓	✓
Off-Nominal	✱	✓	✓
Malicious	✓	✱	✱
Degraded	?	✱	✱

WHEN

Operating Conditions

AS – required behavior in test or field

All Quality Outcomes derived from same primary data sources



Quality Outcomes

Trustworthiness

Dependability

Safety

Security

Common Data Model

Pre-Release (Development) measurements

Post-Release (Field Operation) measurements

Intrinsic SOI Indicators

- Artifacts
- Activity
- Risks
- Competence
- Provenance

Measureable SOI Behavior

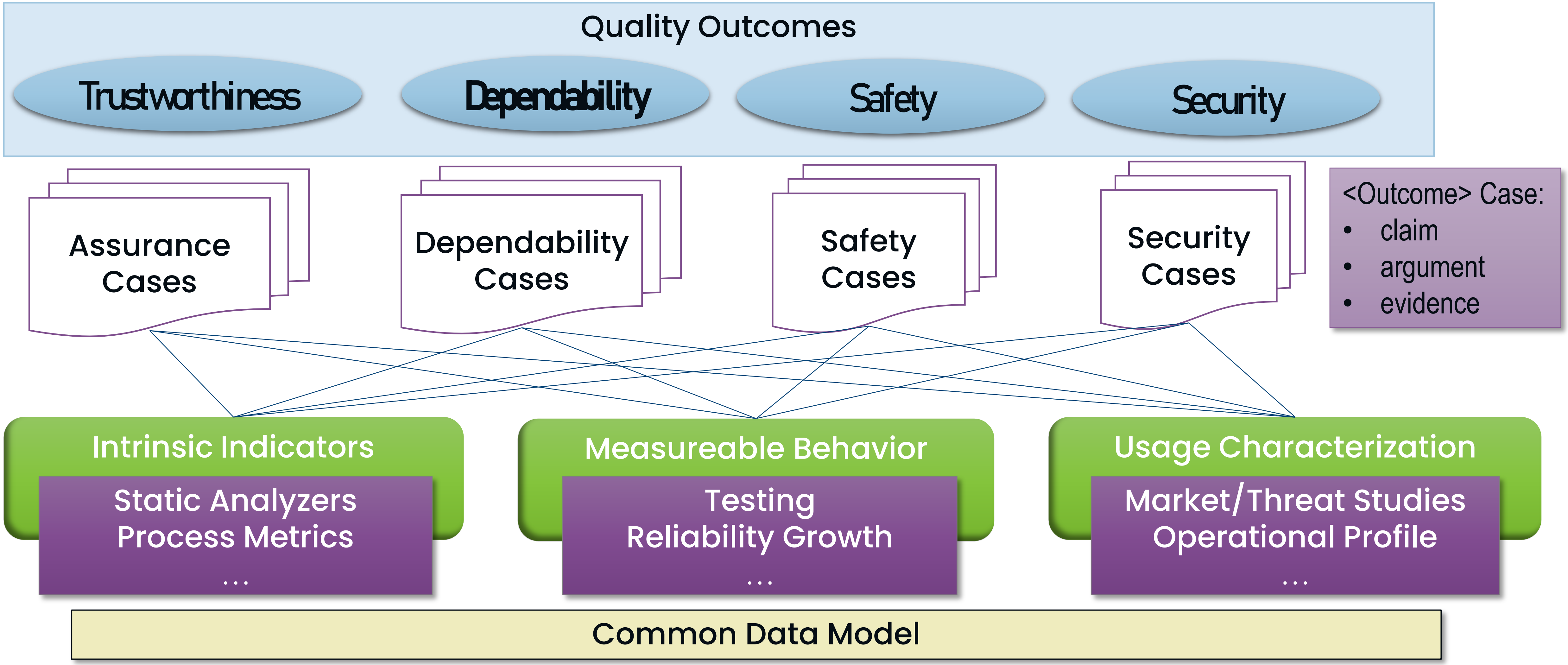
- maintainability
- Availability
- Reliability
- Performance
- Efficiency
- ...

SOI Usage & Environment

- Nominal
- Off Nominal
- Malicious
- Degraded

SOI – System of Interest

Pre-release analysis and prognostication



Quality Outcomes

Trustworthiness

Dependability

Safety

Security

Assurance Cases

Dependability Cases

Safety Cases

Security Cases

<Outcome> Case:

- claim
- argument
- evidence

Intrinsic Indicators

Static Analyzers
Process Metrics
. . .

Measureable Behavior

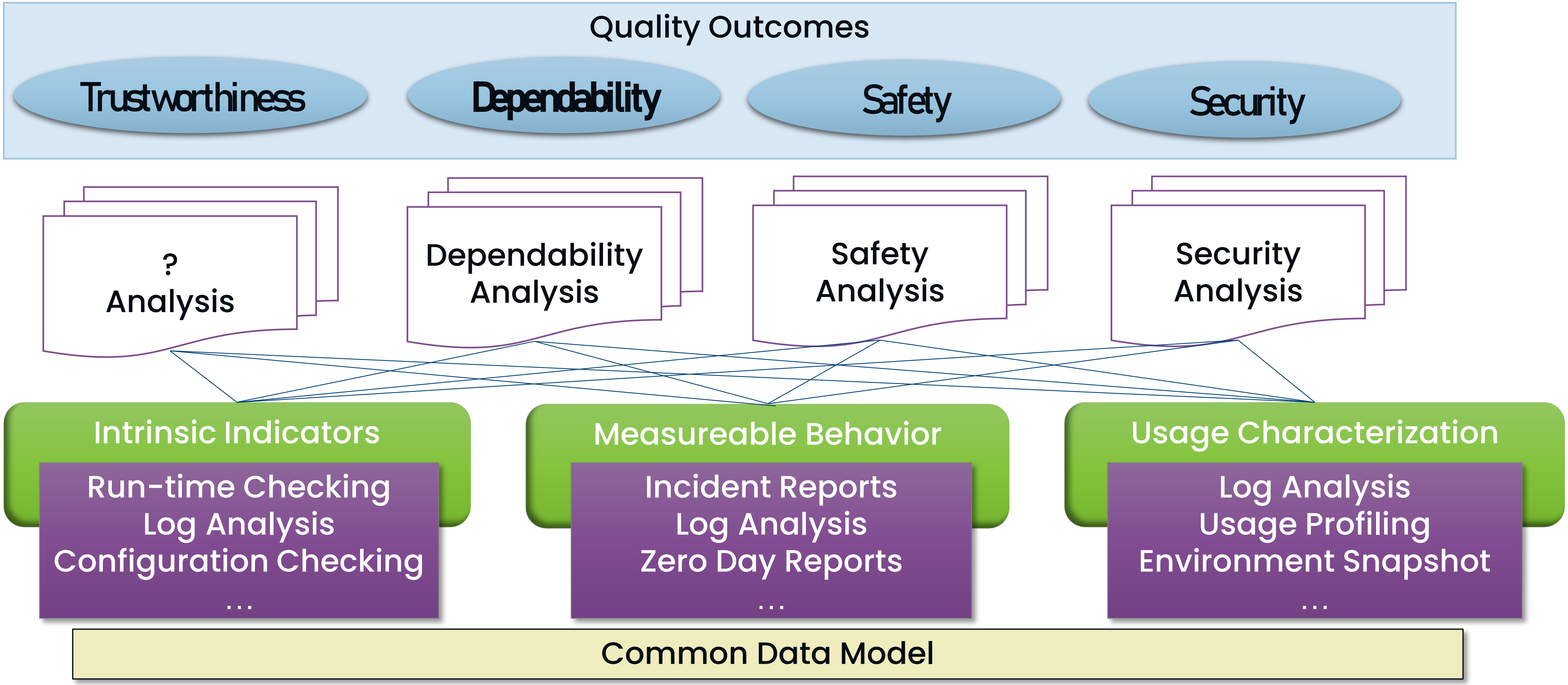
Testing
Reliability Growth
. . .

Usage Characterization

Market/Threat Studies
Operational Profile
. . .

Common Data Model

Post-release Monitoring



Quality Outcomes

Trustworthiness

Dependability

Safety

Security

? Analysis

Dependability Analysis

Safety Analysis

Security Analysis

Intrinsic Indicators

Run-time Checking
Log Analysis
Configuration Checking
...

Measureable Behavior

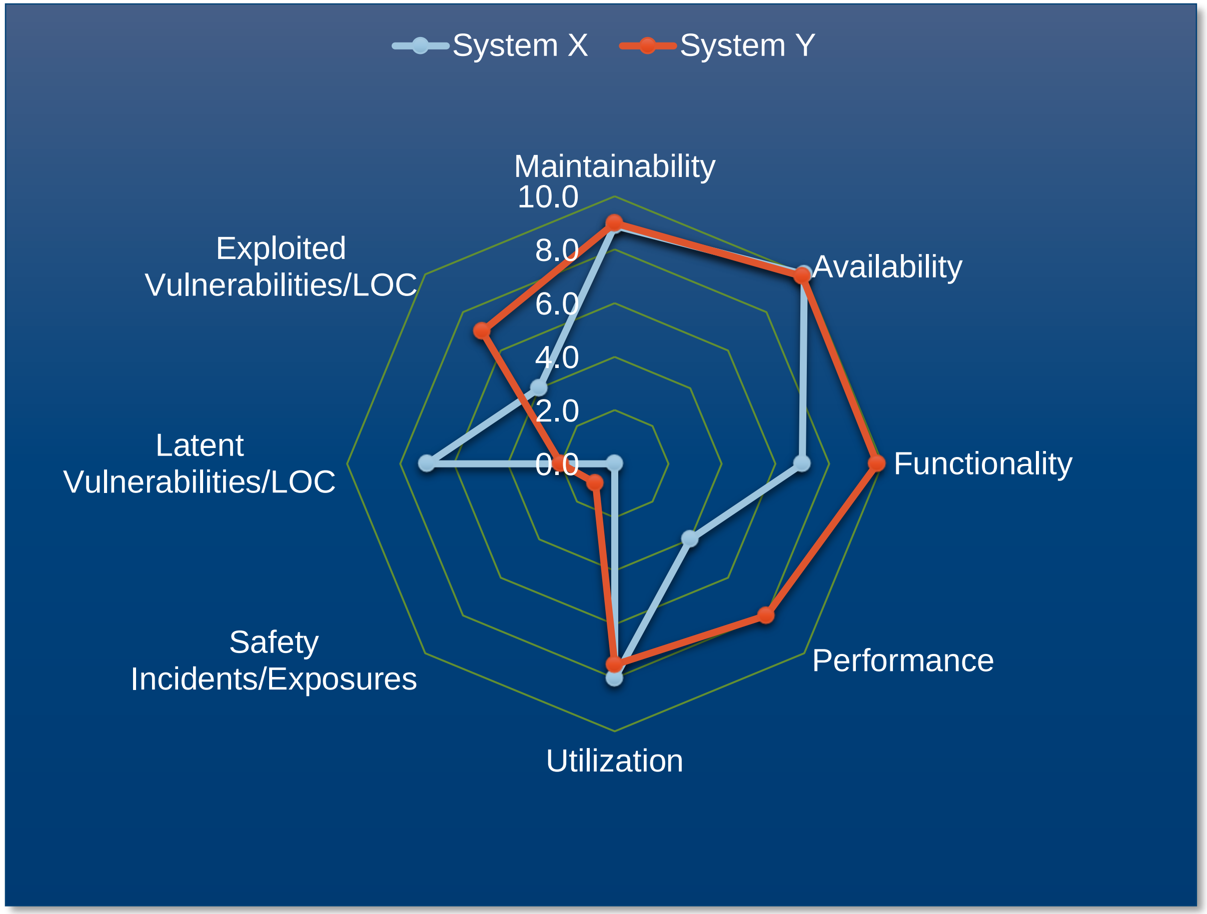
Incident Reports
Log Analysis
Zero Day Reports
...

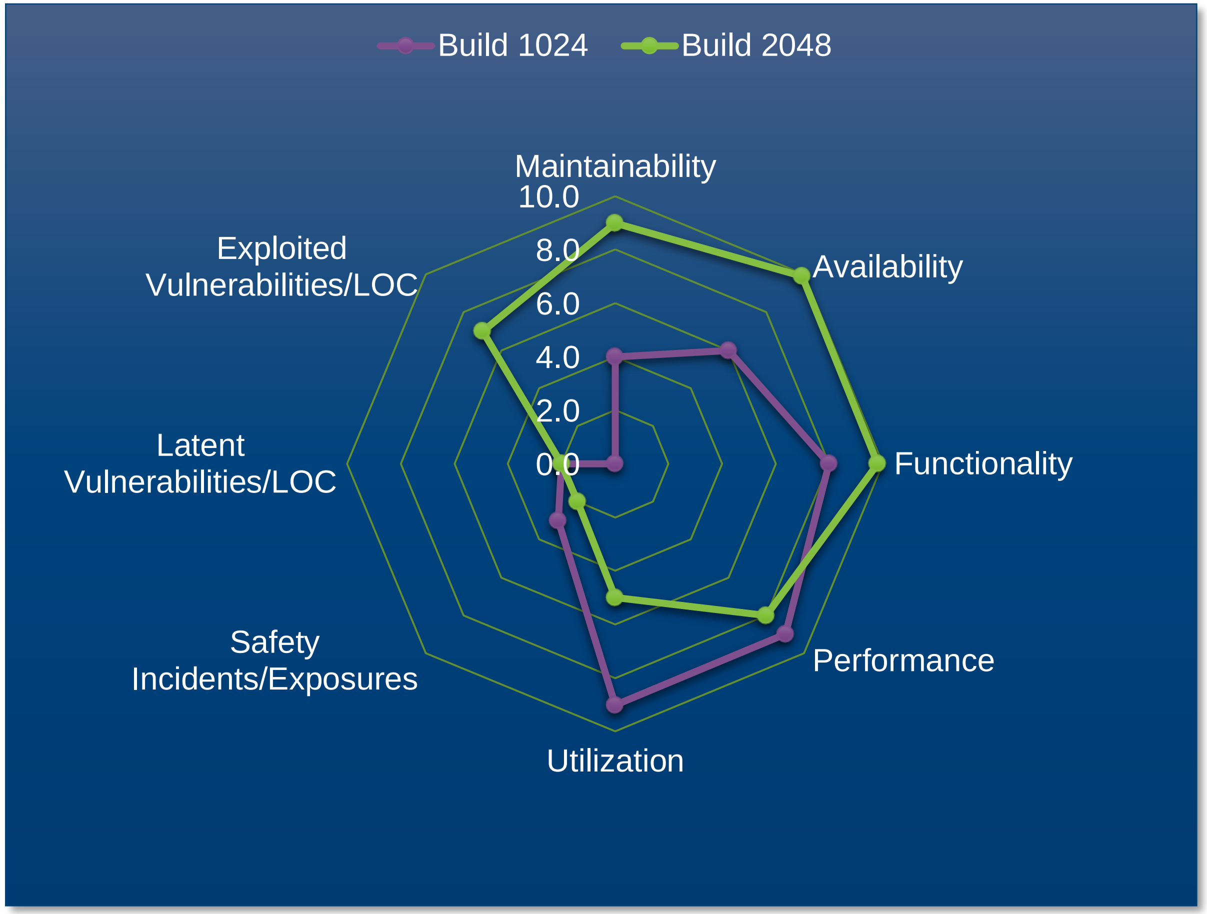
Usage Characterization

Log Analysis
Usage Profiling
Environment Snapshot
...

Common Data Model

Towards Comparing Dependabilities





982.1 Working Group highlights to date

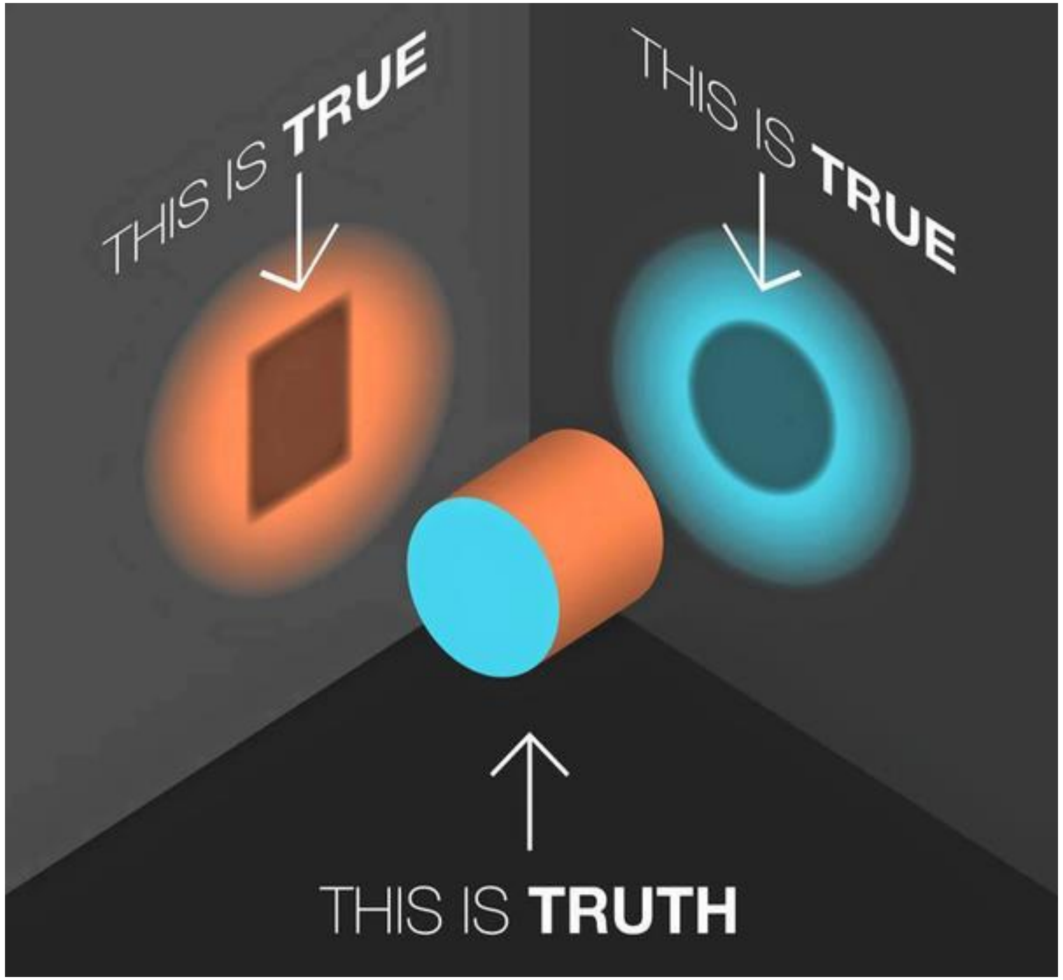
- Leaning towards IEC "ability to perform as and when required"
  - "As" – measureable quality attributes with threshold and target values
  - "When" – typical and adverse operational profiles
- Introduced the idea of a *"Quality Outcome"* to distinguish abstract categories from measurable properties.
  - *Dependability is a Quality Outcome*
  - Quality *Outcomes* bundle quantity attributes
- "Little ***m***" Maintainability (field updates, no-code re-configuration)
- Operational profiles for typical ***and*** adverse conditions are necessary for adequate assessment of pre-release dependability
- A common data model for pre- and post-release items will facilitate devops performance

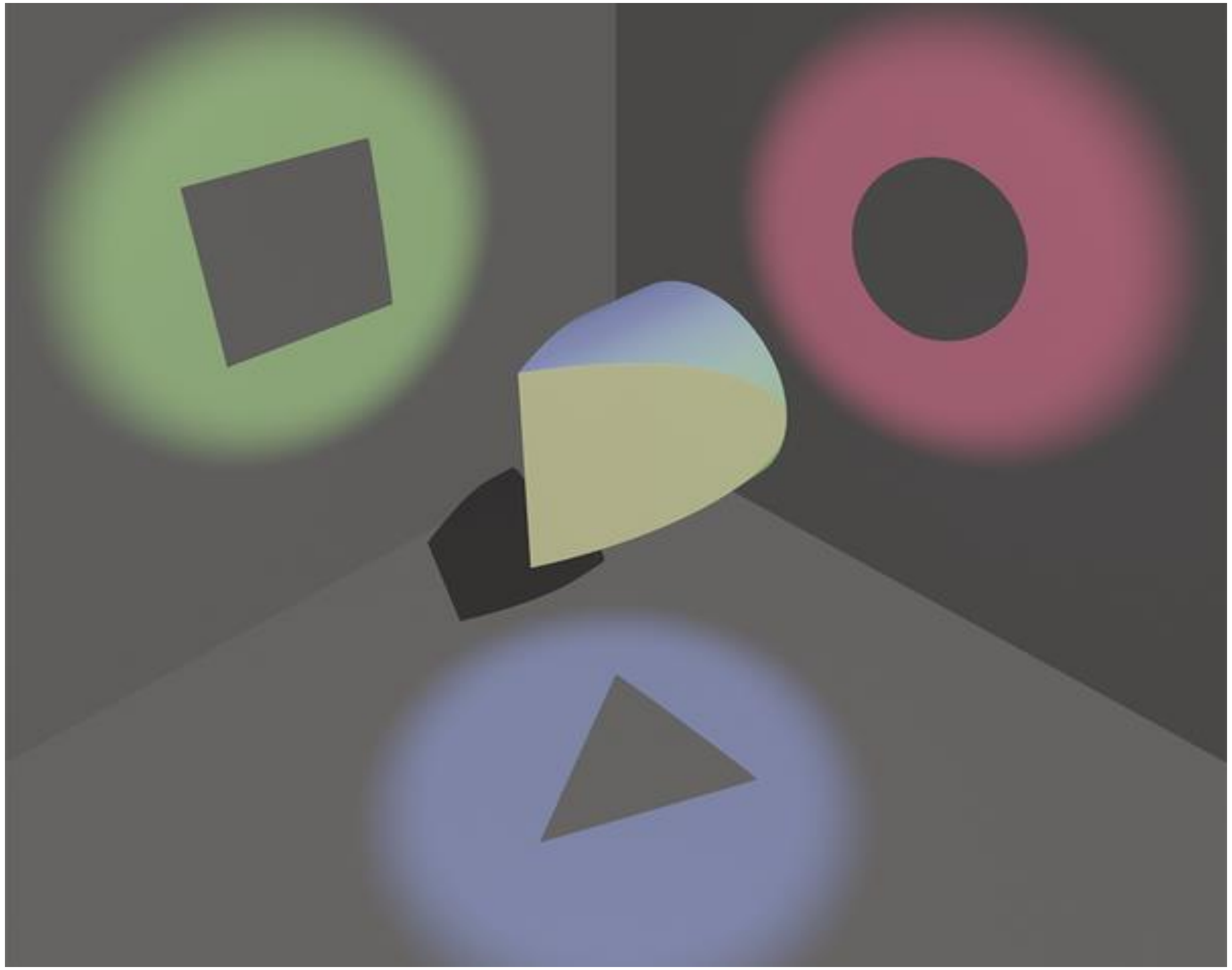
This presentation is snapshot of work in progress.

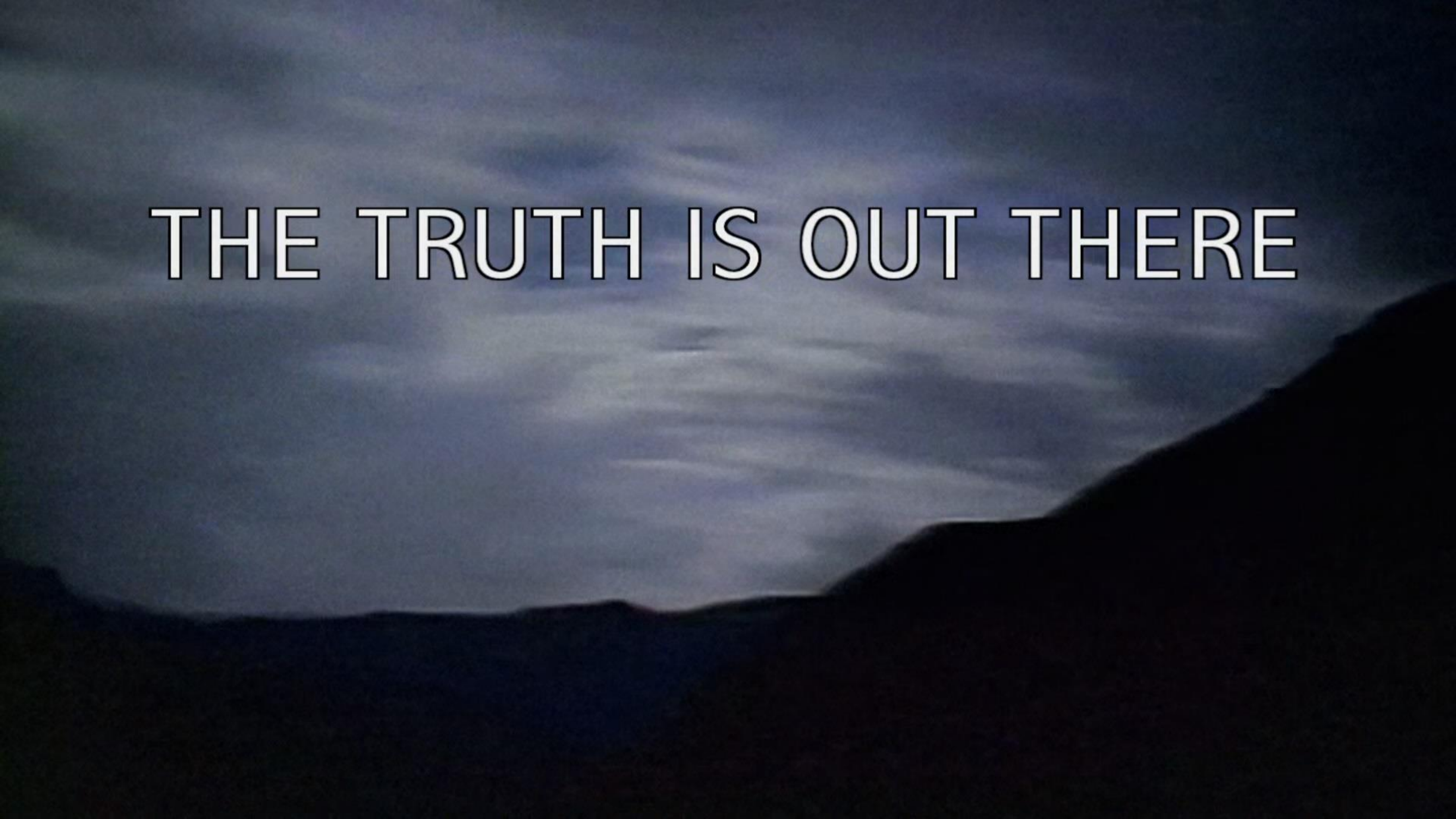
All concepts, terms, etc. are subject to change.

9th UCAAT

What the process seems like now







THE TRUTH IS OUT THERE

Thank you!
Any questions?

rbinder@ieee.org