31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

John S. Brtis
Principal Systems Engineer
The MITRE Corporation

Michael A. McEvilley
System Assurance Lead
The MITRE Corporation

Michael J. Pennock
Principal Systems Engineer
The MITRE Corporation

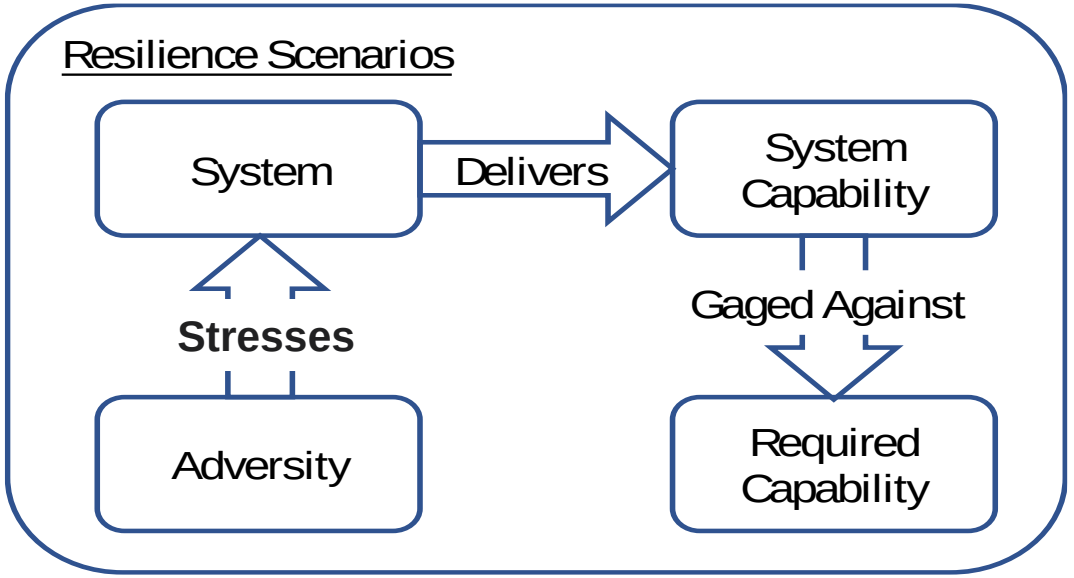
Patterns for Resilience Requirements

Working Definition of Resilience

What we mean by resilience:

Resilience is the ability to provide required capability when facing adversity.

(INCOSE SEBOK)



Resilience Requirements are Compound and Complex

- Resilience Requirements
  - functional/capability content
  - performance content
  - environment content
  - system state and mode content
  - often requirements about requirements
  - can have parameters that vary with time
- Making such a requirement computationally consumable and computer consumable adds to the challenge

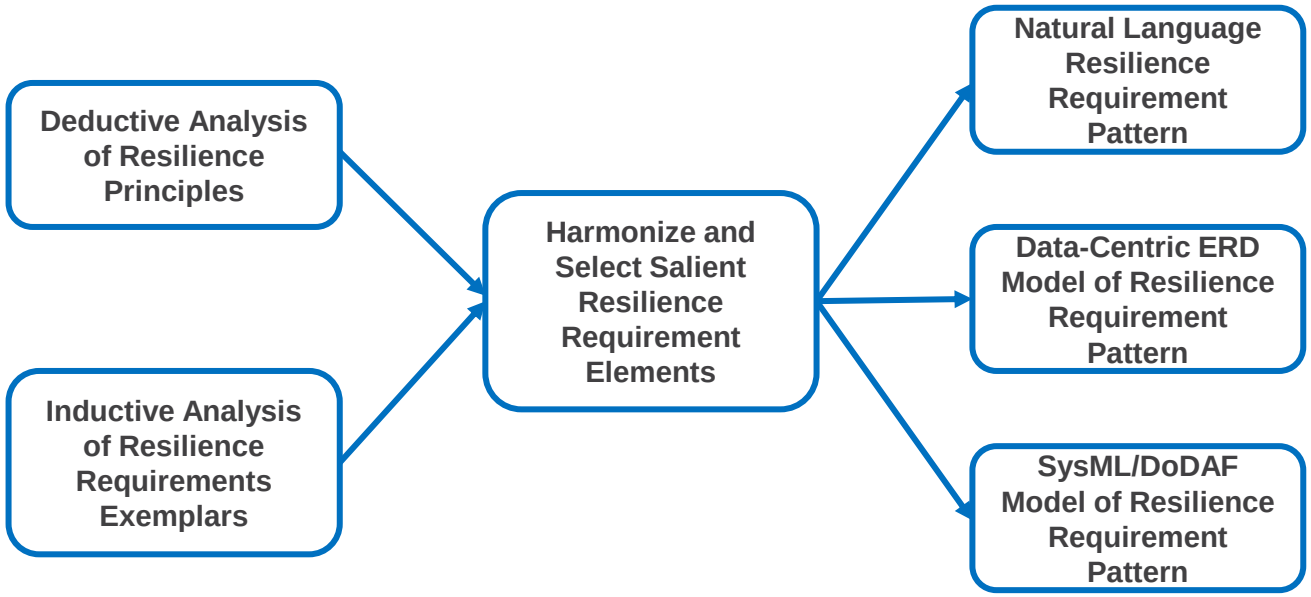
Most Models Capture Requirements as Unstructured Natural Language Text

- E.g., from the OMG SysML Standard
  - A standard requirement includes properties to specify its unique identifier and text requirement. Additional properties, such as verification status, can be specified by the user.
  - Attributes of Requirements
    - id:String The unique id of the requirement.
    - text:String The textual representation or a reference to the textual representation of the requirement.

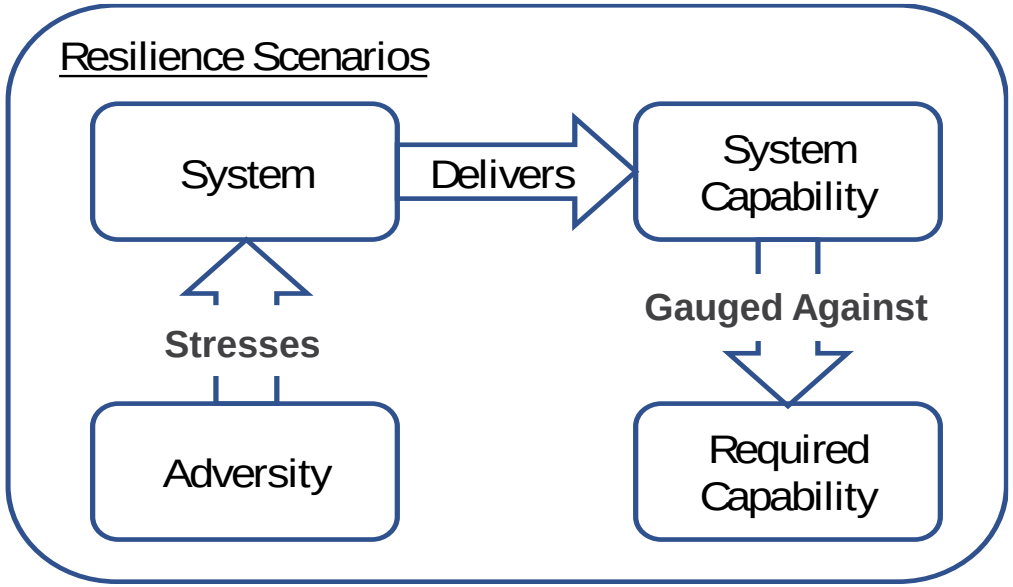
Our Goal

- Identify the underlying structure of resilience requirements
  - content
  - syntax
  - semantics
- Develop reusable patterns for resilience requirements
  - that are easily human readable
  - that are formal, rigorous and data-centric
  - that are computationally and computer consumable, supporting MBSE & DE

Our Approach

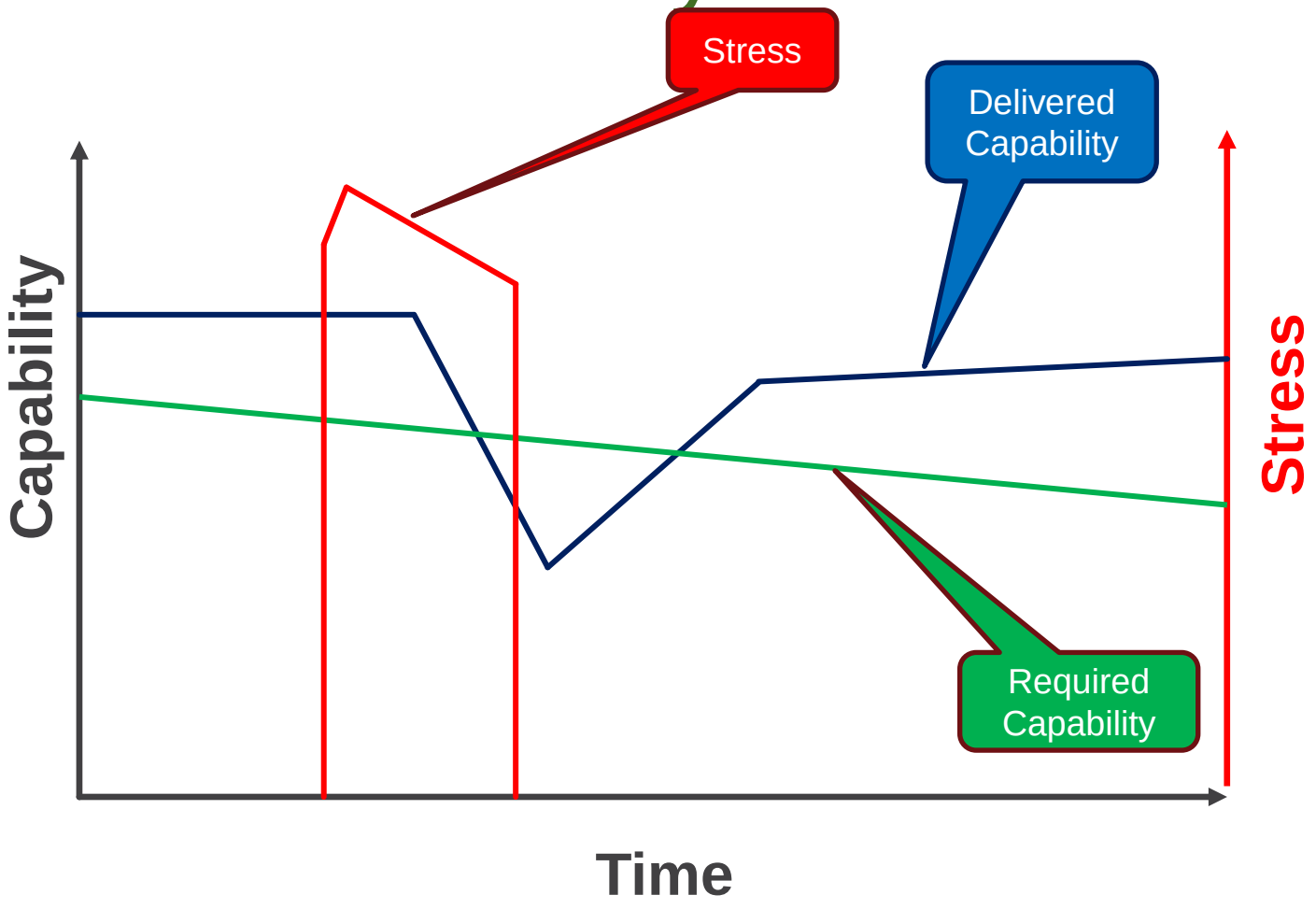


Deductive Analysis of the Resilience Definition



- <system or subsystem of interest>
- <system capability of interest>
- <adversity of interest>
- <stress imposed by the adversity on the system>
- <required capability level>

Deductive Analysis of the Resilience Scenario Lifecycle



- <scenario timeframe of interests>
- <time periods within the overall timeframe>
- <timewise variation in stress>
- <timewise variation in delivered capability>
- <timewise variation in required capability>
- <timewise modes of the system>
- <timewise states of the system>

Examples of Exemplar Requirements Evaluated

- light water reactors, acceptance criteria for emergency core cooling system (10CFR50.46)
- nuclear power plant, loss of coolant accident (10CFR50)
- nuclear power plant, loss of all alternating current power (10CFR50.56)
- hospital critical electric power system, loss of offsite power
- network protection (metro Ethernet forum 2004)
- aircraft design requirement, high-intensity radiation fields protection (14CFR23.2520)
- aircraft design requirement, system power generation, storage, and distribution (14CFR23.2525)
- NASA international space station lifeboat requirement

Inductive Analysis of a Resilience Exemplar

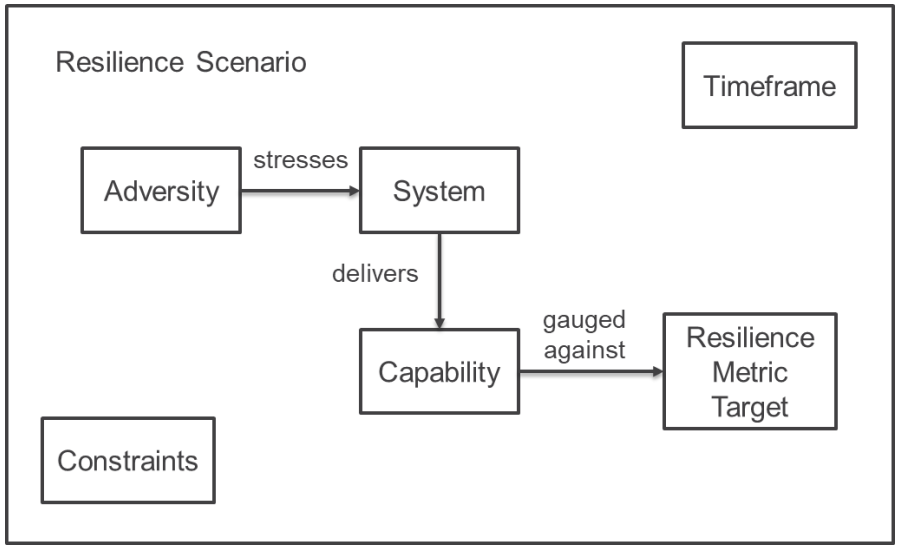
A hospital <system> experiencing adverse weather <adversity>, which causes the loss of quality offsite power <stress> affecting life-support critical AC power <subsystem>, shall without any maintenance or external resources <scenario constraint> for up to 72 hours <scenario timeframe>, achieve backup power <capability> at the nominal specified quality to all life-support critical AC power circuits within an initial 300 ms. <resilience metric, resilience units, resilience target>

Three Representations of the Resilience Requirements Pattern (simple, non-verbose versions)

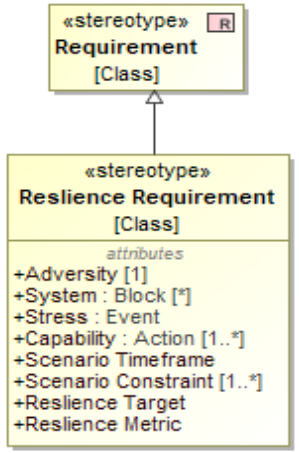
Natural language text pattern (simple form):

The <system> encountering <adversity>, which imposes <stress> affecting delivery of <capability> during <scenario timeframe> and under <scenario constraints> shall achieve <resilience target> for <resilience metric>.

ERD representation (simple form)



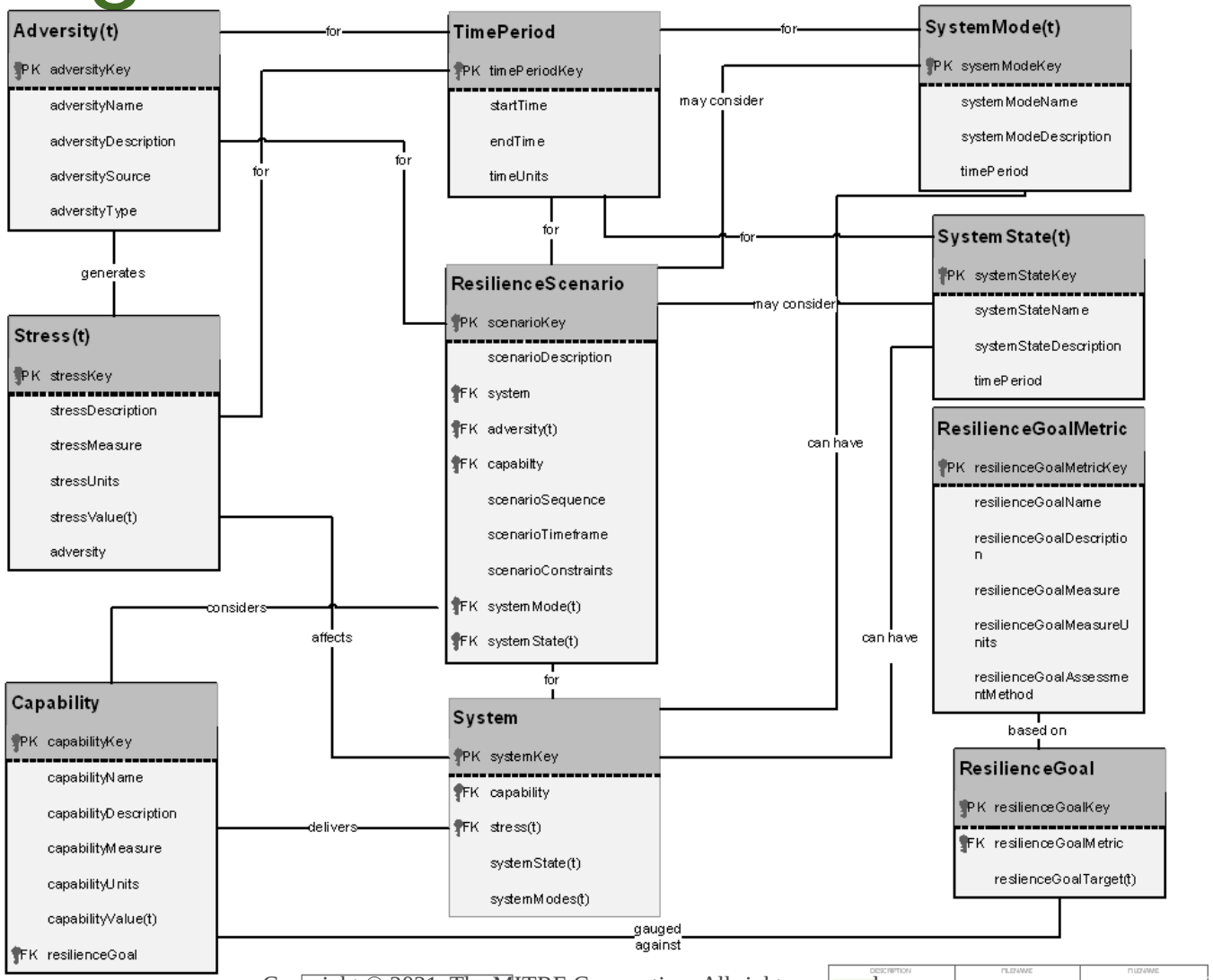
SysML Requirement Class Extension (simple form)



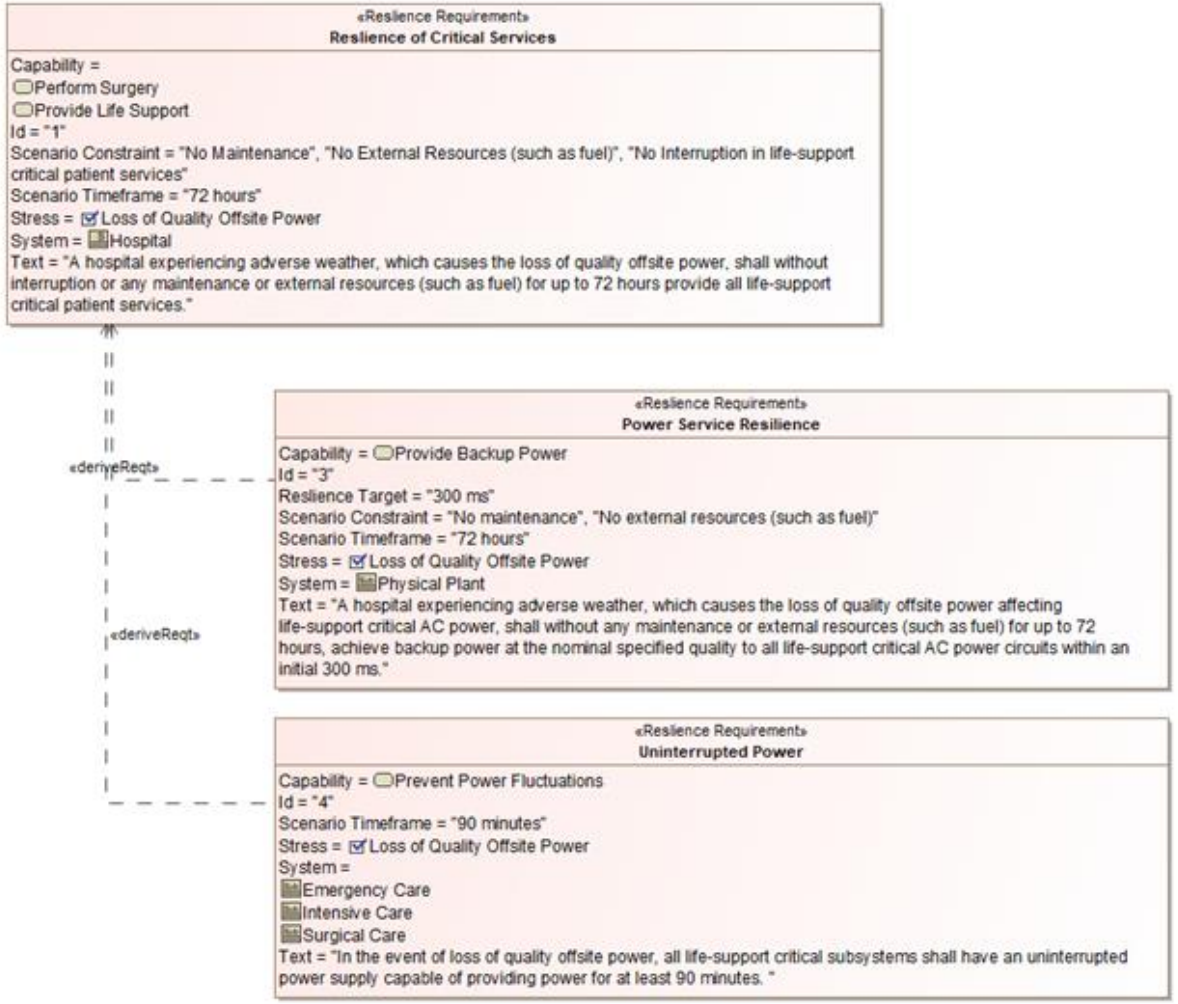
Verbose Natural Language Text Pattern

The <system, mode(t), state(t)> encountering <adversity(t), type> which imposes <stress(t)> thus affecting delivery of <capability, required capability(t), capability metric, units> during <scenario timeframe> and under <scenario constraints(t)> shall achieve <resilience target(t)> for <resilience metric, units>

Verbose Logical ERD of the Pattern



SysML Requirement (Stakeholder and System): Hospital Emergency Power Example



Mapping of Elements to SysML

Element	SysML Entities	Comments
System	Block	The system of interest should be captured as a block in both a block definition diagram and an internal block diagram. The internal block diagram should document the flows that will be stressed during the resilience scenario.
System State	State	System states should be captured in a state machine diagram where the stress triggers a state transition.
System Mode	State	System modes relevant to the resilience requirement should be captured in the state machine diagram.
Adversity	Actor, Block, State, Event	SysML has multiple valid ways to represent an adversity. The most appropriate will depend on the nature of the adversity. For example, a malicious actor may be best represented as a SysML Actor while a SysML event can represent a random failure.
Capability	Activity/Action	In the context of SysML, capabilities should be documented using activities as they relate to a system's behavior. As the capability is decomposed during the architecting process, it may be necessary to derive additional resilience requirements that apply to the activities and functions that provide the capability. These activities will serve as the capability for each of these derived requirements.
Stress	Event, Value Property, Flow Property, Constraint	SysML has multiple ways to represent a stress. The most appropriate will depend on the nature of the stress. An instantaneous change may be captured using an event while a time varying stress may require a more complex description in a property or constraint. A parametric diagram can aid in documenting complex relationships (See SysML 1.5 Annex E).
Resilience Metric	Value Property	Specific resilience metrics can be documented in a SysML value property.
Resilience Target	Value Property, Constraint	Simple, fixed-point targets may be captured in value property or constraints. More complex relationships may be better expressed through a parametric diagram (See SysML 1.5 Annex E).
Scenario Timeframe	Value Property, Constraint	Timeframes can be documented in a SysML value property or constraint.
Scenario Constraints	Constraint	Documenting scenario constraints will depend on the nature of the constraint. Parametric constraints can be captured using values, constraints, and parametric diagrams (See SysML 1.5 Annex E). Qualitative constraints such as, "no external resources such as fuel" can be captured textually using either an extended resilience requirement stereotype or a constraint with a textural specification.

Mapping of Elements to DoDAF

Element	DoDAF 2.02 Viewpoints	Comments
System	SV-1, Svc-1	The systems or services to which the resilience requirement will apply will typically be defined as blocks in the SV-1 or SvcV-1 view, which describes system components and their interfaces. The system is linked to the capabilities it provides via a chain of traceability through functions to operational activities to capabilities. (e.g., SV-4 to SV-5a to CV-6). One possible exception to this would be when the resilience requirement applies to an organization (e.g., a brigade). In that case the "System" may be an organization documented in the OV-4.
System State	OV-6b, SV-10b, SvcV-10b	DoDAF has two different levels of state machines. Operational level state machines are captured in the OV-6b while system level state machines are documented in the SV-10b for systems or the SvcV-10b for services. States related to the resilience requirement should be captured in one of these views depending on the level of the requirement.
System Mode	OV-6b, SV-10b, SvcV-10b	DoDAF has two different levels of state machines. Operational level state machines are captured in the OV-6b while system level state machines are documented in the SV-10b for systems or the SvcV-10b for services. Modes related to the resilience requirement should be captured in one of these views depending on the level of the requirement.
Adversity	OV-6c, SV-10c, SvcV-10c,	The specific implementation of an adversity will vary, but it should at least appear in the sequence diagram view appropriate for the level of resilience requirement (OV-6c, SV-10c, or SvcV-10c). If the adversity is modeled as an event (e.g., a random failure), it should be a transaction in the sequence diagram. If it is modeled as an actor or block (e.g., a malicious actor), it should have a lifeline in the sequence diagram.
Capability	CV-2, OV-5a/b, SV-4, SvcV-4	In DoDAF, high-level capabilities are captured in the CV-2. These capabilities are provided by operational activities from the OV-5. These operational activities are dependent, in part, on functions described in the SV-4/SvcV-4. Depending on the level of resilience requirement, the capability should be captured in one of these views.
Stress	OV-6b, SV-10b, SvcV-10b, OV-6c, SV-10c, SvcV-10c, SV-6, SvcV-6	Modeling a stress in DoDAF will likely involve multiple views and be dependent on the nature of the stress. At a minimum, it should be modeled in the OV-6 for operational level requirements or the SV-10/SvcV-10 for system/services level requirements. Each is made up of three sub-views (a, b, and c) that are closely interrelated. The 'b' view is a state machine, and the 'c' view is a sequence diagram. An instantaneous stress can be a trigger event in the state machine and/or a transaction in the sequence diagram. If both views are used, they should be mutually consistent. More complex stress trajectories (e.g., decreasing available power over time) may require documentation in the SV-6/SvcV-6 resource flow matrix to maintain the linkage to the affected resource flows, if any.
Resilience Metric	SV-7, SvcV-7	At the systems and services level, a specific view, the SV-7/Svc-7, is intended to document key performance metrics. If the resilience requirement applies to the operational level, the metric may need to be defined in the OV-6a along with the resilience target.
Resilience Target	OV-6a, SV-10a, SvcV-10a	Constraints and targets can be captured in the operational rules model (OV-6a) for operational level requirements and the system/services rule model (SV-10a/SvcV-10a) for system level requirements.
Scenario Timeframe	OV-6a, SV-10a, SvcV-10a	Constraints and targets can be captured in the operational rules model (OV-6a) for operational level requirements and the system/services rule model (SV-10a/SvcV-10a) for system level requirements.
Scenario Constraints	OV-6a, SV-10a, SvcV-10a	Constraints and targets can be captured in the operational rules model (OV-6a) for operational level requirements and the system/services rule model (SV-10a/SvcV-10a) for system level requirements.

A Few of the Interesting Findings

- Elements not in “normal” requirements: adversities, stresses, resilience metrics & targets, scenario information.
- Definite need to extend SysML requirements class to capture the critical content of resilience requirements
- Resilience requirements often take the form of scenarios, which are well modeled as SysML Use Cases.
- Adversities can be represented as SysML actors.
- Identifying stress as the proximate adversity can be important
- Stress may appear in SysML as triggers on state diagrams.
- Resilience metrics often differ from the capability of interest metric.

Next Steps

- We believe most loss-driven systems engineering specialty areas (security, safety, operational risk, quality, availability, etc.) have similarly complex requirements.
- We are working on patterns for security and plan to pursue other loss-driven systems engineering specialty areas.
- It may be possible to develop a unified set of requirements patterns that address all loss-driven areas.
- I suggest that INCOSE establish a curated repository of requirements patterns.

Key Terms

Adversity – (for the purpose of resilience) anything that can degrade the desired capability of a system. (SEBOK 2019)

Capability – ability to achieve a specific objective under stated conditions. (INCOSE SEH).

Entity Relationship Diagram (ERD) – a diagrammatic modeling tool that shows entities, their attributes and the relationships among the entities

Mode – a design-significant type of intended operation of the system. E.g., normal operation mode, training mode, testing mode etc.

Metric – quantitative measure of the degree to which a system, component, or process possesses a given attribute. (ISO/IEC/IEEE 2010)

Natural Language – A human written or spoken language as opposed to a computer language.

Pattern -- a pattern is an idea that has been useful in one practical context and will probably be useful in others. (Fowler 1997)

Requirement – a statement that translates or expresses a need and its associated constraints and conditions (ISO/IEC/IEEE 29148:2011)

Resilience – the ability to provide required capability in the face of adversity. (SEBOK 2019)

Scenario – a resilience scenario is a specific sequence of situations illustrating behavior of a system in the face of adversity. A scenario should describe the capability to be delivered and the environment and other conditions under which this will be performed.

State – a condition of existence that a system, component or simulation may be in (ISO 24765-2010)

Stress – a force or influence directly affecting the system that could cause degradation of the system's ability to deliver required capability.

Systems Modeling Language (SysML) – a modeling language that extends the unified modeling language (UML) to address the needs of modeling systems.

System – an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not. (INCOSE SEH)

Target – the intended outcome (ISO 24765-2010).

Contact Information

John S. Brtis, jbrtis@johnsbrtis.com
Michael A. McEvilley, mcevilley@mitre.org
Michael J. Pennock, mpennock@mitre.org

31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021