Booz | Allen | Hamilton

A PRAGMATIC APPROACH TO SYSTEM MODELING FOR HAZARD IDENTIFICATION AND RISK MANAGEMENT

Michael J. Vinarcik, ESEP-Acq, OCSMP-Model Builder Advanced

2017 National Defense Industrial Association

Systems Engineering Conference

OCTOBER 26, 2017

UNCLASSIFIED: Distribution Statement A. Approved for public release; distribution is unlimited.

CONTACT INFORMATION

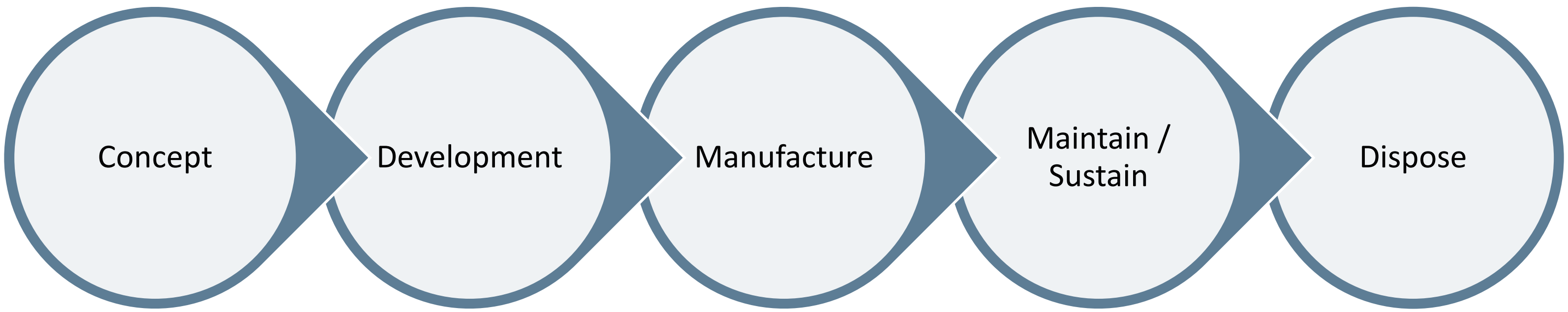
Michael J. Vinarcik

248-227-1659

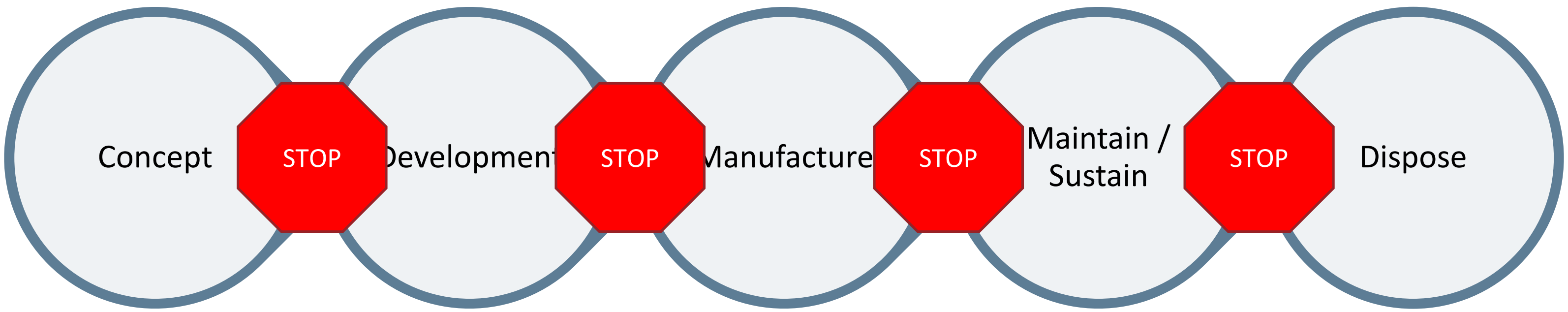
Booz Allen Hamilton

vinarcik_michael@bah.com

AN ABSTRACT VIEW OF PRODUCT DEVELOPMENT



AIR GAPS



Fidelity and momentum is lost every time there is a handoff; this is caused by the “air gaps.”

INDUSTRIAL AGE VS. INFORMATION AGE

"Our current defense acquisition system applies industrial age processes to solve information age problems."

- LtGen Robert D. McMurray, AFLCMC/CC
  Keynote address
  2017 Wright Dialogue With Industry Conference,
  Dayton OH, 18 July 2017

YOU HEAR THAT, MR. ANDERSON? … THAT IS THE SOUND OF INEVITABILITY…

Agent Smith, *The Matrix*

DIGITAL ENGINEERING

- The Department of Defense is developing a strategy to transform its end-to-end acquisition process.
- It is expected to be released for use by 2019.
- This presentation will focus on methods that ESOH professionals can use to smoothly integrate their efforts with digital engineering.
- The following four slides are extracted from another presentation here at the NDIA SE Conference; please seek out Ms. Philomena Zimmerman or her team for more information.
- I have indicated where this presentation supports the strategy.

DoD Digital Engineering Strategy

Ms. Philomena Zimmerman
Deputy Director, Engineering Tools and Environments
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

UNCLASSIFIED

Digital Engineering Strategy: Five Goals

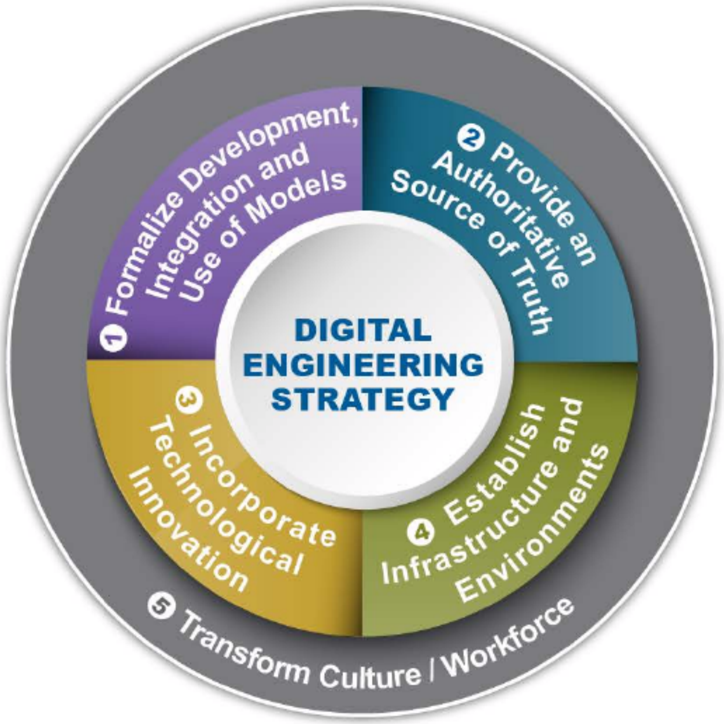
1 Formalize the **development, integration and use of models** to inform enterprise and program decision making

2 Provide an enduring **authoritative source of truth**

3 Incorporate **technological innovation** to improve the engineering practice

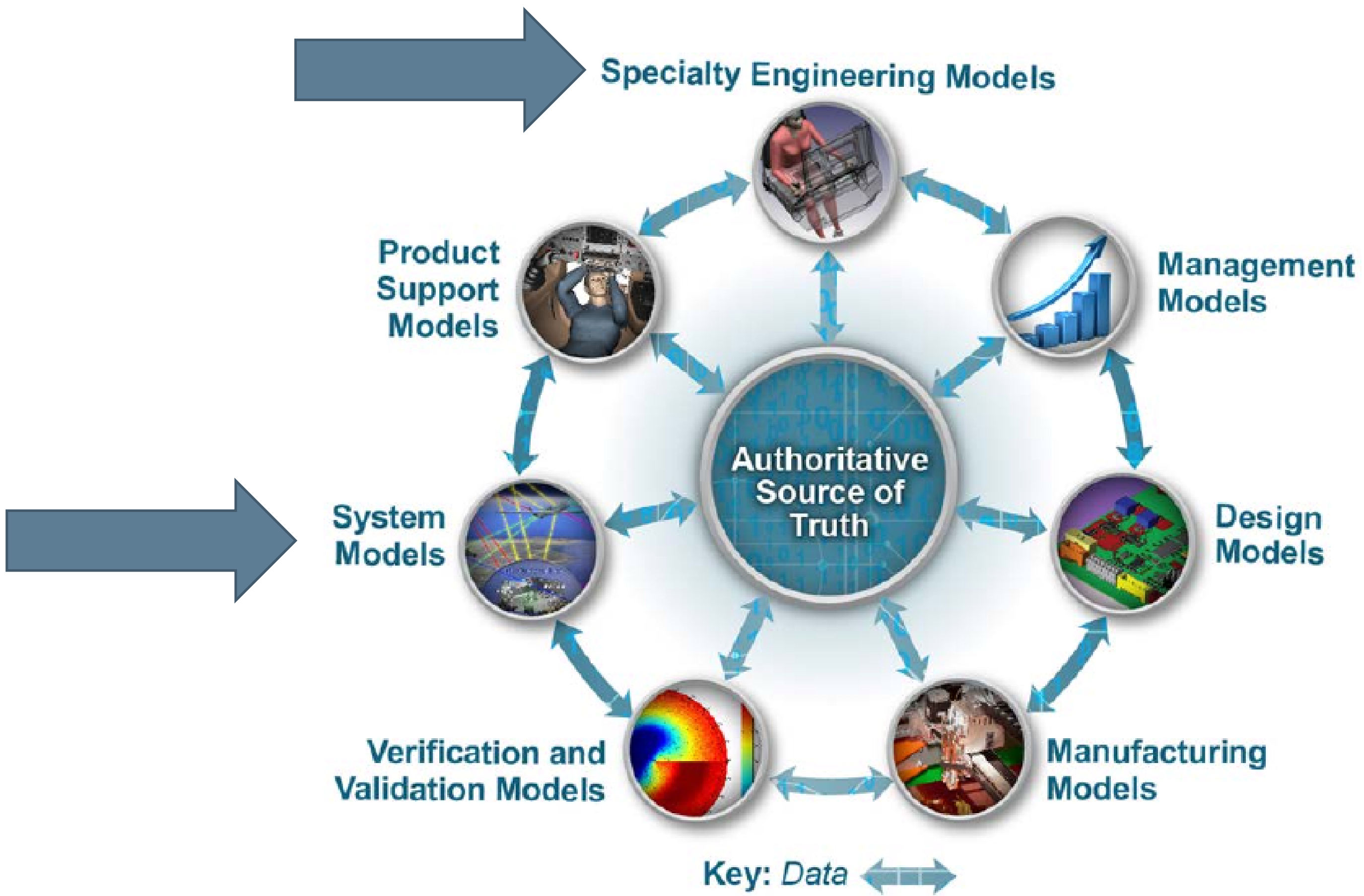
4 Establish supporting **infrastructure and environments** to perform activities, collaborate, and communicate across stakeholders

5 Transform a **culture and workforce** that adopts and supports Digital Engineering across the lifecycle



Drives the engineering practice towards improved agility, quality, and efficiency, which results in improvements in acquisition

Goal #1: Formalize Development, Integration & Use of Models



Models as the cohesive element across a system‚s lifecycle

For Additional Information

Philomena Zimmerman

ODASD, Systems Engineering

571-372-6695 | philomena.m.zimmerman.civ@mail.mil

Other Contributors:

Tracee Walker Gilbert, Ph.D.

571-372-6145 | tracee.w.gilbert.ctr@mail.mil

Frank Salvatore

973-265-9837 | frank.j.salvatore.ctr@mail.mil

Tyesia Pompey Alexander, Ph.D.

571-372-6697 | tyesia.p.alexander.ctr@mail.mil

Darryl Howell

571-372-6699 | Darryl.l.Howell.ctr@mail.mil

SYSTEM MODELING

- System modeling is emerging as a way to manage the inherent complexity of modern systems by providing a mechanism to store, manage, and associate information about a system under development.
- This information can then be extracted and presented to stakeholders in formats relevant to them.

Models grow organically as detail is added with no loss of fidelity.

from *Modeling Safety and CyberSecurity Controls in SysML,* 2016 NDIA Systems Engineering Conference, Vinarcik

SYSML: THE SYSTEMS MODELING LANGUAGE

- SysML is the most widely-adopted modeling language and has a thriving tool ecosystem.
- A well-constructed system model unambiguously represents a system's behavior, structure, and interrelationships between elements.
- Its flexibility allows integration of other discipline-specific analyses
  - Reliability
  - Safety

BENEFITS OF INTEGRATION

- Eliminating other tools from the analysis chain pays dividends:
  - Reduction in license costs
  - Elimination of interface/integration
  - Improved visibility to all stakeholders
  - Common language and understanding

Reduce lag and drag!

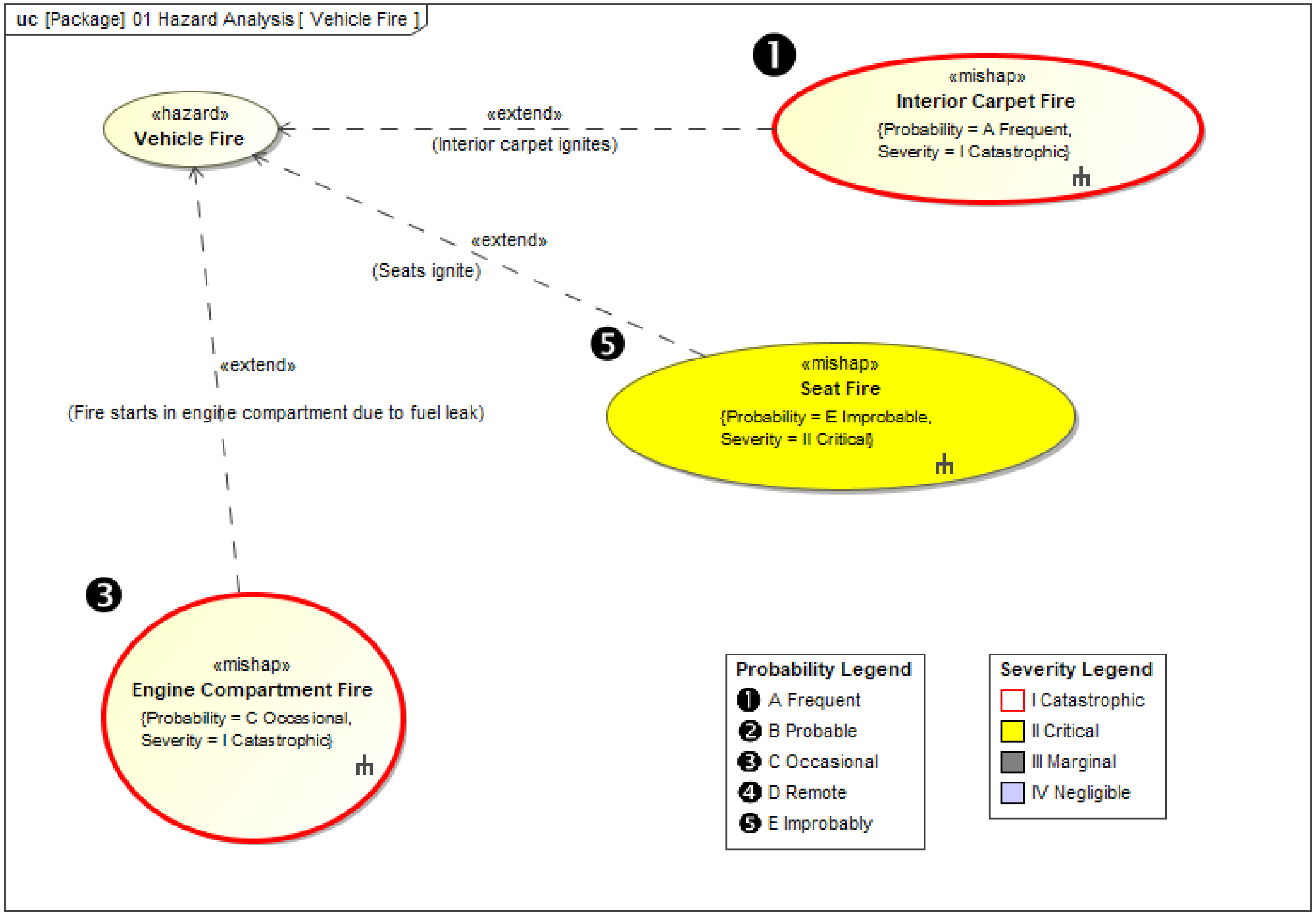
AN EXAMPLE: NOTIONAL PASSENGER AUTOMOBILE

- An unclassified, non-DoD example was needed for this presentation.
- A notional automobile is used as the basis for this example, which uses “fire” as the hazard.
- Note: I am not an ESOH professional and this is provided as an example of one approach to integrate ESOH into an evolving system model.

A REQUIRED MINDSET SHIFT

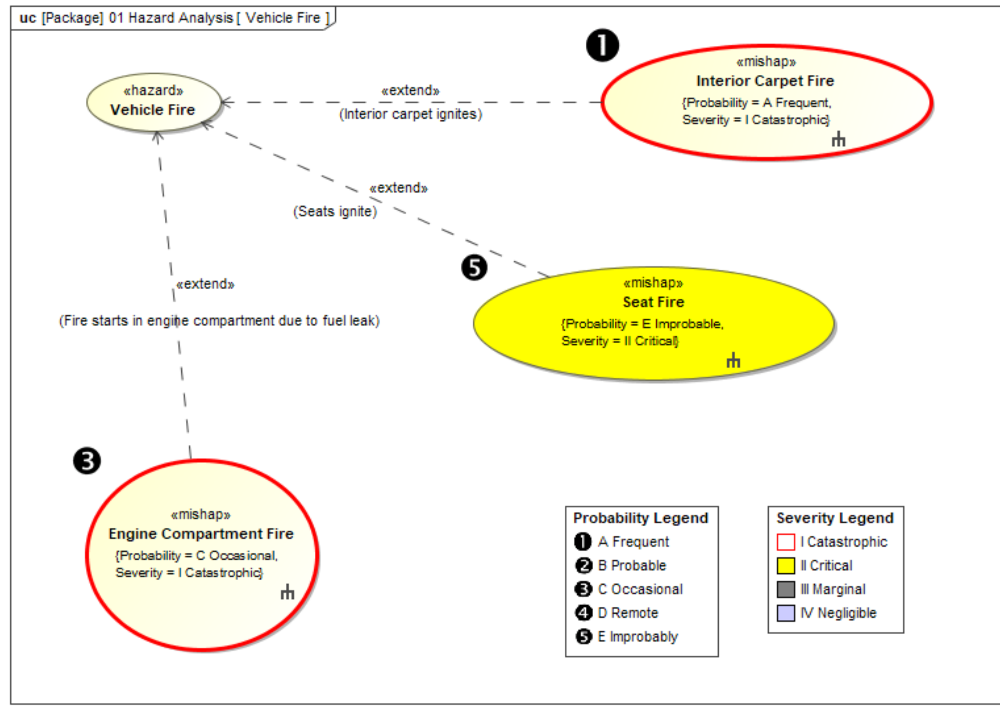
- To successfully leverage SysML, any user must understand that it is not “about” the diagrams.
- What is truly important is:
  - Elements and their properties
  - Relationships, their properties, and what they connect
- Once you see analyses in these terms, representing them in a system model is much easier.
- The collection of elements (including logic/branching elements) permits a rich description of system behavior, structure, interfaces, and parametrics.

NOTIONAL HAZARD ANALYSIS



HAZARD ANALYSIS: ELEMENTS USED

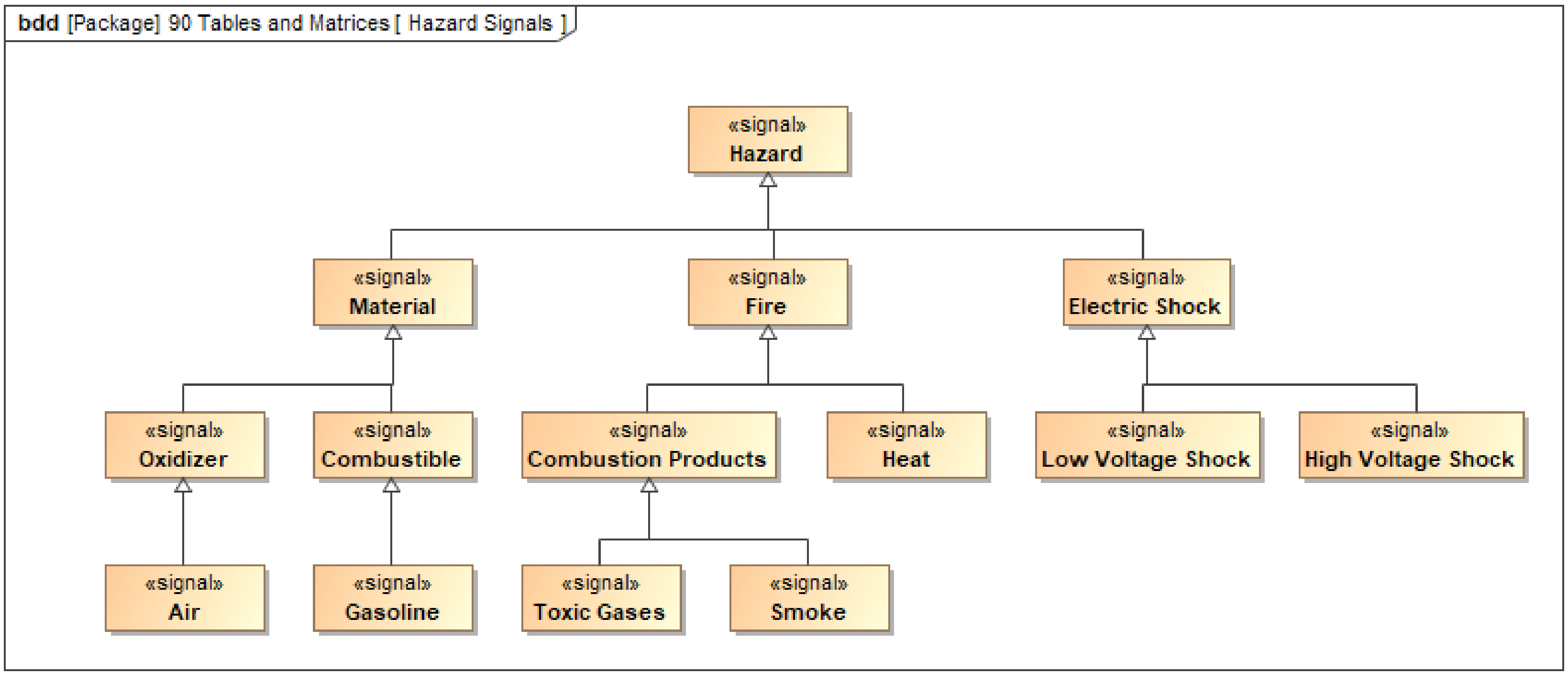
- *Use cases* with <<hazard>> and <<mishap>> stereotypes
- *Extension points* as causal factors
- <<extend>> relationships between mishaps and hazard
- Dynamic legends (color, fill, and icons based on properties of the elements)



WHY USE CASES?

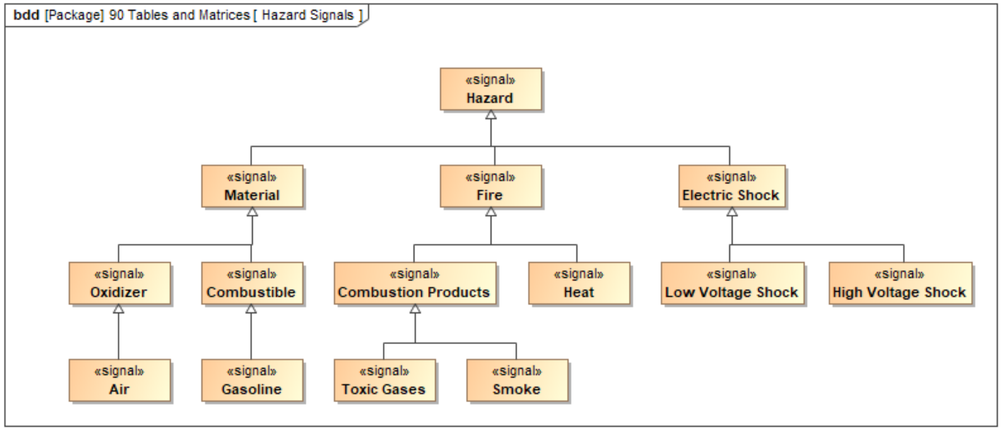
- *Use cases* are convenient SysML representations of behavior. They include:
  - *<<extend>>* relationships for conditional triggering of alternate *use cases*
  - They may be decomposed by activity diagrams

HAZARD SIGNALS

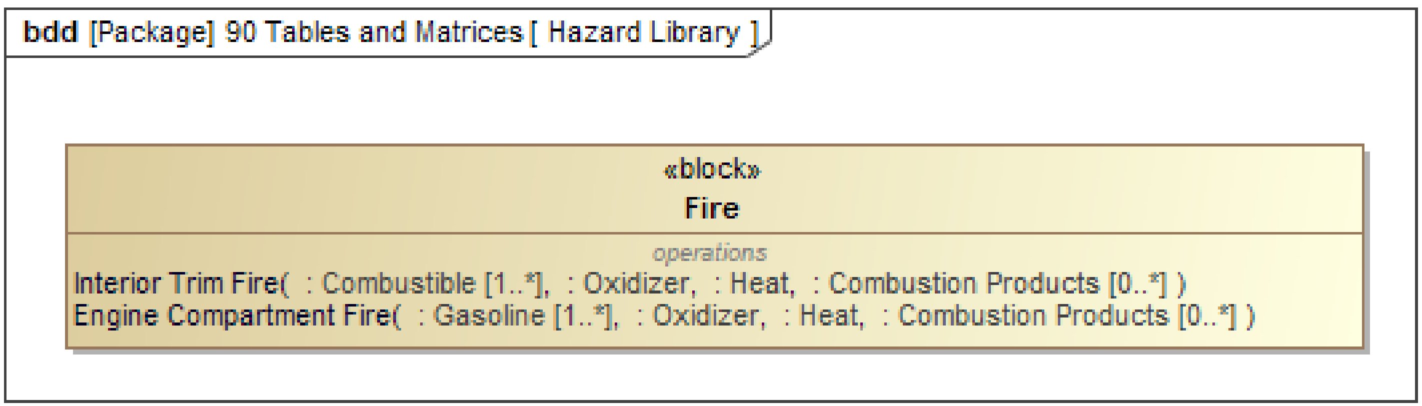


SIGNAL USAGE

- <<signals>> are used to type flow properties on interfaces, content conveyed on flows, and input/output parameters
- This hierarchy allows more specific signals to be used to satisfy more general input/output parameters

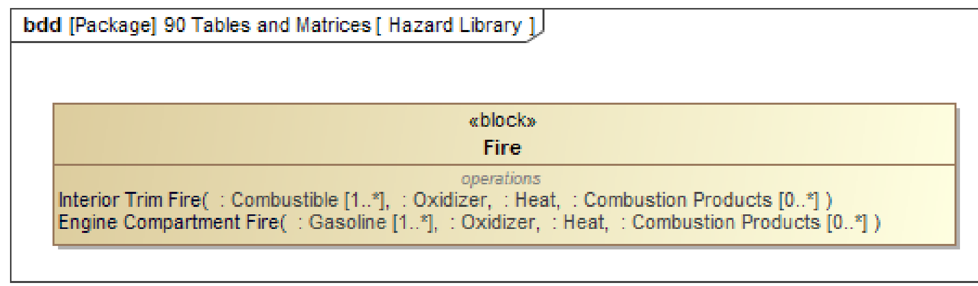


HAZARD BLOCK



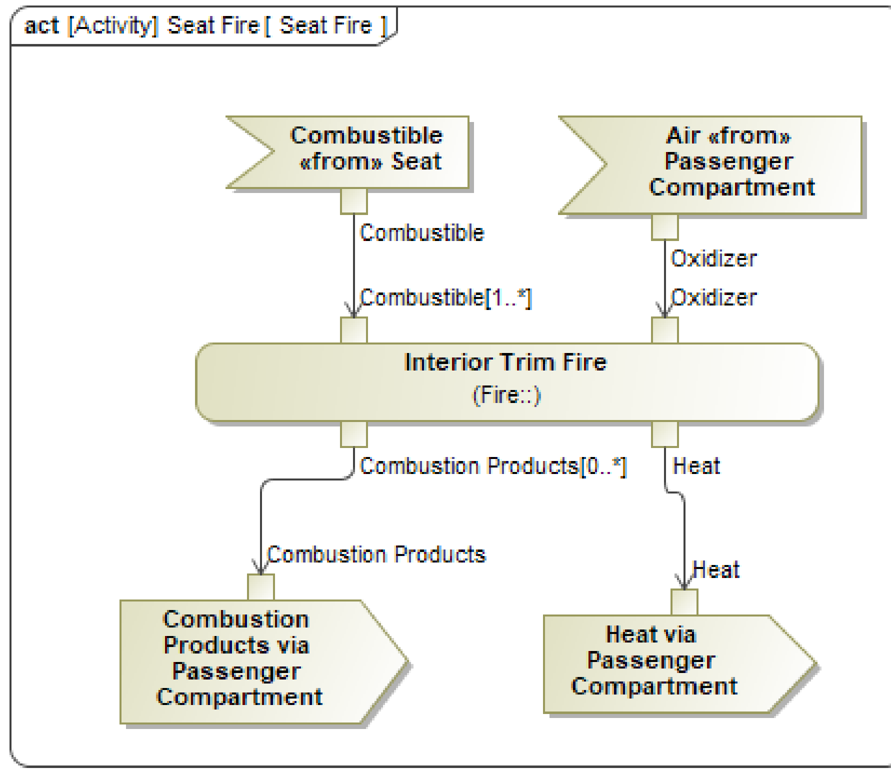
HAZARDS AS OPERATIONS

- <<operations>> own input/output *parameters*
- In this case, an Interior Trim Fire requires at least one combustible, an oxidizer, and generated heat and may generate combustion products (smoke, toxic gas, etc.)



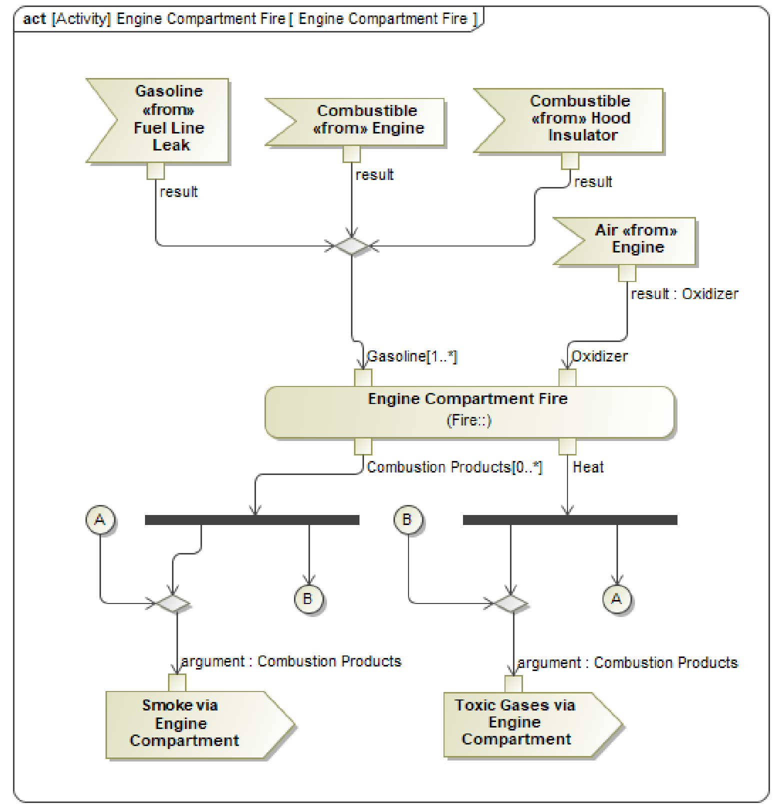
MISHAP DECOMPOSITION

- This activity diagram shows the operation an its input/output *parameters*.
- Each *pin* must be connected (no unconnected pins).
- This forces the analyst to identify the source and destination of all inputs and outputs.
- *Flow final* nodes may be used if there is no output of interest.



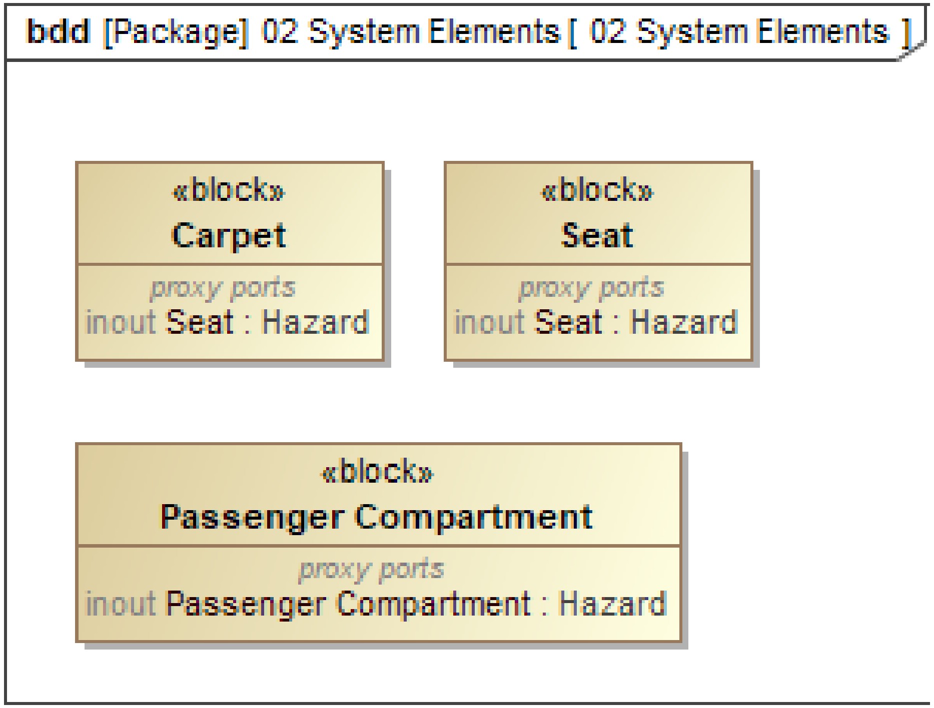
ENGINE COMPARTMENT FIRE

- Note the more complex logic and multiple sources for inputs.



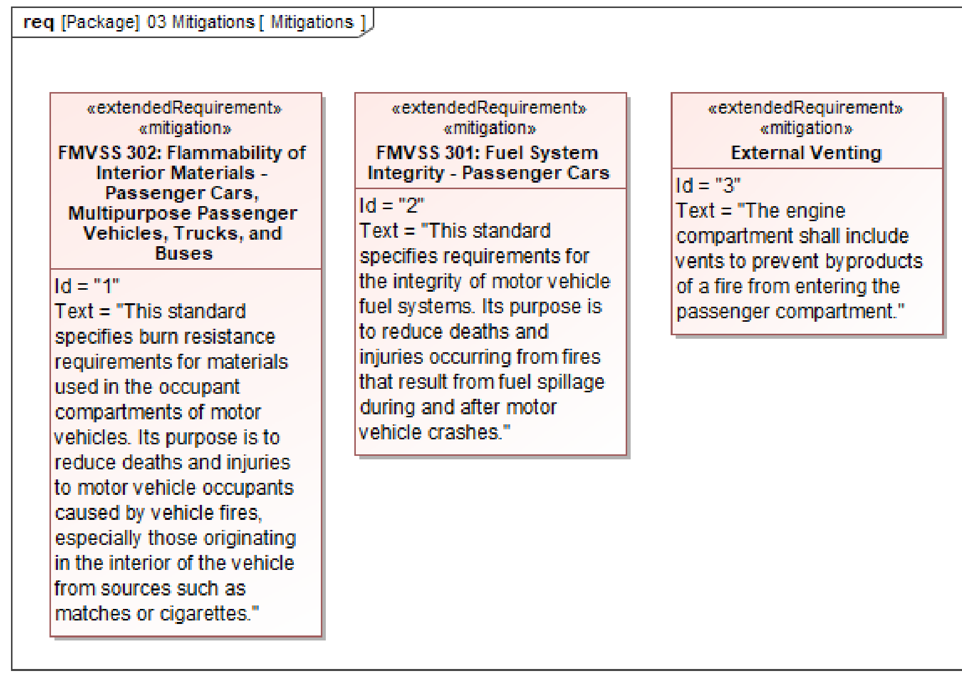
HAZARD PORTS

- The *send signal* and *accept event* elements may be assigned to *ports*.
- This allows the modeler to specify the source or destination of the flow.
- *Hazard ports* (which can legally flow hazard signals) are added to each system element to facilitate this.
- These ports would be hidden/excluded from normal architectural analysis.



MITIGATIONS

- Mitigations are requirements that have a <<mitigation>> *stereotype* applied.
- They may have body text and hyperlinks to the standard, design guidelines, or other relevant material.



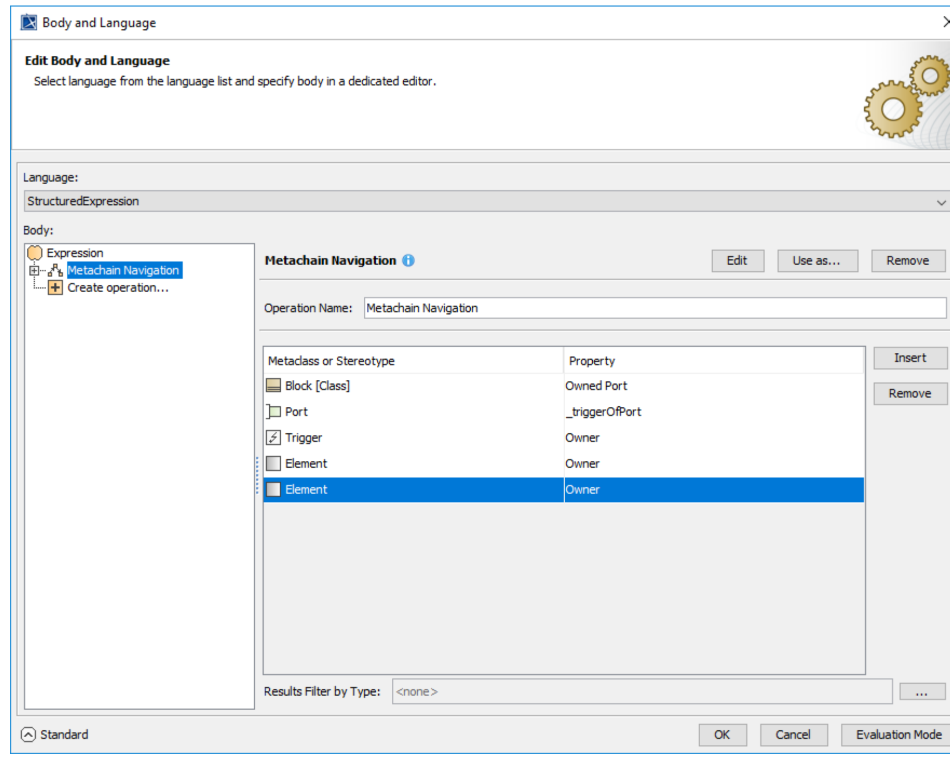
MISHAPS

#	Name	Documentation	Severity	Probability	Causal Factor	Related Hazard
1	Engine Compartment Fire	This mishap describes the outcome of a fire starting in the engine compartment due to a fuel leak.	I Catastrophic	C Occasional	Fire starts in engine compartment due to fuel leak	Vehicle Fire
2	Interior Carpet Fire	This mishap describes the outcome of an interior carpet fire.	I Catastrophic	A Frequent	Interior carpet ignites	Vehicle Fire
3	Seat Fire	This mishap describes the outcome of vehicle seats igniting.	II Critical	E Improbable	Seats ignite	Vehicle Fire

Note: All of these columns populate due to properties or querying the mishap analysis

METACHAIN NAVIGATION

- Metachain navigation uses structured expressions to navigate elements, relationships, and properties.
- It can also perform set-based operations (intersection, exclude, etc.), property tests, and mathematical operations.
- Metrics can also be developed (e.g., number of unconnected pins)



NOTIONAL METACHAIN: SYSTEM ELEMENT TO HAZARDS TO WHICH IT CONTRIBUTES

Metaclass or Stereotype	Property
Block [Class]	Owned Port
Port	_triggerOfPort
Trigger	Owner
Element	Owner
Element	Owner

SYSTEM ELEMENTS

#	Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations	Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability					
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting					
3	Engine Compartment					Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire									
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline						
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible						
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability	Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability				1 FMVSS 302: Flammability	

CONTRIBUTIONS AND MITIGATIONS

#	△ Name	Contributes to Mishaps	Mishap Severity	Contributes	Potential Contribution Mitigations
1	Carpet	Interior Carpet Fire	I Catastrophic	Combustible	1 FMVSS 302: Flammability
2	Engine	Engine Compartment Fire	I Catastrophic	Combustible Air	2 FMVSS 301: Fuel System 3 External Venting
3	Engine Compartment				
4	Fire				
5	Fuel Line	Engine Compartment Fire	I Catastrophic	Gasoline	
6	Hood Insulator	Engine Compartment Fire	I Catastrophic	Combustible	
7	Passenger Compartment	Interior Carpet Fire Seat Fire	I Catastrophic II Critical	Air	1 FMVSS 302: Flammability
8	Seat	Seat Fire	II Critical	Combustible	1 FMVSS 302: Flammability

RECEPTIONS, MITIGATIONS, AND ERRORS

Recipient of Hazard	Receives	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
Engine Compartment Fire	Toxic Gases Smoke	2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
Seat Fire Interior Carpet Fire	Combustion Products Heat Toxic Gases Smoke			
			1 FMVSS 302: Flammability	

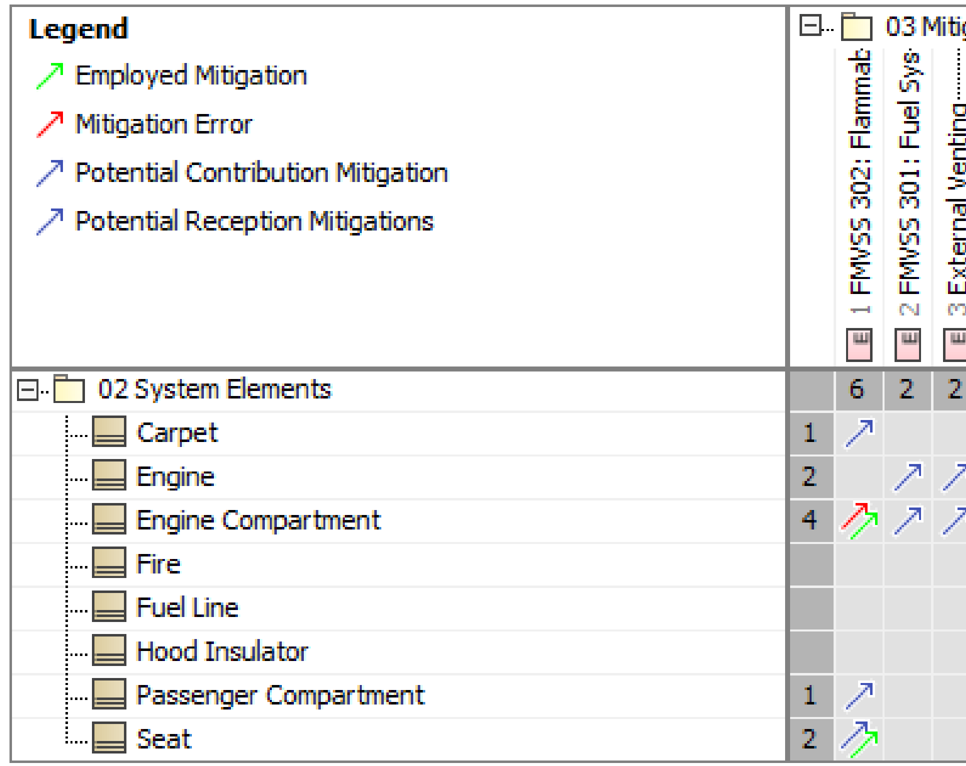
MITIGATION ERRORS

#	△ Name	Potential Contribution Mitigations	Potential Reception Mitigations	Employed Mitigation	Mitigation Error
1	Carpet	1 FMVSS 302: Flammability			
2	Engine	2 FMVSS 301: Fuel System 3 External Venting			
3	Engine Compartment		2 FMVSS 301: Fuel System 3 External Venting	1 FMVSS 302: Flammability	1 FMVSS 302: Flammability
4	Fire				
5	Fuel Line				
6	Hood Insulator				
7	Passenger Compartment	1 FMVSS 302: Flammability			
8	Seat	1 FMVSS 302: Flammability		1 FMVSS 302: Flammability	

FMVSS 302 is neither a potential contribution nor a reception mitigation, so its employment is an error.

MITIGATION RELATIONSHIPS

- Relationships may also be displayed in a matrix using direct connections or custom metachains.
- Any relationship in a table may be shown in a matrix (and icons may be used in place of arrows).



ERROR CHECKING

#	Name	Owner	Type	△ Incoming	Outgoing
1		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
2		Combustible	Combustible		Object Flow[Combustible -> Combustible[1..*]]
3		Engine Compartment Fire	Combustion Products		Object Flow[Combustion Products[0..*] ->]
4		Interior Trim Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb
5		Interior Carpet Fire	Combustion Products		Object Flow[Combustion Products[0..*] -> Comb Object Flow[Combustion Products[0..*] -> Comb
6		Interior Carpet Fire	Heat		Object Flow[Heat -> Heat]
7		Interior Trim Fire	Heat		Object Flow[Heat -> Heat]
8		Engine Compartment Fire	Heat		Object Flow[Heat ->]
9		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
10		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
11		Combustible			Object Flow[->]
12		Combustible			Object Flow[->]
13		Gasoline	Gasoline		Object Flow[Gasoline ->]
14		Air	Oxidizer		Object Flow[Oxidizer -> Oxidizer]
15		Smoke	Combustion Products	Object Flow[-> Combustion Products]	
16		Toxic Gases	Combustion Products	Object Flow[-> Combustion Products]	
17		Engine Compartment Fire	Gasoline	Object Flow[-> Gasoline[1..*]]	
18		Interior Carpet Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
19		Interior Trim Fire	Combustible	Object Flow[Combustible -> Combustible[1..*]]	
20		Toxic Gases	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
21		Combustion Products	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
22		Smoke	Combustion Products	Object Flow[Combustion Products[0..*] -> Combustion Proc	
23		Heat	Heat	Object Flow[Heat -> Heat]	
24		Heat	Heat	Object Flow[Heat -> Heat]	
25		Interior Carpet Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
26		Engine Compartment Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	
27		Interior Trim Fire	Oxidizer	Object Flow[Oxidizer -> Oxidizer]	

CONCLUSIONS

- The use of a relatively small number of customizations can be used to enable the integration of ESOH analysis into the system model used in support of systems architecture and engineering.
- The error-checking and customized queries made possible by this approach allow maximum insight to be achieved with little incremental effort.
- Reuse, the elimination of adjacent tools and systems, and the reduction in lag between analysis and stakeholder visibility are all possible with this approach.