Modeling Safety and CyberSecurity Controls in SysML

Michael J. Vinarcik, ESEP-Acq, OCSMP-Model Builder—Advanced
Brian Pepper, OCSMP-Model User
Booz Allen Hamilton

National Defense Industrial Association
19th Annual Systems Engineering Conference
October 24-27, 2016

Booz | Allen | Hamilton

Contact information

Michael J. Vinarcik

248-227-1659

Booz Allen Hamilton

vinarcik_michael@bah.com

Managing Details

"The devil is in the details, but so is salvation."

-- ADM Hyman G. Rickover
(photo from U.S. Naval Historical Center)

- A good system modeling effort manages the details that improve the odds of program success.
- This presentation will focus on modeling safety and cyber-security content.

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.
- Modeling starts with user needs, develops system behaviors and functions, and ultimately describes the physical elements that provide the functions (with linkages to requirements and test cases).
- Failure Mode Effects Analyses (FMEAs), cybersecurity controls, and Functional Hazard Analyses (FHAs) may be easily integrated into a system model (providing deeper insight into the system).

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

Why SysML?

- Other system modeling languages exist, but SysML is the most widely-adopted and has a thriving tool ecosystem.
- A well-constructed system model unambiguously represents a system's behavior, structure, and interrelationships between elements.
- It also fosters a "crispness" in the formulation of issues (according to David Miller, NASA Chief Technologist).
- In addition, current SysML tools allow the model content to be expressed as tables, matrices, and other derivative work products.
- These derived work products enable the system to "talk to us," exposing patterns and content not easily gleaned from the review of traditional document-based artifacts.

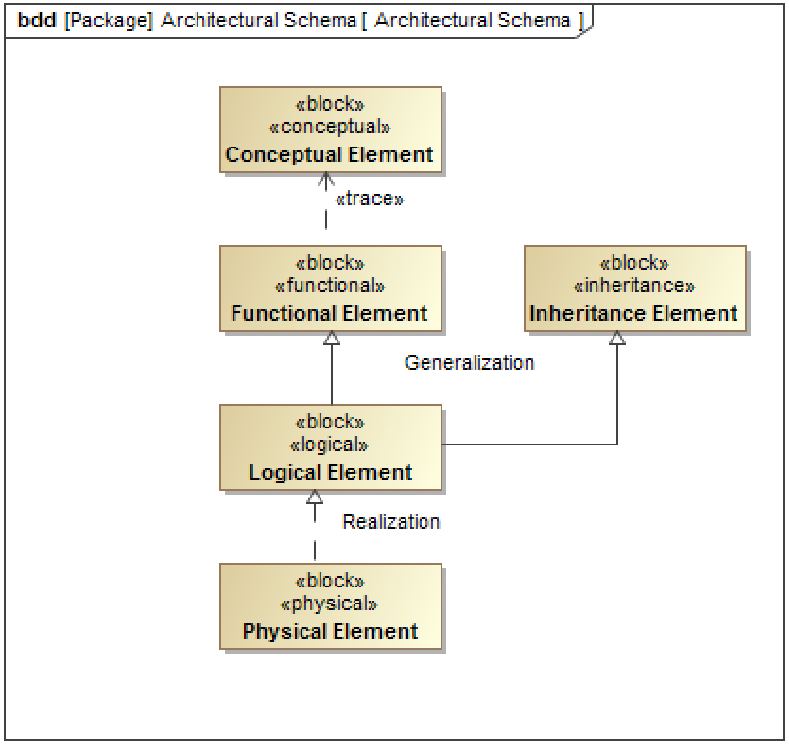
An Example: Unmanned Aircraft Systems

- An unclassified, non-DoD example was needed for this presentation.
- In 2007, NASA released NASA/TM-2007-214539: Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems
  - 71 pages
  - Included NASA, Boeing, Certification Services, and AvioniCon staff
- This presentation is not intended as a criticism of their work but will highlight errors and inconsistencies exposed by translating it into a SysML model.
- These deficiencies illustrate the inherent limitations of a non-model based approach.

Imported Content

- The following content was imported directly from the report (some Excel reformatting and reorganization was necessary):
  - Glossary of terms
  - Functional decomposition
  - Operational consequences
- MagicDraw 18.4 with the SysML plugin was used to demonstrate what is possible with “stock” SysML. Other alternatives considered were:
  - UPDM
  - Cameo Safety and Reliability Analyzer (built on Medical devices – Application of risk management to medical devices (ISO 14971:2007, Corrected version 2007-10-01))
    - Allows fault tree and FMEA analysis
    - Rejected due to presenter’s lack of familiarity with this newly-released plugin

Architectural Schema

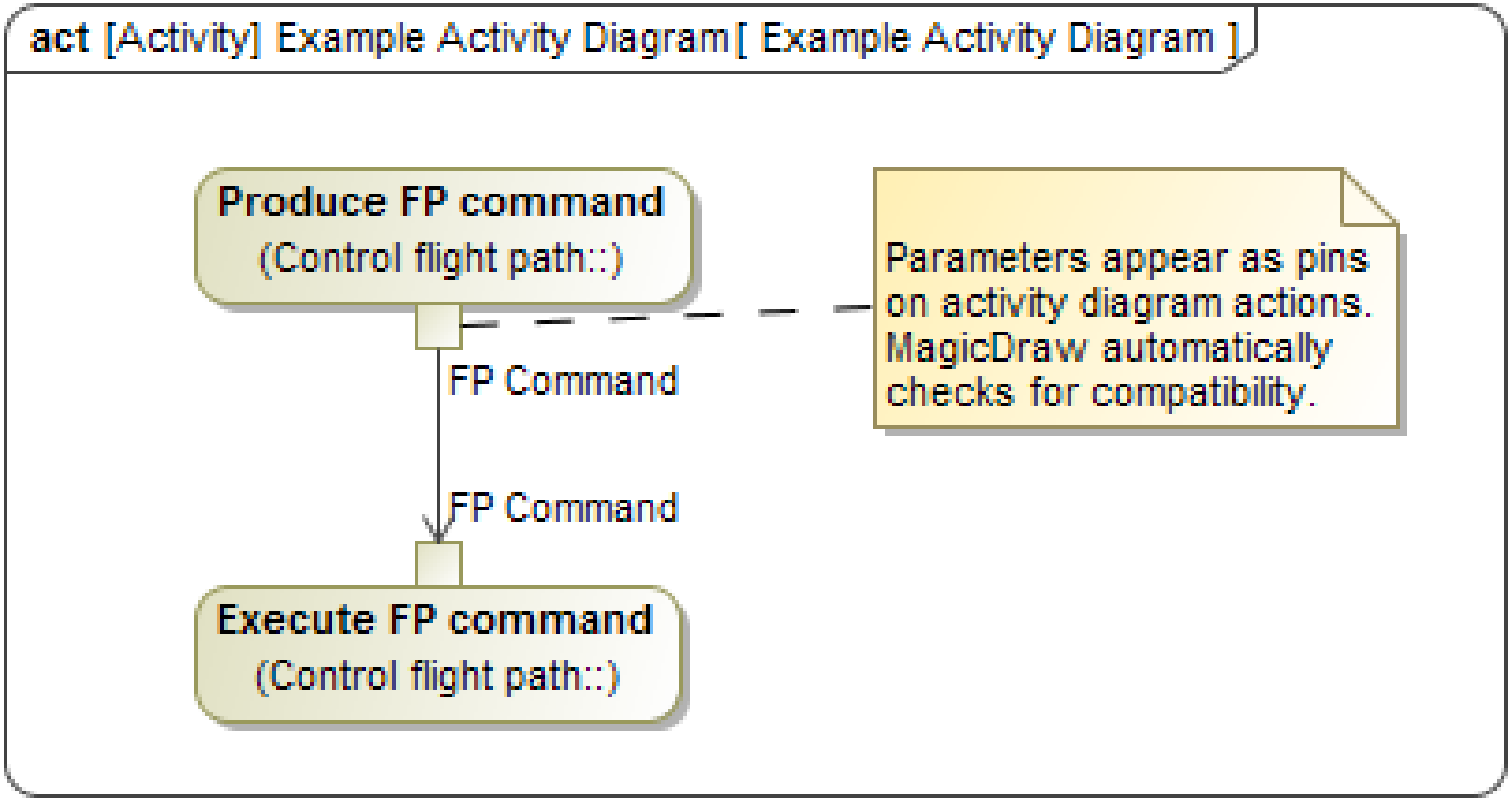


- Functional elements are traced to conceptual elements
- Functional elements generalize logical elements
- Physical elements realize logical elements

Functions As Operations

- *Operations* are used to represent functions:
  - *Operations* own *parameters* typed by *signals* to capture inputs, outputs, and results
- *Operations* are owned by *functional blocks* and are called by *call operation* actions on activity diagrams
- For the purposes of this analysis, no detailed activity diagrams were generated. Functions from the analysis were imported and owned by functional blocks.
- *Signals* were manually created based upon the functions (for example, FP Command because there were functions that generated and executed FP commands).
- *Parameters* were added to *operations* and were typed by *signals* (as appropriate)

Example activity diagram



Examples of functions

#	Name	Owner	Owned Parameter
1	Aviate	UAS	
2	Avoid adverse environmental conditions	Mitigate	
3	Avoid air traffic	Avoid collisions	
4	Avoid collisions	Mitigate	
5	Avoid ground and vertical structures [while airborne]	Avoid collisions	
6	Avoid ground path obstructions [while landing or on gro	Avoid collisions	
7	Broadcast communications	Broadcast info to ATC and other aircraft	out : Signals::Communicat
8	Broadcast info to ATC and other aircraft	Communicate	
9	Broadcast transponder data	Broadcast info to ATC and other aircraft	
10	Command and control between control station and UAS	Aviate	
11	Communicate	UAS	
12	Control air/ground transition	Aviate	
13	Control center of gravity	Control UAS subsystems	
14	Control environment inside the UAS	Control UAS subsystems	
15	Control fire supression subsystem	Control UAS subsystems	
16	Control flight path	Aviate	
17	Control ground path	Aviate	
18	Control power subsystems [hydraulic/electrical]	Control UAS subsystems	
19	Control UAS subsystems	Aviate	
20	Convey AGT command status	Control air/ground transition	out : Signals::AGT Comma
21	Convey AGT state	Control air/ground transition	out : Signals::AGT State
22	Convey FP command status	Control flight path	out : Signals::FP Comman
23	Convey FP State	Control flight path	inout : Signals::FP State
24	Convey GP command status	Control ground path	out : Signals::GP Comman
25	Convey GP state	Control ground path	out : Signals::GP State

Identification of duplicates

27	Convey post corrective action status to ATC	Avoid ground and vertical structures [while air…	
28	Convey post corrective action status to ATC	Avoid adverse environmental conditions	
29	Convey post corrective action status to ATC	Avoid air traffic	
30	Convey post corrective action status to ATC	Avoid ground path obstructions [while landing …	
31	Convey relative location of adverse environmental conc	Avoid adverse environmental conditions	
32	Convey status of command	Manage contingencies	out : Signals::Command S
33	Convey system status	Manage contingencies	out : Signals::System Stat
34	Detect adverse environmental conditions	Avoid adverse environmental conditions	
35	Detect air traffic	Avoid air traffic	
36	Detect ground and vertical structures	Avoid ground and vertical structures [while air…	
37	Detect ground path obstructions	Avoid ground path obstructions [while landing …	
38	Determine AGT intent	Control air/ground transition	

Signals

#	Name
1	AGT Command
2	AGT Command Status
3	AGT State
4	Command
5	Command Status
6	Communications
7	Contingency Command
8	Corrective Action Command
9	Corrective Action Command Status
10	FP Command
11	FP Command Status
12	FP State
13	GP Command
14	GP Command Status
15	GP State
16	Information
17	Mitigation Command
18	Navigation Command
19	State
20	Transponder Data
21	UAS State
22	Guidance Command
23	Navigation Command Status
24	Navigation state
25	System Status

Operational consequences as use cases

- *Operational consequences* were imported as *use cases* with an <<operational consequence>> stereotype applied:
  - Included *hazard classification* and *remarks* tags
- Hazard classifications were:
  - Catastrophic
  - Hazardous
  - Major
  - Minor
  - No effect
  - TBD

Operational consequences

#	Name	Documentation	Hazard Classification	Remarks
1	Catastrophic		catastrophic	
2	All communication being sent is not received by intended receiver.	All communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice tr
3	All Communication being sent is not received by intended receiver.	All Communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	major	Assumption is that Communicate refers only to voice tr
4	ATC will be expecting a status update, and will consult radar displays and continue to attemp	ATC will be expecting a status update, and will consult radar displays and continue to attempt to reach UAS pilot/operator for outcome.	minor	Assumes ATC can deduce situation based on radar disp
5	C2 system status is not available, therefore if C2 is lost also, then the vehicle cannot be con	C2 system status is not available, therefore if C2 is lost also, then the vehicle cannot be controlled and no action (human or automation) can compensate.	catastrophic	A transient loss of C2 is considered a normal part of flig
6	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance e	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	
7	Flight crew/UAS does not know FP state.	Flight crew/UAS does not know FP state. The flight crew may or may not recognize that the vehicle is not performing correctly: flight termination may or may not be initiated.	hazardous	A similar failure in the AC 23.1309 example is classified
8	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal.	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal. Expect there is a time buffer between initiation and hazardous situation. Loss of safety margin results.	minor	Situations where this failure has more dire consequenc
9	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal.	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal. Expect there is a time buffer between initiation and hazardous situation. More than a significant loss of safety margin results.	hazardous	
10	Flight crew/UAS initiates contingency which takes significantly longer than normal.	Flight crew/UAS initiates contingency which takes significantly longer than normal. Expect there is a time buffer between initiation and the dangerous situation. Loss of safety margin results.	major	
11	Flight crew/UAS is trying to control FP state, but this is ineffective.	Flight crew/UAS is trying to control FP state, but this is ineffective. By function 1.1.5, the UAS/flight crew will recognize that guidance commands are ineffective then use other means to control FP state.	major	
12	Flight crew/UAS is unaware that flight termination system has been deployed.	Flight crew/UAS is unaware that flight termination system has been deployed. Flight crew/UAS will not immediately alert ATC of situation. However, fairly soon because of the behavior of the vehicle will be known to the flight crew and ATC.	major	
13	Flight crew/UAS not able to change FP state.	Flight crew/UAS not able to change FP state. Vehicle is uncontrollable.	hazardous	Execution of a soft landing function assumes that peop

Operational consequence example

#	Name	Documentation	Hazard Classification	Remarks
1	All communication being sent is not received by intended recei	All communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice tr
2	All Communication being sent is not received by intended rece	All Communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	major	Assumption is that Communicate refers only to voice tr
3	ATC will be expecting a status update, and will consult radar d	ATC will be expecting a status update, and will consult radar displays and continue to attempt to reach UAS pilot/operator for outcome.	minor	Assumes ATC can deduce situation based on radar disp

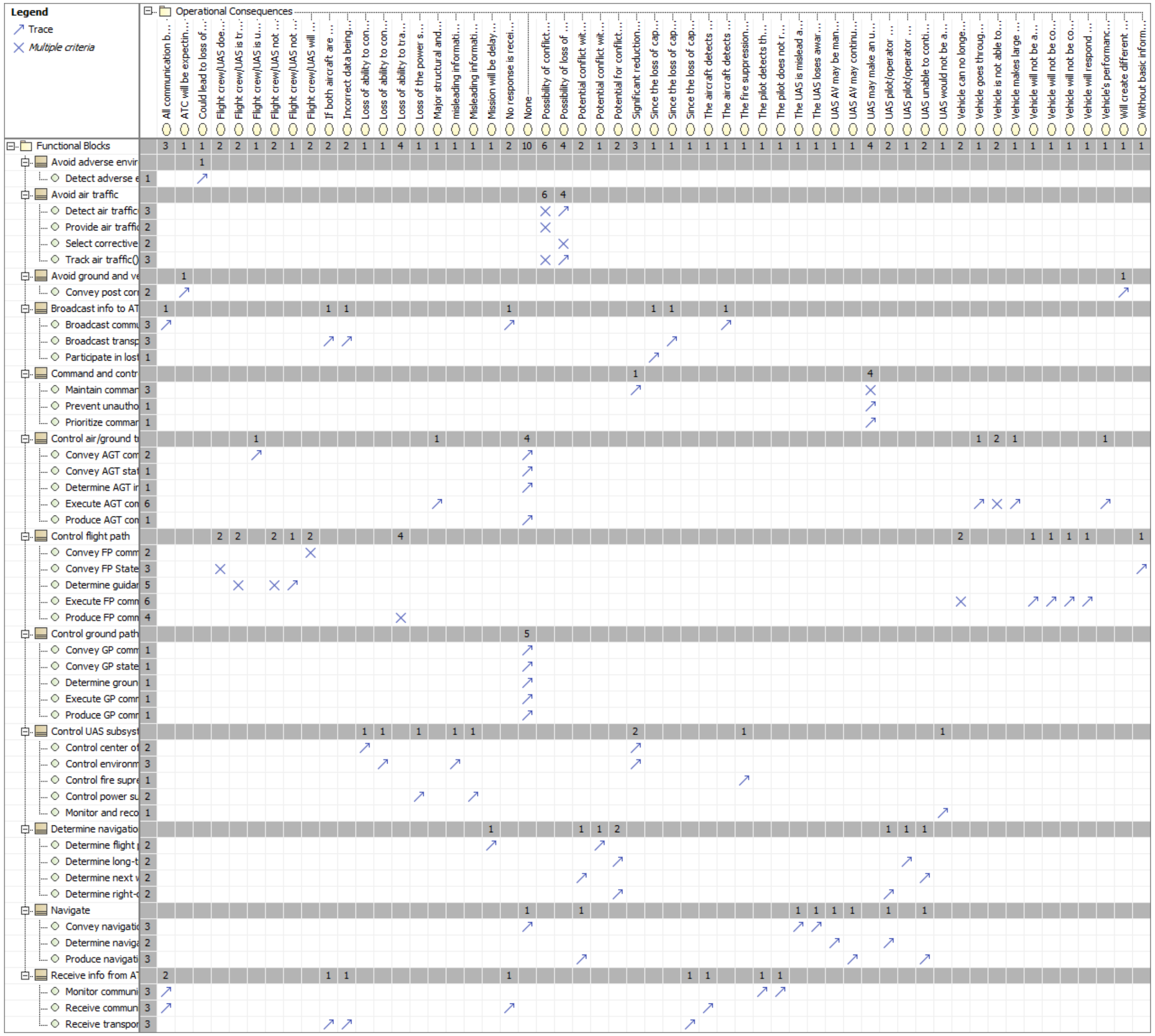
Tracing functions to operational consequences

- The <<trace>> relationship was used to connect functions to operational consequences.
- Each relationship was named with the failure condition identified in the report.

Trace table

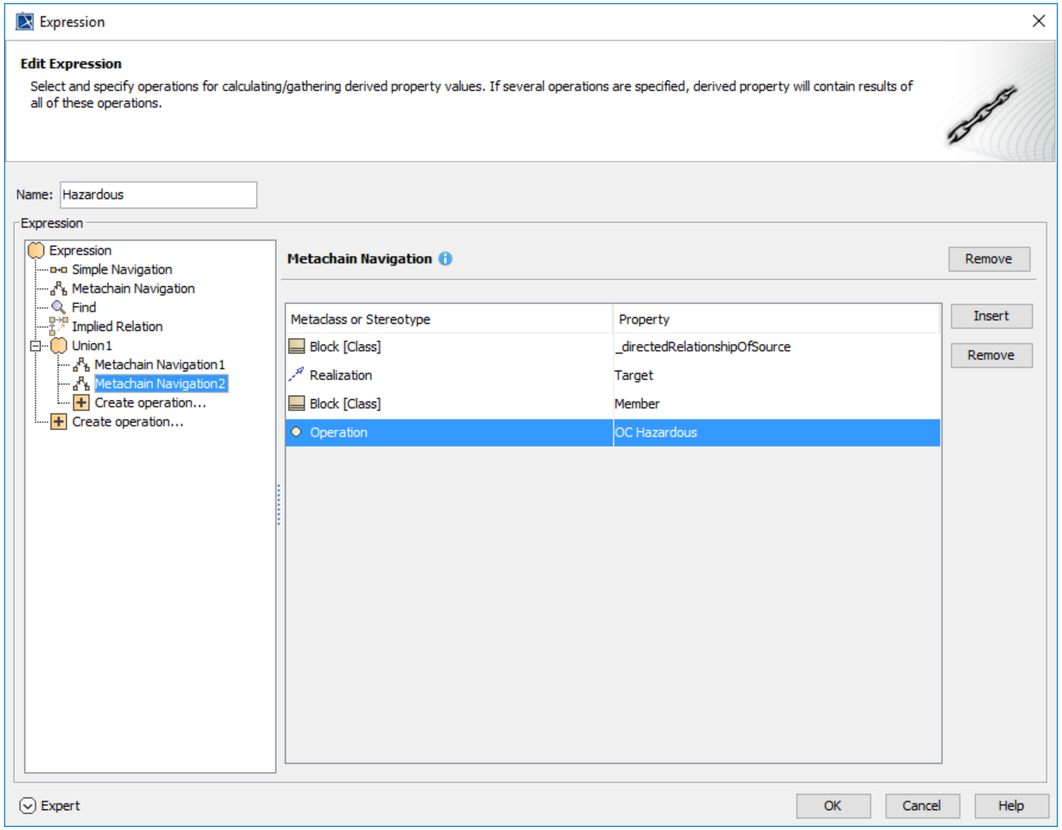
#	Name	Client	Supplier
1		Determine right-of-way rules()	Potential for conflict with other traffic.
2		Convey navigation state(: Navigation state)	None
3	Air traffic not on a collision course is incorrectly tracked as a	Track air traffic()	Possibility of loss of control and/or conflict with another (real) air...
4	Air traffic on a collision course is incorrectly tracked as a non	Track air traffic()	Possibility of conflict with another aircraft.
5	All failure conditions	Control fire supression subsystem()	The fire suppression system is a back-up system that is only requ...
6	All failure conditions	Monitor and record UAS state data(: State [0..*])	UAS would not be able to reproduce state data in case of inciden...
7	Any malfunction	Convey GP state(: GP State)	None
8	Any malfunction	Execute GP command(: GP Command)	None
9	Any malfunction	Convey AGT state(: AGT State)	None
10	Any malfunction	Determine AGT intent()	None
11	Any malfunction	Produce AGT command(: AGT Command)	None
12	Any malfunction	Convey GP command status(: GP Command Status)	None
13	Any malfunction	Determine ground intent()	None
14	Any malfunction	Produce GP command(: GP Command)	None
15	Any malfunction other than loss of status of flight terminatio	Convey AGT command status(: AGT Command Status)	None
16	Corrective action status information is misleading.	Convey post corrective action status to ATC()	Will create different situational perceptions between pilot/operat...
17	Degraded C2 data link function resulting in incorrect signal	Maintain command and control during all phases of flight()	UAS may make an unpredictable maneuver resulting in uncontroll...
18	Degraded communications function	Broadcast communications(: Communications)	All communication being sent is not received by intended receiver.
19	Degraded communications function detected	Receive communications(: Communications)	All communication being sent is not received by intended receiver.
20	Degraded control	Control environment inside the UAS()	Significant reduction in safety margin and increase in pilot worklo...
21	Degraded control of center of gravity	Control center of gravity()	Significant reduction in safety margin and increase in pilot worklo...
22	Degraded function detected	Monitor communications from ATC and other aircraft(: Communi...	All communication being sent is not received by intended receiver.

Trace Matrix



Derived properties

- MagicDraw allows the creation of derived properties and custom columns in tables.
- One of the most powerful features is *metachain navigation*, which allows relationships to be “hopped” from one element to another.

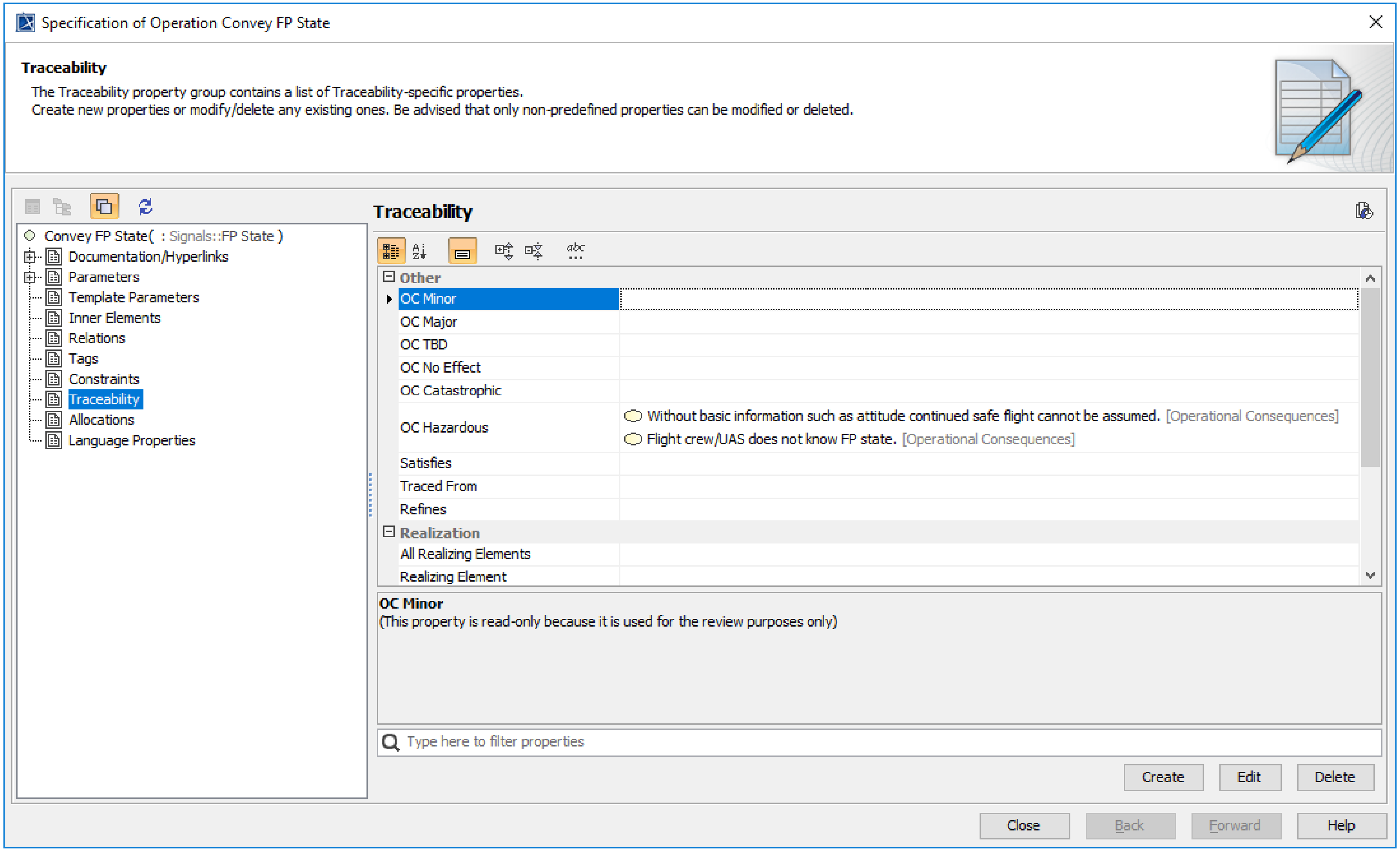


Booz | Allen | Hamilton

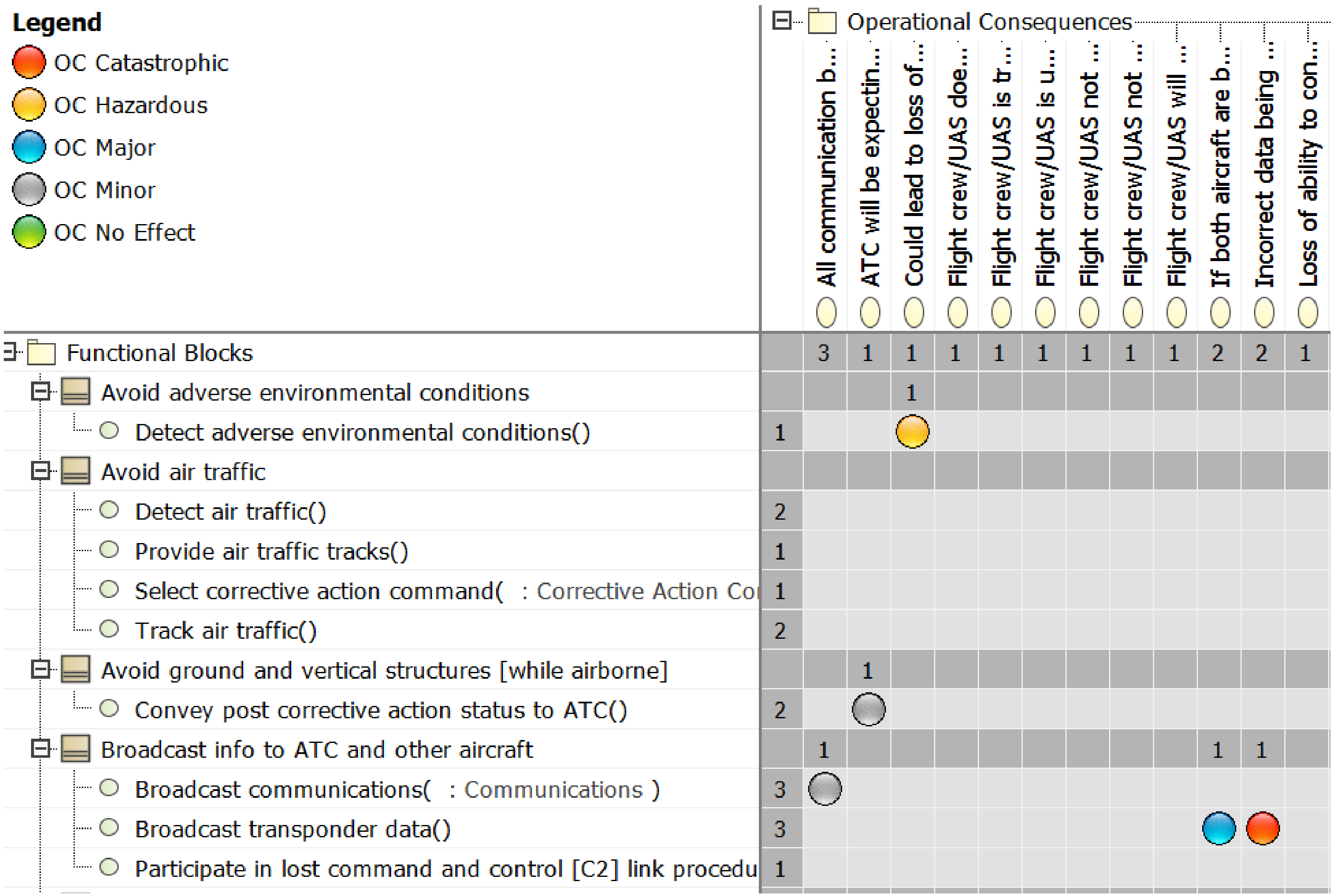
Example of functional block to operational consequence table

#	Name	Catastrophic	Hazardous
1	Aviate		
2	Avoid adverse environmental conditions		Could lead to loss of contr
3	Avoid air traffic		
4	Avoid collisions		
5	Avoid ground and vertical structures [while airborne]		
6	Avoid ground path obstructions [while landing or on ground]		
7	Broadcast info to ATC and other aircraft	Incorrect data being sent to other air	
8	Command and control between control station and UAS	UAS may make an unpredictable mane	
9	Communicate		
10	Control air/ground transition	Major structural and propulsion syster	
11	Control flight path	Vehicle will not be controllable.	Without basic information Flight crew/UAS does not Flight crew/UAS not able t Loss of ability to translate Vehicle will respond slowly. Vehicle can no longer main Vehicle will not be controlla
12	Control ground path		

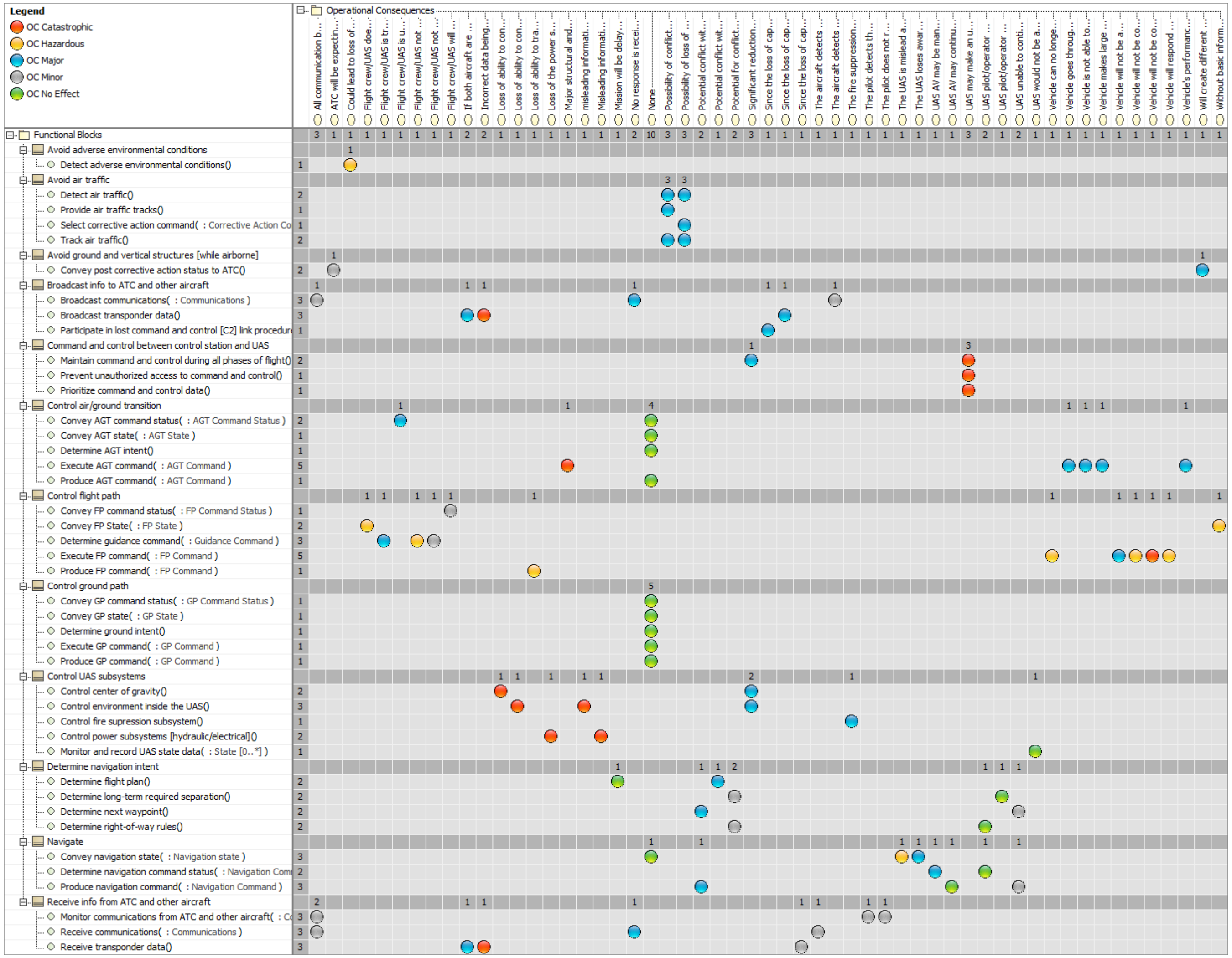
Traceability view



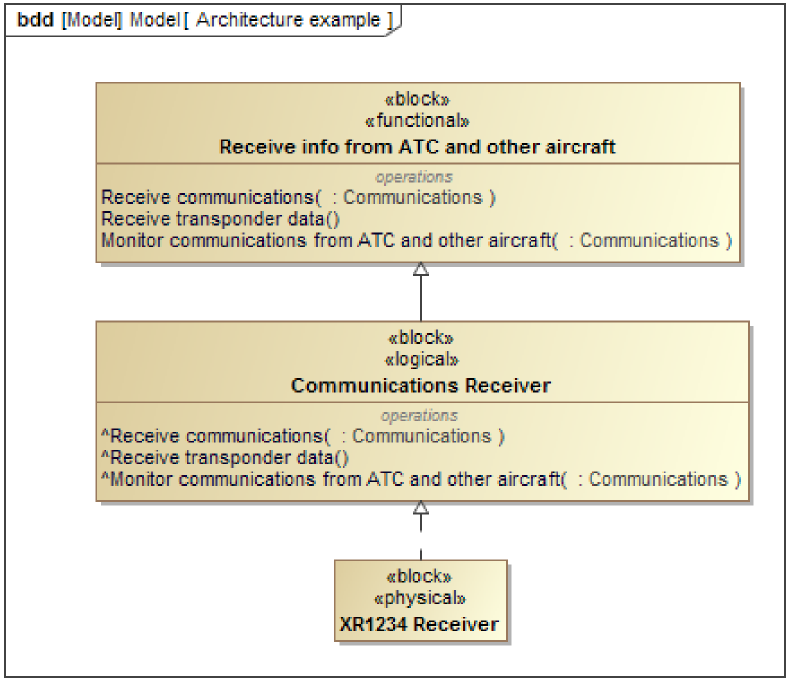
Hazard matrix



Complete hazard matrix



Architecture example



- Example logical and physical elements were created.
- Each inherited traceability to the operational consequences simply by creating the appropriate relationships with the other architectural elements

Logical blocks

#	Name	Catastrophic	Hazardous	Major	Minor	No Effect	TBD
1	Communications Receiver	Incorrect data being sent to other air		No response is received wl If both aircraft are being t	All communication being se The aircraft detects the lo: Since the loss of capability The pilot detects the loss c The pilot does not receive		

Physical blocks

#	Name	Catastrophic	Hazardous	Major	Minor	No Effect	TBD
1	XR1234 Receiver	Incorrect data being sent to other air		No response is received wl If both aircraft are being t	All communication being se The aircraft detects the lo: Since the loss of capability The pilot detects the loss c The pilot does not receive		

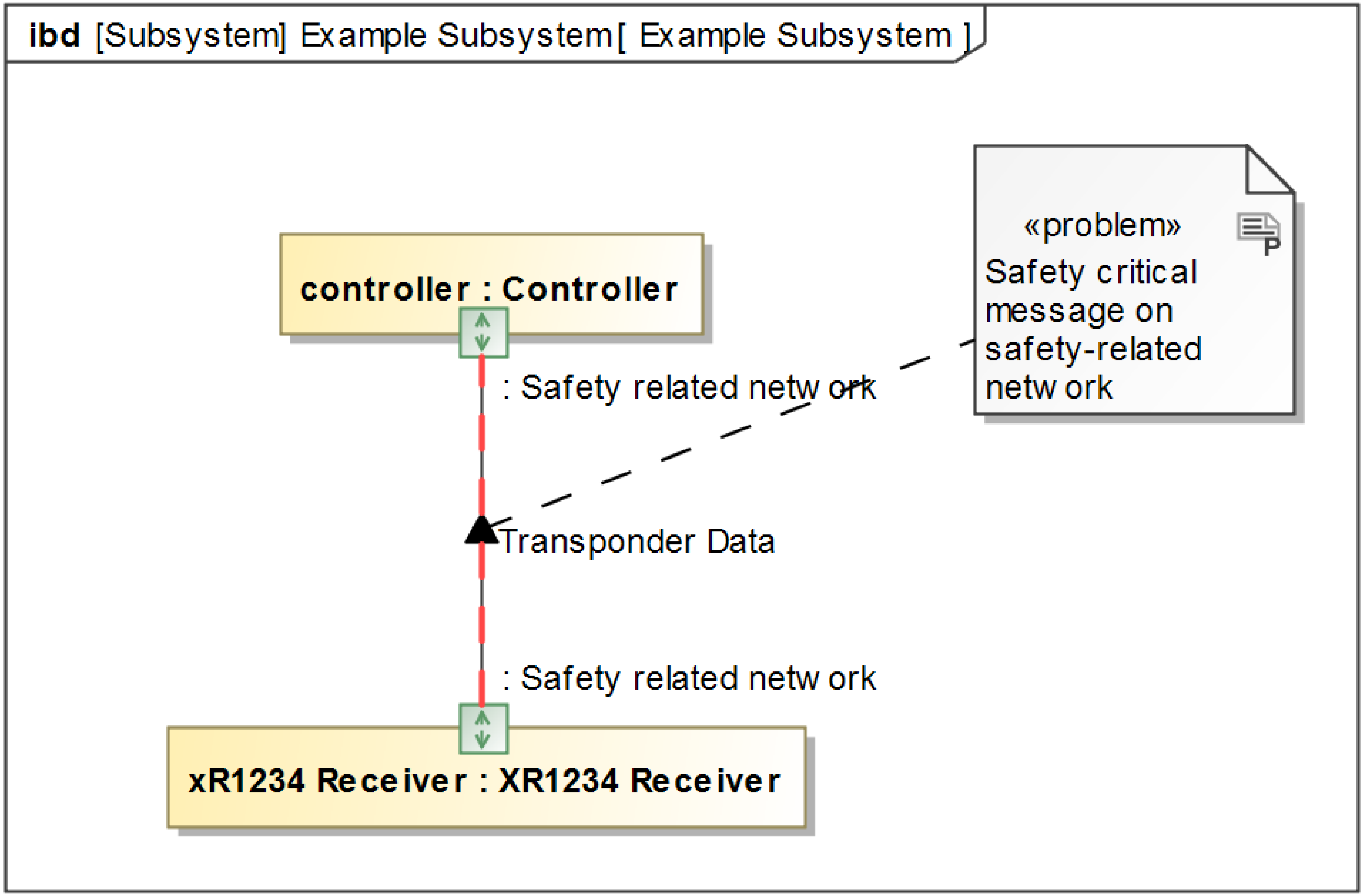
Classifying signals

- One of the most powerful truths about a system model is that it can expose information and improve consistency.
- Tracing *parameters* to *operations* and then to the *operational consequences* and their rating allows the safety criticality to be objectively assessed.
- The rules applied for this analysis were:
  - Catastrophic / hazardous = safety critical
  - Major = safety significant
  - Minor = safety related
  - No effect = not safety related
  - TBD = TBD

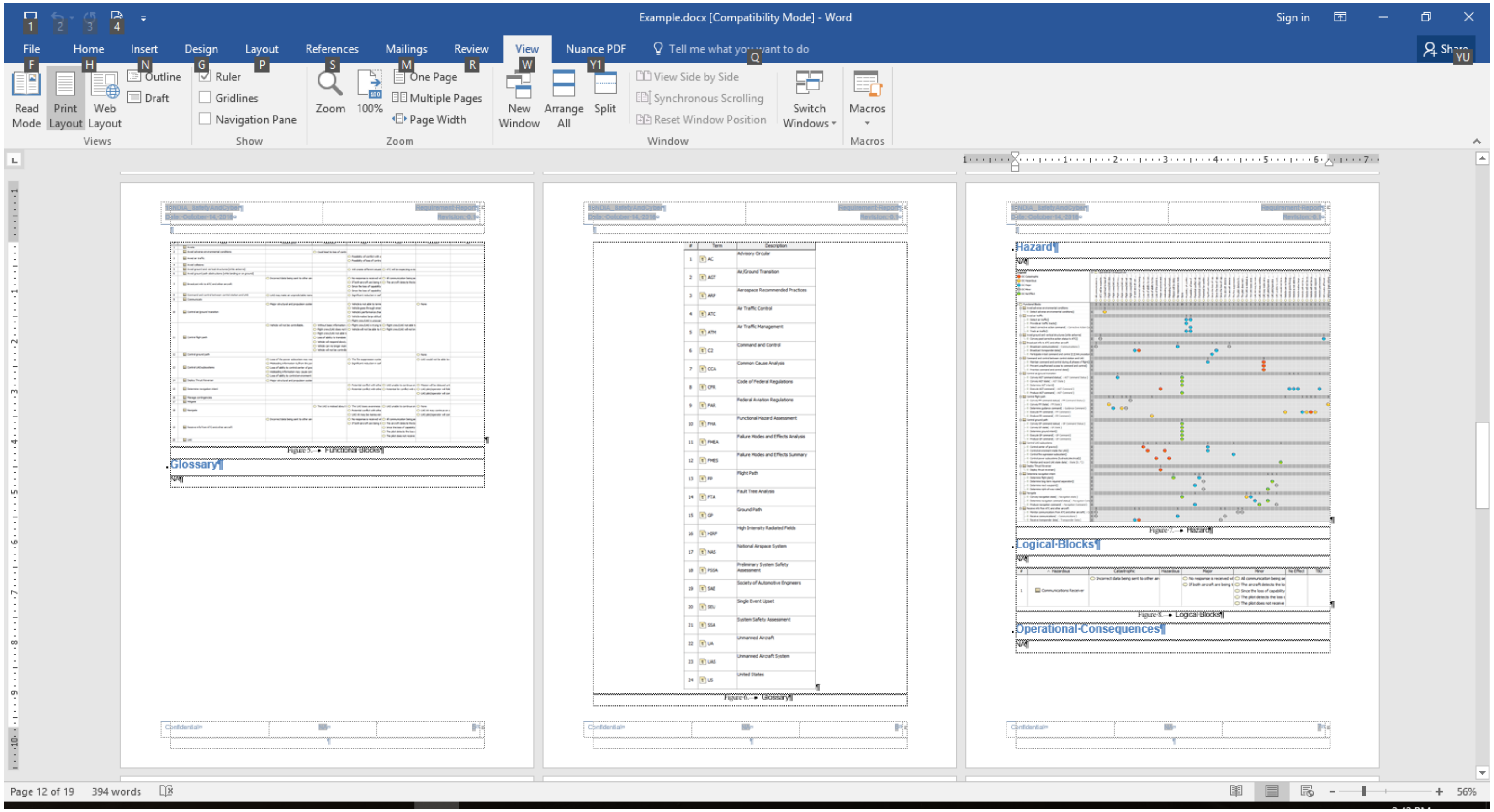
Signal classification

#	Type	Owner	OC Severity Rollup	Signal Classification
1	AGT Command	Execute AGT command(: AGT Command)	catastrophic major	safety critical
2	AGT Command	Produce AGT command(: AGT Command)	no effect	safety critical
3	AGT Command Status	Convey AGT command status(: AGT Command Status)	major no effect	safety significant
4	AGT State	Convey AGT state(: AGT State)	no effect	not safety related
5	Command Status	Convey status of command(: Command Status)		TBD
6	Communications	Monitor communications from ATC and other aircraft(: Communications)	minor	safety significant
7	Communications	Receive communications(: Communications)	major minor	safety significant
8	Communications	Broadcast communications(: Communications)	major minor	safety significant
9	Contingency Command	Determine contingency command(: Contingency Command)		TBD
10	Corrective Action Command	Execute corrective action command(: Corrective Action Command)		safety significant
11	Corrective Action Command	Execute corrective action command(: Corrective Action Command)		safety significant
12	Corrective Action Command	Execute corrective action command(: Corrective Action Command)		safety significant
13	Corrective Action Command	Execute corrective action command(: Corrective Action Command)		safety significant
14	Corrective Action Command	Select corrective action command(: Corrective Action Command [0..*], : C...	major	safety significant
15	Corrective Action Command	Determine corrective action(: Corrective Action Command)		safety significant
16	Corrective Action Command	Produce corrective action command(: Corrective Action Command)		safety significant
17	Corrective Action Command	Determine corrective action(: Corrective Action Command)		safety significant
18	Corrective Action Command	Select corrective action command(: Corrective Action Command [0..*], : C...	major	safety significant
19	Corrective Action Command	Produce corrective action command(: Corrective Action Command)		safety significant
20	Corrective Action Command	Determine corrective action(: Corrective Action Command)		safety significant
21	Corrective Action Command	Determine corrective action(: Corrective Action Command)		safety significant
22	Corrective Action Command	Produce corrective action command(: Corrective Action Command)		safety significant

Error checking



Document export



Booz | Allen | Hamilton

Cybersecurity controls are similar

- Cybersecurity controls may be associated with system model elements in exactly the same way:
  - Messages may be classified to error-check and ensure they flow on the correct network type
  - Controls may be applied to functions, messages, interfaces, or other system elements (and appear in tables, matrices, and traceability).
- Tables and matrices (and reuses of elements) ensures that all instances of a given message or interface are identified.

Conclusions

- System modeling, when competently applied, allows robust Functional Hazard Analysis and cybersecurity analysis.
- Reuse of model elements ensures consistency (numerous examples of non-singularized outcomes and slight wording differences were identified).
- Custom properties enable rapid visualization and enhance traceability.
- Exports of tables and matrices (or sharing via Cameo Collaborator) enable subject matter expert review.
- Report export (via document modeling) ensures 100% consistency between analysis and the final work product.