

Innovation center, Washington, D.C.

INTERDICTION: THE APPLICATION OF SYSML STATE MACHINES TO CYBERSECURITY

*Michael J. Vinarcik, ESEP-Acq / Jeff Colwander, CISSP
Senior Lead Systems Engineer /Lead Technologist
2018 NDIA Systems Engineering Conference*

OCTOBER 24, 2018

PERSPECTIVES AND DISCLAIMER

- The information and opinions presented here are drawn from my personal network and experiences and do not reflect the opinions of my employers and related organizations (including, but not limited to, Booz Allen Hamilton, the University of Detroit Mercy, the International Council on Systems Engineering, the National Defense Industrial Association, and the Object Management Group).

“I DON’T CARE WHAT ANYTHING
WAS *DESIGNED* TO DO.
I CARE ABOUT WHAT IT *CAN*
DO.”

Gene Kranz, as portrayed by Ed Harris, Apollo 13, 1995

HELP STAMP OUT BAD MODELING!

- Unfortunately, there is a lot of inferior system modeling being conducted and it is hampering the growth of this critical discipline.
- There are three primary causes:
 - Document-centric mindset
 - Unskilled practitioners
 - Inferior modeling tools
- In addition, most stakeholders are not sufficiently sophisticated to demand state-of-the-art system models.

DIAGRAM-CENTRIC VIEWPOINTS

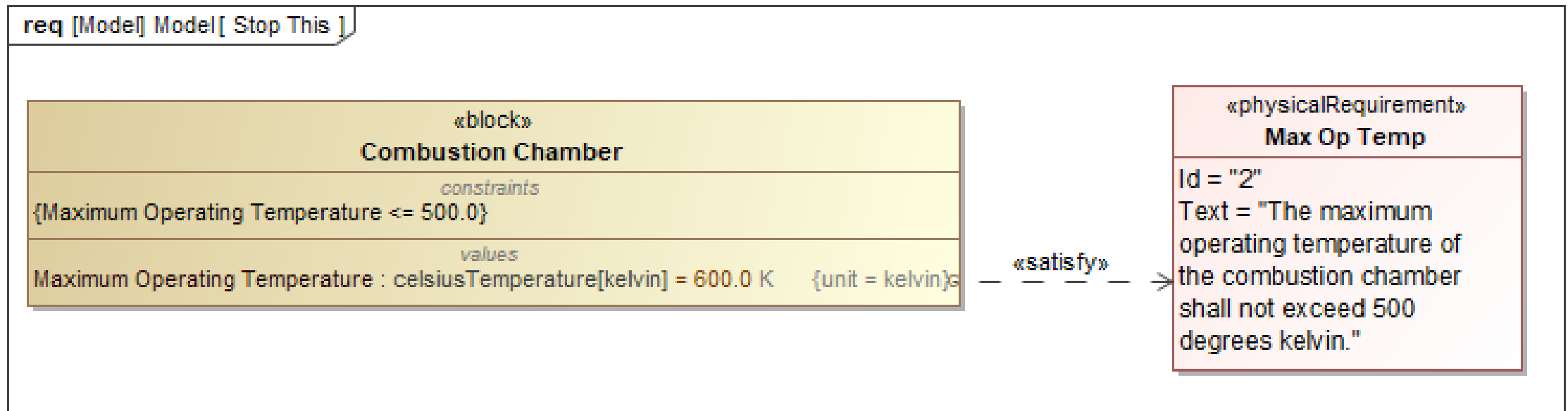
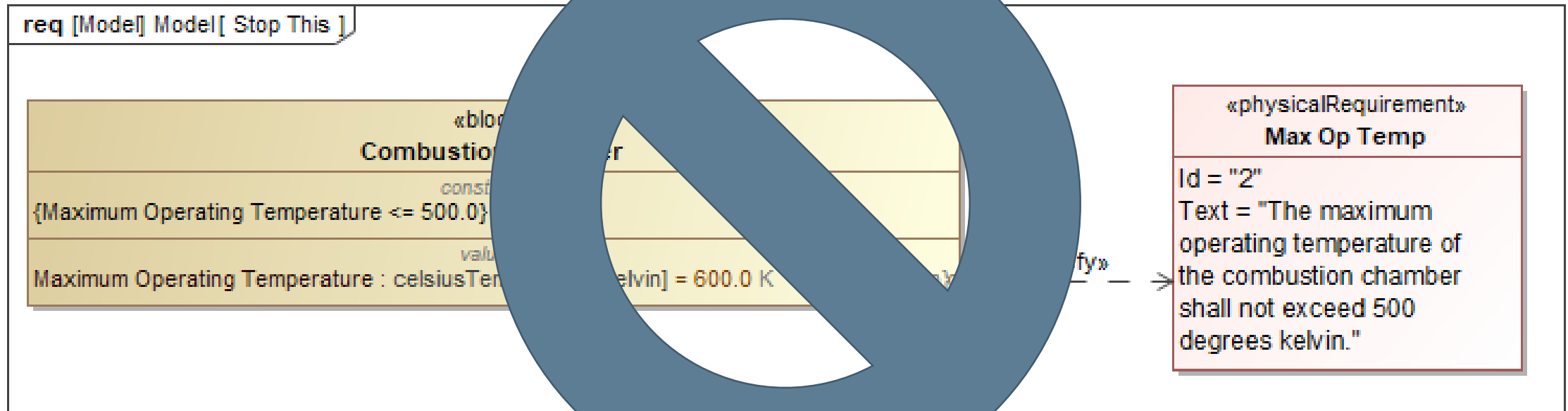
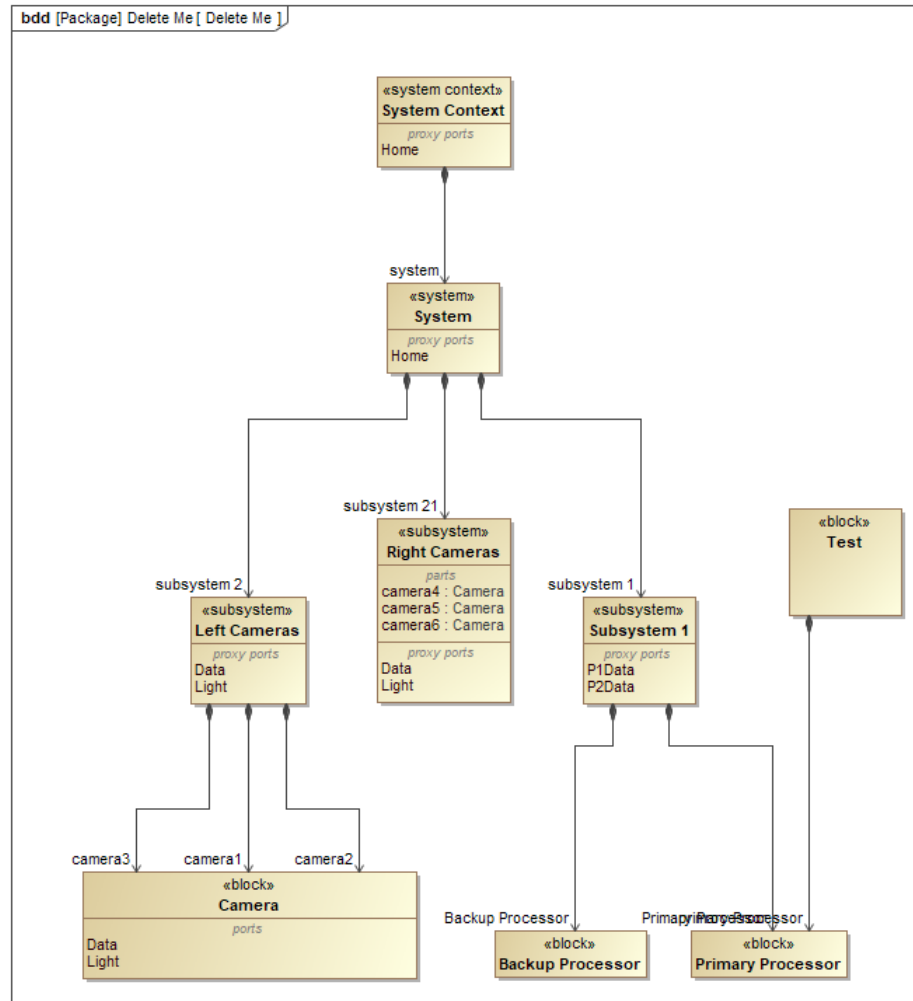


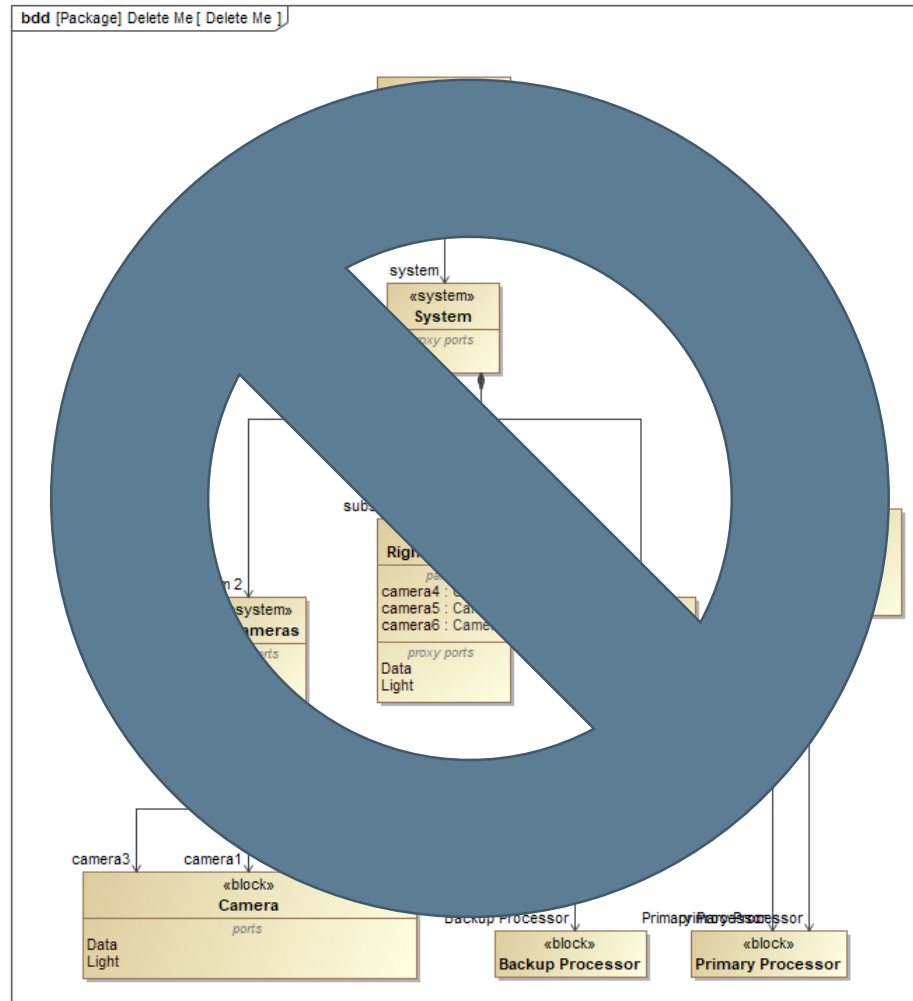
DIAGRAM-CENTRIC VIEWPOINTS



MORE DIAGRAM-CENTRIC VIEWPOINTS



MORE DIAGRAM-CENTRIC VIEWPOINTS



DESCRIPTIVE SYSTEM MODELS ARE NOT DIAGRAMS

- Descriptive system models are composed of elements, attributes, and relationships.
- Competent use of queries can be used to:
 - Identify omissions and errors
 - Expose redundancies and conflicts
 - Eliminate the need to manually tag/identify related content

Models are much more than just diagrams!

HYPERMODELING

WHAT IS HYPERMODELING?

- Hypermodeling is the author's term for his approach to system modeling using SysML.
- It is a pragmatic approach that favors minimizing the number of elements and relationships needed to fully describe a system by maximizing the use of inference and queries.
- It is aligned with the Model-Based Engineering Manifesto (available at manifesto.systemsarchitectureguild.org).

THE MODEL-BASED ENGINEERING MANIFESTO

Faced with increasing system complexity, interdependencies, breakdown of document-based methods, and other challenges, MBE provides the transformation in which we value:

- Information *over* artifacts
- Integration *over* independence
- Expressiveness with rigor *over* flexibility
- Model usage *over* model creation

We value the items on the right, but not at the sacrifice of the items on the left.

WHY A REFERENCE HYPERMODEL?

- A reference hypermodel was created to unify a variety of modeling techniques that the author had developed in the past several years and demonstrate their utility and coherence in a larger effort.
- It provides a publicly available reference model, drawn from unclassified and non-proprietary sources, that may be used as a testbed for new modeling techniques, analyses, and development.
- It was intended to challenge the status quo in modeling and demonstrate that there is a way to model systems effectively using relatively few relationships and element types while still maintaining a coherent and rigorous model narrative of the system of interest.

THE NEMO ORBITER MODEL AT HYPERMODELING.SYSTEMS

- It was constructed by six students (January 2018, MENG 5925, *Modeling of Complex Systems via SysML Programming* at the University of Detroit Mercy) in fourteen weeks.
- It was solely based on publicly available information about a NASA next generation Mars orbiter and other unclassified content.
- The NeMO hypermodel is now available at <http://hypermodeling.systems>
 - Customizations
 - Opaque behaviors
 - Reference content
- More than five hours of video (including detailed hypermodeling methods) are available at videos.systemsarchitectureguild.org.

CYBERSECURITY ANALYSIS

Q.E.D.

- What is the *Question* we need to answer?
- How can we *Extract* relevant information from the model?
- How should we *Display* it to stakeholders in a meaningful, easy to consume way?

See Tim Weilkiens's *Query-Driven Modeling* for similar concepts.

TABULAR EMPHASIS: FRED BROOKS UNDERSTOOD

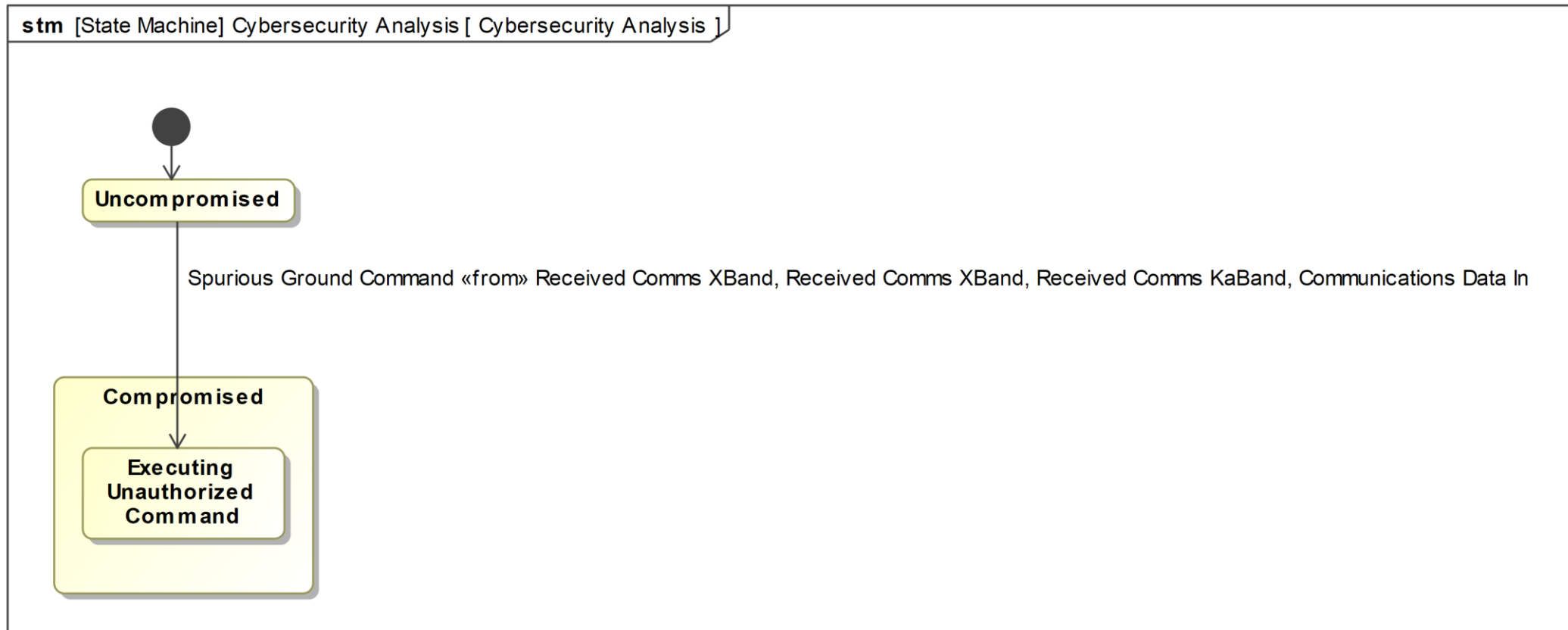
“Show me your flowcharts and conceal your tables, and I shall continue to be mystified. Show me your tables, and I won’t usually need your flowcharts; they’ll be obvious.”

From *The Mythical Man-Month: Essays on Software Engineering* (1975, 1995)
[Originally published in 1975; Brooks, Frederick, page numbers refer to the substantially expanded Anniversary Edition (2nd Edition), 1995, Addison-Wesley, ISBN 0-201-83595-9], Pp. 102–3.

IMPORTING CYBER CONTROLS

- The NeMO orbiter model was constructed without purposeful cybersecurity analysis.
- To facilitate the state machine interdiction analysis, a set of cybersecurity controls was imported into the NeMO model.
- The CIS Controls from the Center for Internet Security (www.cisecurity.org) were selected because they were readily importable and licensed under the Creative Commons license.

STATE MACHINE TO DESCRIBE VULNERABILITIES

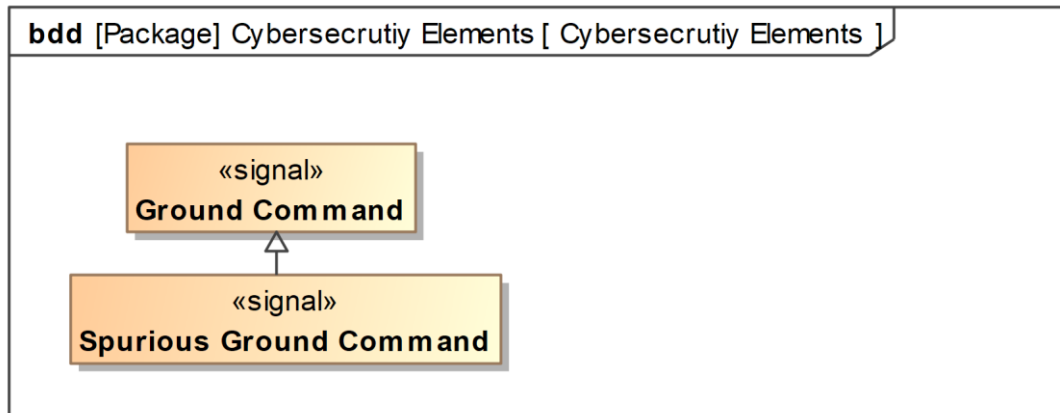


DEFINE THE TRIGGER THAT CAUSES A TRANSITION TO A COMPROMISED STATE

Trigger	
Event Type	SignalEvent
Trigger	Trigger:Spurious Ground Command [70 Analysis::Cybersecurity Analy...
Event Element	<input checked="" type="checkbox"/> SignalEvent Spurious Ground Command [70 Analysis::Cybersecurity A...
Name	
Qualified Name	70 Analysis::Cybersecurity Analysis::Cybersecurity Analysis::
Signal	Spurious Ground Command [70 Analysis::Cybersecurity Analysis::Cyb...
Element ID	_19_0_ea90360_1538360731954_244825_6811
Documentation	A spurious command is received by the orbiter and executed as a legitimate instruction.
Port	<input type="checkbox"/> out Received Comms XBand : Library::Interface Blocks::Physical Interfac <input type="checkbox"/> in Received Comms XBand : ~Library::Interface Blocks::Physical Interfac <input type="checkbox"/> in Received Comms KaBand : ~Library::Interface Blocks::Physical Interfa <input type="checkbox"/> inout Communications Data In : Library::Interface Blocks::Logical Interfa

- ***Spurious Ground Command*** is identified as triggering the Compromised substate of ***Executing Unauthorized Command***.
- The trigger is documented and assigned to possible ports (to aid in defining possible entry points).

SPECIALIZE THE LEGITIMATE SIGNAL



- Creating this relationship rigorously defines that ***Spurious Ground Command*** is a specific type of ***Ground Command***.
- This means that ***Spurious Ground Command*** is now a valid input for any function expecting a ***Ground Command***.
- This relationship now permits queries and other data manipulation.

FERRET TABLES

- **Ferret Tables** are used to rapidly determine the usages of one or more elements in a model. They leverage **Smart Packages** and self-scoping table methods to allow drag-and-drop examination of selected model elements.
- See Ferret Table video at videos.systemsarchitectureguild.org

#	Name	Owner	Architecture Level	Method	Parameter Signals	Activity Calls
1	Authenticate Message	Telecommunication Security	<<> logical [NamedElement]	Authenticate Message	Ground Command	
2	Authenticate Message	Telecommunication Security	<<> logical [NamedElement]	Authenticate Message	Ground Command	
3	Authenticate Message	Telecommunication Security	<<> physical [NamedElement]	Authenticate Message	Ground Command	
4	Compute Attitude Error	HGN&C SW	<<> physical [NamedElement]		Current Attitude Ground Command	
5	Compute Attitude Error	GN&C SW	<<> logical [NamedElement]		Current Attitude Ground Command	Correct Attitude Perform Hohmann Transfer Navigate Deep Space
6	Compute EO Trajectory	HGN&C SW	<<> physical [NamedElement]		Ground Command ME Firing Time	
7	Compute EO Trajectory	GN&C SW	<<> logical [NamedElement]		Ground Command ME Firing Time	Establish Earth Orbit
8	Compute Main Engine Firing Solution	HGN&C SW	<<> physical [NamedElement]		ME Firing Time Ground Command	
9	Compute Main Engine Firing Solution	GN&C SW	<<> logical [NamedElement]		ME Firing Time Ground Command	Navigate Deep Space
10	Interpret Ground Command	Flight Software	<<> physical [NamedElement]		Ground Command NeMO Command Signal Command Conflict	Execute Ground Command Execute Ground Command

SPURIOUS SIGNAL FERRET

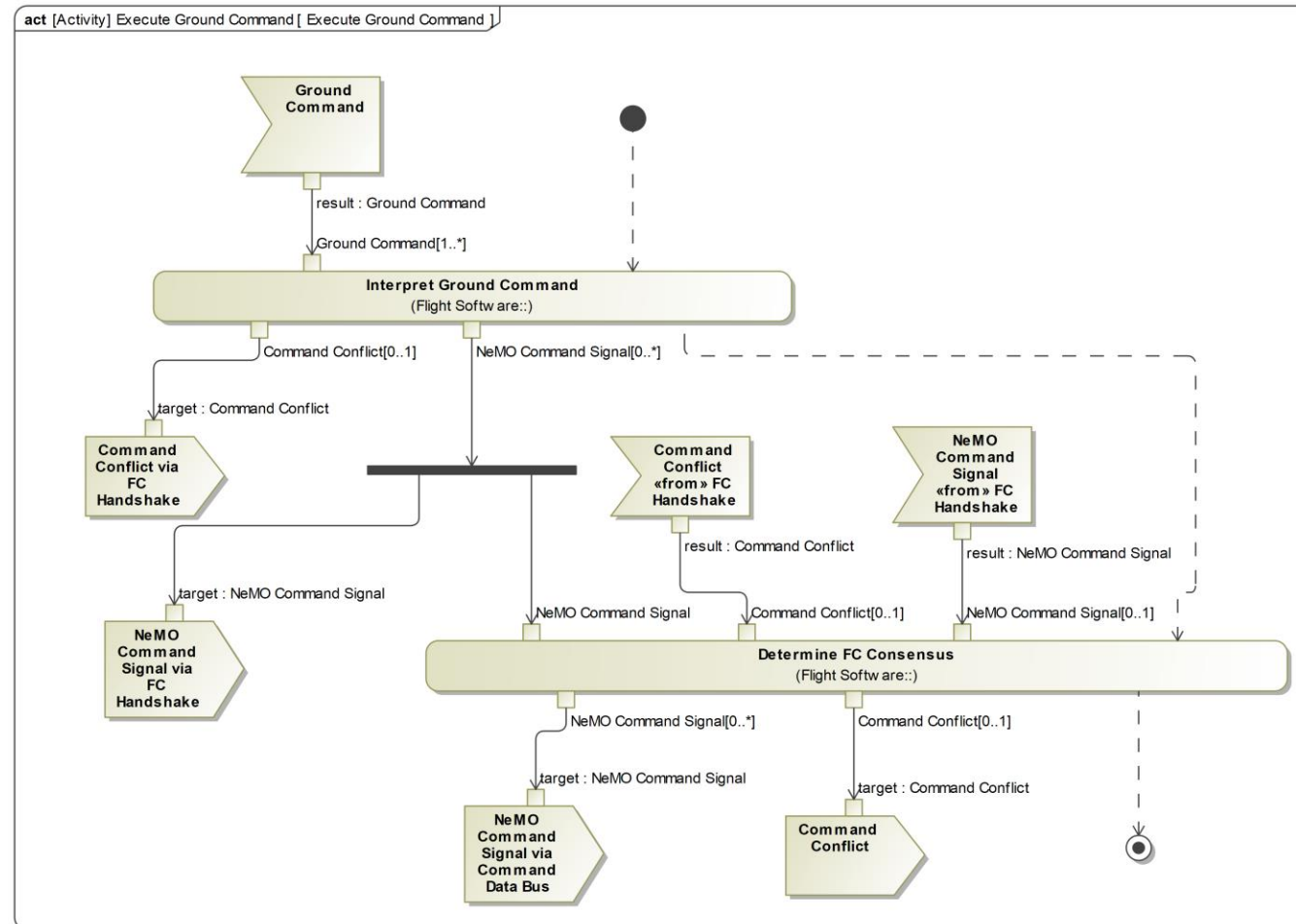
- The Signal Ferret Table was modified to follow the generalization from the ***Spurious Ground Command*** to ***Ground Command***.
- These functions use ***Ground Command*** as an input or output (and therefore may be compromised):
 - Authenticate Message
 - Monitor Ground Command
 - Compute Attitude Error
 - Compute EO Trajectory
 - Compute Main Engine Firing Solution
 - Track Horizon
 - Interpret Ground Command
 - Compute Attitude Error
 - Compute EO Trajectory

IDENTIFYING ARCHITECTURAL GAPS

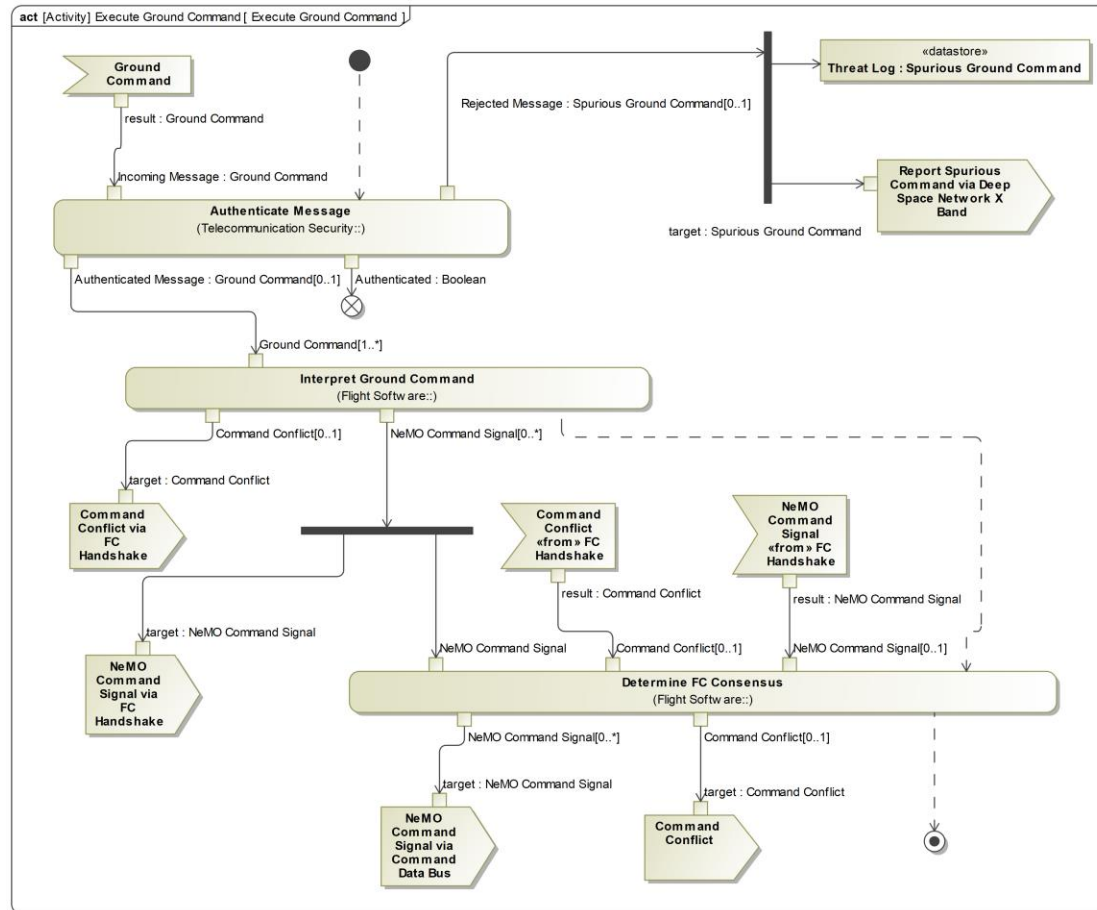
Using the *Operations Ferret*, these gaps were identified:

- *Authenticate message* was never called.
- *Interpret Ground Command* inputs *Ground Command* and outputs *NeMo Command Signal*.
- No other function should have *Ground Command* as an input parameter: *NeMO Command Signal* is the appropriate parameter.

INITIAL EXECUTE GROUND COMMAND BEHAVIOR

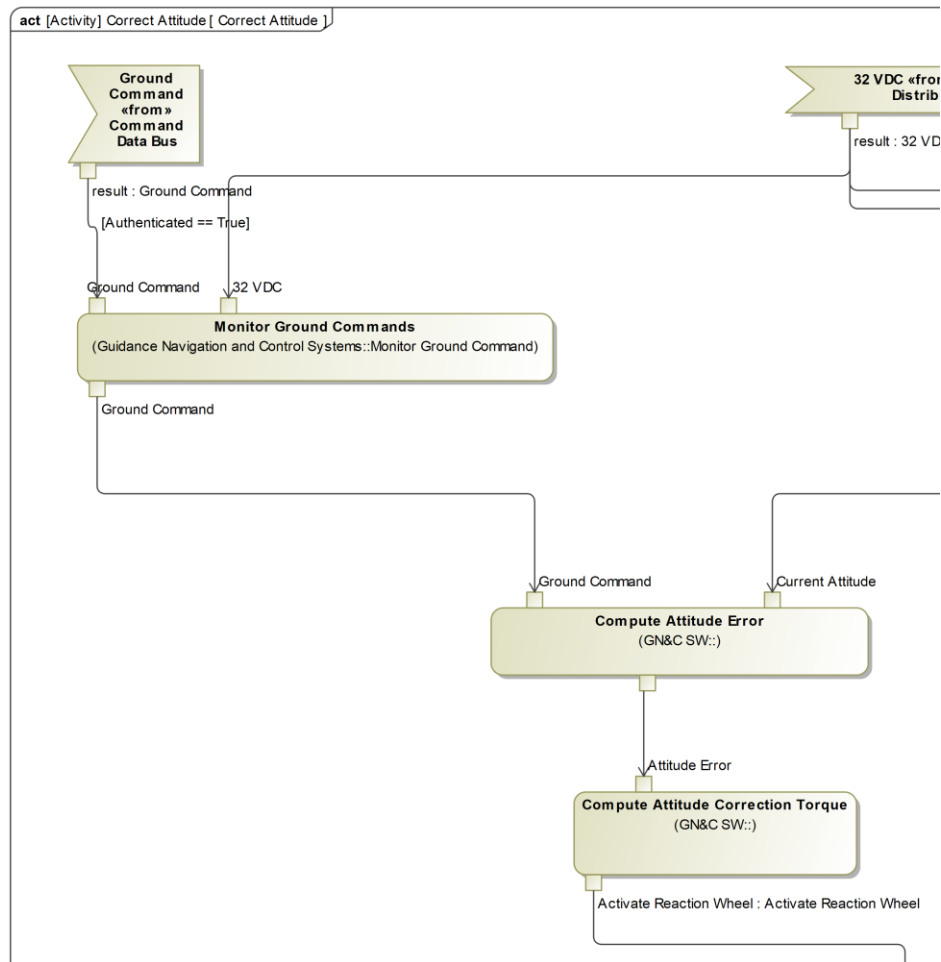


REVISED EXECUTE GROUND COMMAND BEHAVIOR



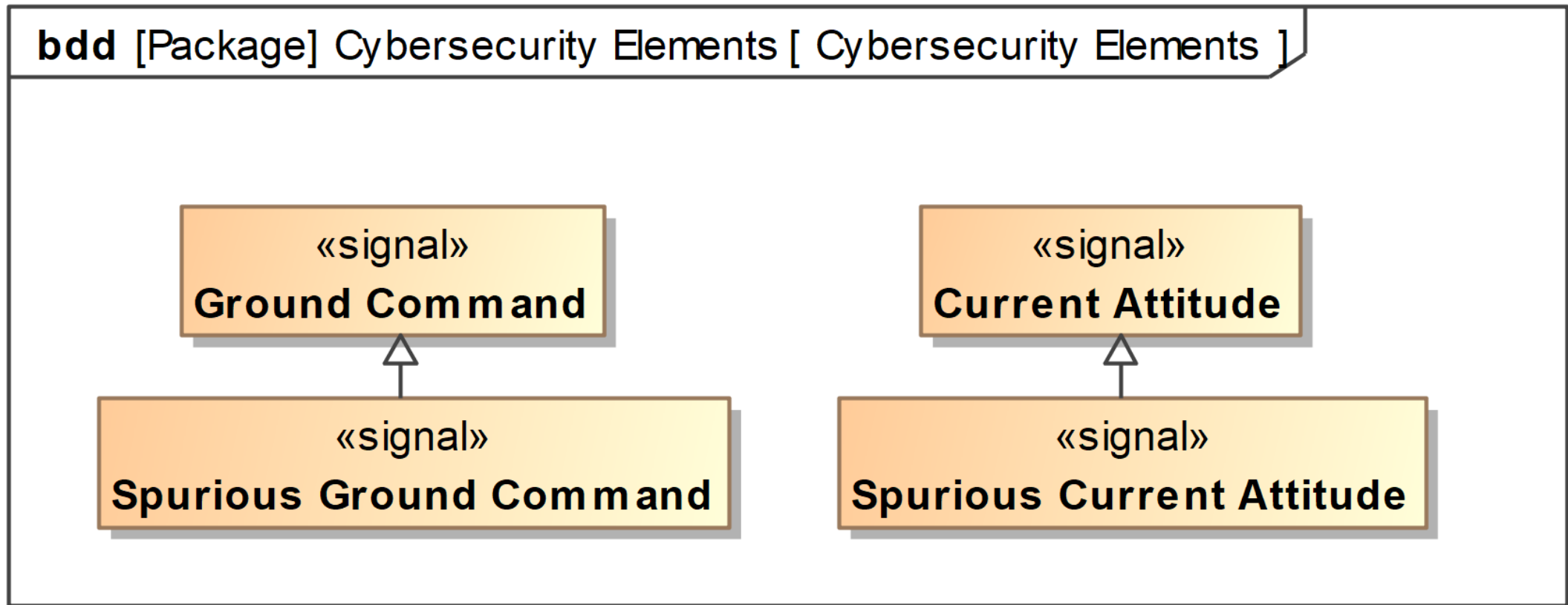
- This Revision added **Authenticate Message** operation, **Threat Logging**, and **Reporting Spurious Message via the Deep Space Network**.
- This should be the ONLY place **Ground Command** is used...the other usages should be replaced with **NeMO Command Signal**.

OTHER ACTIVITY DIAGRAMS: CORRECT ATTITUDE

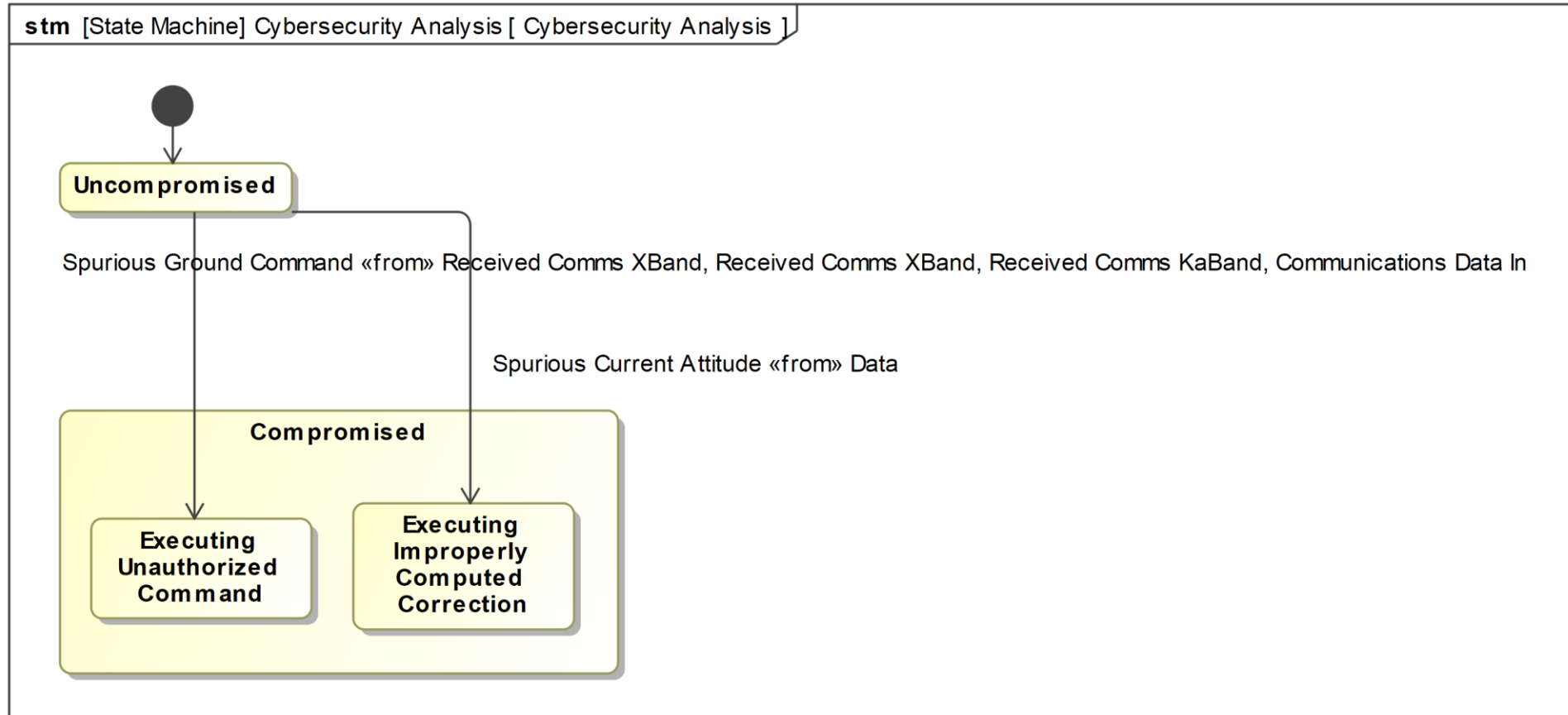


- The Operation Ferret (using all operations that input/output **Ground Command**) led to **Correct Attitude**.
- This diagram had {Authenticated == True} as a guard on **Ground Command**.
- **Compute Attitude Error** also had **Current Attitude** as an input.
- This could also be compromised by an adversary to trigger improper navigation corrections.

SPURIOUS CURRENT ATTITUDE SIGNAL ADDED












ADDITIONAL COMPROMISED STATE ADDED



TRANSITION TABLE ILLUSTRATES WHICH TRANSITIONS ARE NOT INTERDICTED

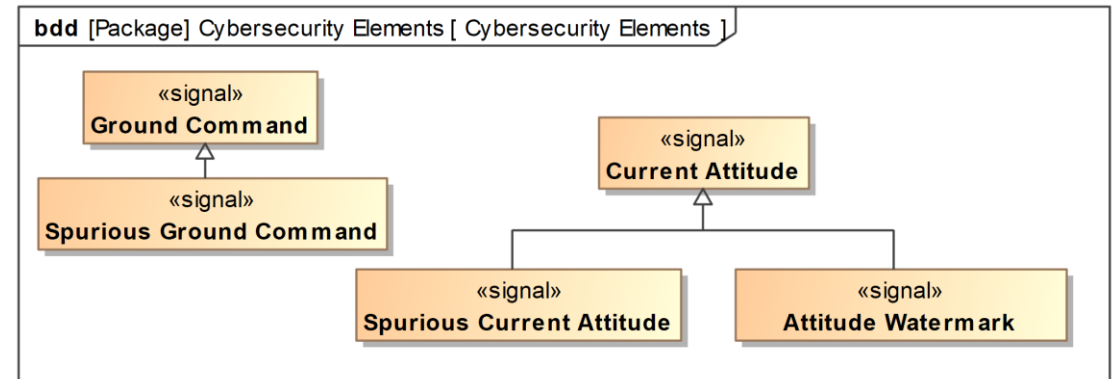
- Interdiction Boolean: The Trigger is an output of a function that satisfies a cybersecurity control.
- The Spurious commands are indistinguishable from authorized commands until filtered out and logged by an authentication function.

#	Name	Trigger	Port	Target	Source	Interdicted by Cybersecurity Function?
1		 Trigger:Spurious Current Attitude	 inout Command Data: Dat	<input type="radio"/> Executing Improperly Computed Navigation Action	<input type="radio"/> Uncompromised	<input type="checkbox"/> false
2		 Trigger:Spurious Ground Command	 out Received Comms XBanc  in Received Comms XBanc  in Received Comms KaBar  inout Communications Dal	<input type="radio"/> Executing Unauthorized Command	<input type="radio"/> Uncompromised	<input checked="" type="checkbox"/> true

AUTHENTICATING THE CURRENT ATTITUDE

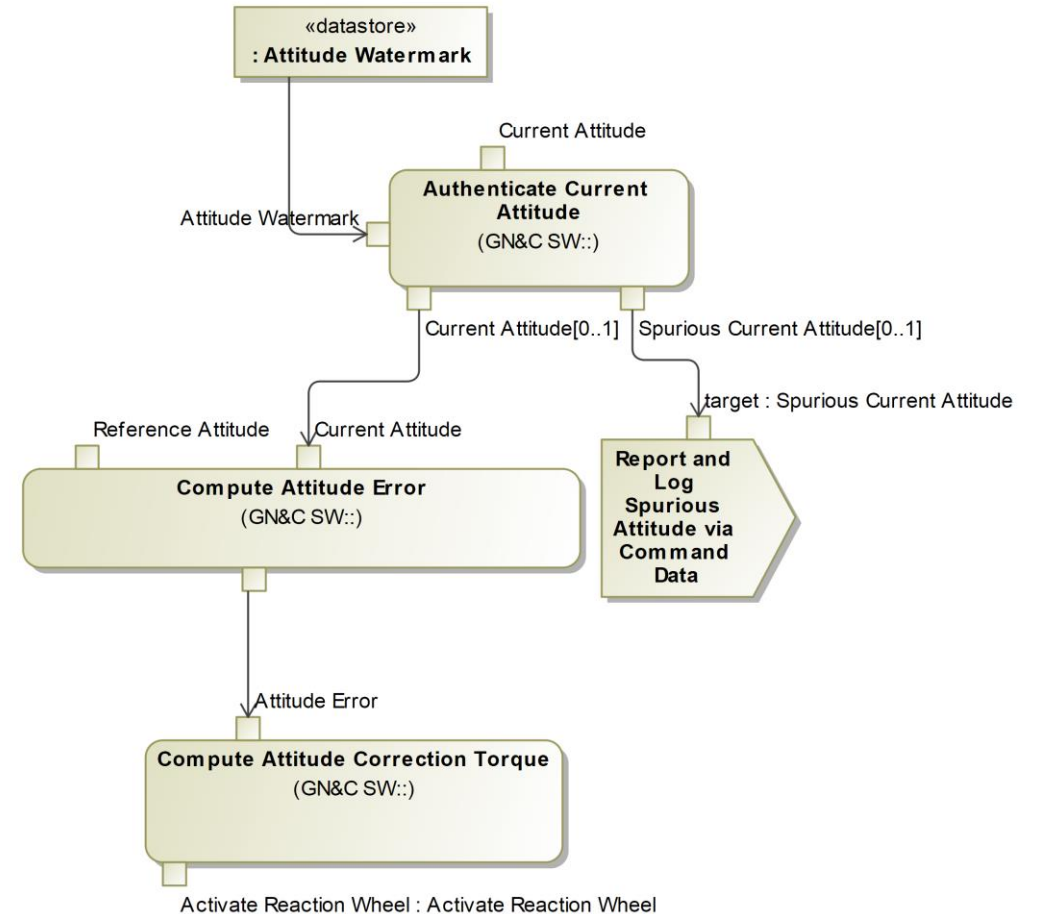
- Booz Allen has experience in protecting satellites, unmanned aerial vehicles (UAVs), and other systems from cybersecurity threats.
- One appropriate method is to introduce known perturbations (known as “dynamic watermarking”).
- This allows “spoofed” information to be detected because it lacks the expected authentication signature.

(See Dynamic Watermarking References)





ADDING AN AUTHENTICATION FUNCTION

- The addition of the **Attitude Signature** datastore and the *Authenticate Current Attitude* function interdict this transition.
- **Authenticate Current Attitude** <<satisfies>> a cybersecurity control.


















TRANSITION TABLE ILLUSTRATES ALL TRANSITIONS ARE INTERDICTED

- The addition of the authentication function and its relationship to a cybersecurity control result in this table now showing that all transitions to compromised states have been interdicted

#	Name	Trigger	Port	Target	Source	Interdicted by Cybersecurity Function?
1	↗	 Trigger:Spurious Current Attitude	<input type="checkbox"/> inout Command Data: Data	<input type="checkbox"/> Executing Improperly Computed Navigation Action	<input type="checkbox"/> Uncompromised	<input checked="" type="checkbox"/> true
2	↗	 Trigger:Spurious Ground Command	<input type="checkbox"/> out Received Comms XBand: Re <input type="checkbox"/> in Received Comms XBand: ~Re <input type="checkbox"/> in Received Comms KaBand: ~R <input type="checkbox"/> inout Communications Data In: I	<input type="checkbox"/> Executing Unauthorized Command	<input type="checkbox"/> Uncompromised	<input checked="" type="checkbox"/> true



CYBERSECURITY INTERFACE ANALYSIS TABLE

- The information in the system model can be queried to show possible transitions sorted by the port/interface which may convey them.
- This view also facilitates cybersecurity analysis

#	△ Name	Owner	Consequences	Signal Trigger
1	Command Data	 Guidance Navigation and Control Systems	 Executing Improperly Computed Navigation Acti	 Spurious Current Attitude
2	Communications Data In	 Antennas and Telecommunication	 Executing Unauthorized Command	 Spurious Ground Command
3	Received Comms KaBand	 Transponder	 Executing Unauthorized Command	 Spurious Ground Command
4	Received Comms XBand	 Transponder	 Executing Unauthorized Command	 Spurious Ground Command
5	Received Comms XBand	 HG Antenna	 Executing Unauthorized Command	 Spurious Ground Command

CYBERSECURITY SIGNALS TABLE








- This view shows the functions compromised by a spurious function, what compromised behaviors are triggered, and what functions detect the spurious signal.

#	Name	Compromised Function	Triggers	Detected by Function
1	 Spurious Current Attitude	<ul style="list-style-type: none"> GNC Sensors Update(result: Current Attitude, result1 Monitor GNC Sensors(argument: 32 VDC, Current Altit Determine Attitude(: 32 VDC) : Current Attitude Determine current attitude(): Current Attitude Compute Attitude Error(: Current Attitude, : Referenc Determine current attitude(): Current Attitude GNC Sensors Update(result: Current Attitude, result1 Determine Attitude(: 32 VDC) : Current Attitude Compute Attitude Error(: Current Attitude, : NeMO C Authenticate Current Attitude(: Current Attitude, : At 	<ul style="list-style-type: none"> Executing Improperly Computed Navigation Action 	<ul style="list-style-type: none"> Authenticate Current Attitude(: Current Attitude, : Attitude We
2	 Spurious Ground Command	<ul style="list-style-type: none"> Interpret Ground Command(: Ground Command[1..*] Interpret Ground Command(: Ground Command[1..*] Authenticate Message(Incoming Message: Ground Co Authenticate Message(Incoming Message: Ground Co 	<ul style="list-style-type: none"> Executing Unauthorized Command 	<ul style="list-style-type: none"> Authenticate Message(Incoming Message: Ground Command Authenticate Message(Incoming Message: Ground Command

REVISIONS

- The Signal Ferret table was used to replace all ***Ground Command*** inputs with ***NeMO Command Signal*** except for ***Authenticate Message*** and ***Interpret Ground Command***.
- Multiple ***Authenticate Message*** functions were identified; they were reduced to two (one in logical architecture, one in the physical architecture).
- ***Authenticate Message*** <<satisfies>> CISv7-16.3 (Require Multi-factor Authentication).

CIS TABLE SHOWING SATISFY RELATIONSHIPS

#	Name	Text	Asset Type	Security Function	Traced To	Satisfied By
31	 CISv7-4.4 Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	Users	Protect		
32	 CISv7-4.5 Use Multifactor Authentication For All Administrative Ac	Use multi-factor authentication and encrypted channels for all administrative account access.	Users	Protect		
92	 CISv7-11.5 Manage Network Devices Using Multi-Factor Authent	Manage all network devices using multi-factor authentication and encrypted sessions.	Network	Protect		
98	 CISv7-12.11 Require All Remote Login to Use Multi-factor Authent	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor	Users	Protect		
140	 CISv7-16.3 Require Multi-factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	Users	Protect		<ul style="list-style-type: none">  Authenticate Message(Inc  Authenticate Message(Inc

CONCLUSION

- Integrating cybersecurity analysis into a descriptive system model allows rigorous identification of potential threats.
- Characterizing threats as triggering transitions into compromised states is a convenient method for representing them.
- Specializing existing messages/signals allows rigorous detection of all impacted functions.
- Refactoring the model to remove unintended uses of messages improves security and consistency.
- The application of novel authentication methods (such as physical perturbations) is facilitated by this analysis.

DYNAMIC WATERMARKING REFERENCES

- Kumar, P.R. and Satchidanandan, B. (2017). *Dynamic Watermarking: Active Defense of Networked Cyber-Physical Systems*. Proceedings of the IEEE, 105(2), 219-240.
- Mo, Y., Weerakkody, S., and Sinopoli, B. (2015). *Physical Authentication of Control Systems: Designing Watermarked Control Inputs to Detect Counterfeit Sensor Outputs*. IEEE Control Systems, 35(1), 93–109.
- Marquis, V., Ho, R., Rainey, W., Kimpel, M., Ghiorzi, J., Cricchi, W., and Bezzo, N. (2018). *Toward Attack-Resilient State Estimation and Control of Autonomous Cyber-Physical Systems*. 2018 Systems and Information Engineering Design Symposium (SIEDS), 27-27 April 2018.

QUESTIONS?

CONTACT INFORMATION



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

vinarcik_michael@bah.com

Model available at
<http://www.showmethewow.com>