31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

Experience in Designing for Cyber Resiliency in Embedded DoD Systems

www.incose.org/symp2021

Jennifer Barzeele, CISSP
Raytheon Intelligence and Space
El Segundo, CA
Jennifer.S.Barzeele@rtx.com

Liana Suantak, PhD
Raytheon Missiles & Defense
Tucson, AZ
Liana.Suantak@rtx.com

Mike Robinson
Raytheon Missiles & Defense
Tucson, AZ
Michael.D.Robinson@rtx.com

Patrice Williams
Raytheon Intelligence and Space
Sterling, VA
Patrice.Dillon.Williams@rtx.com

John Merems
Raytheon Missiles & Defense
Tucson, AZ
John.A.Merems@rtx.com

Kit Siu, PhD
General Electric Research
Niskayuna, NY
Siu@ge.com

Michael Durling
General Electric Research
Niskayuna, NY
Durling@ge.com

Daniel Prince
GE Aviation
Grand Rapids, MI
Daniel.Prince@ge.com

Abha Moitra, PhD
General Electric Research
Niskayuna, NY
MoitraA@ge.com

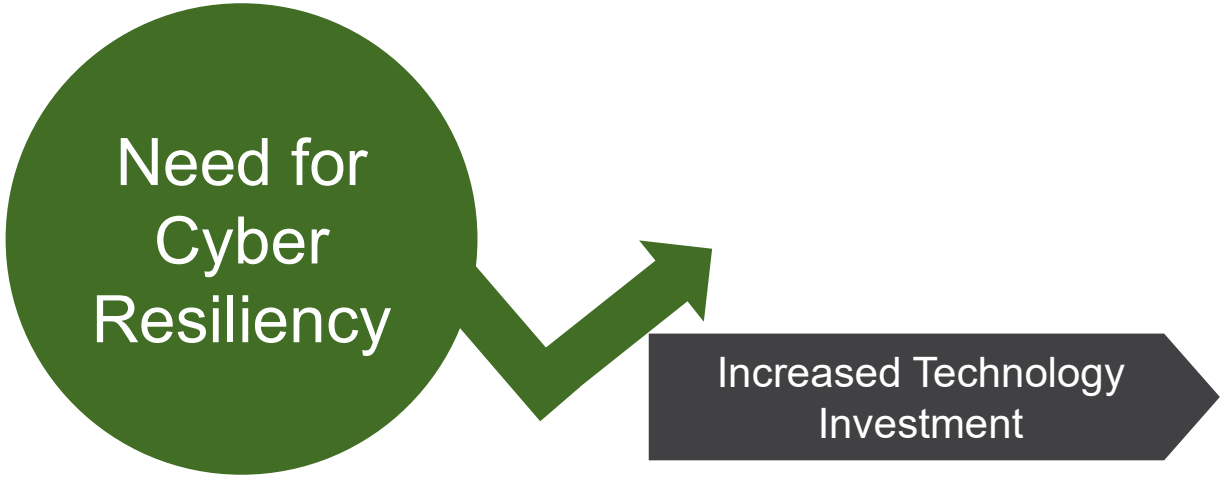
Baoluo Meng, PhD
General Electric Research
Niskayuna, NY
Baoluo@ge.com

What Is Cyber Resiliency?

Ability for the system to achieve all, or part, of its mission requirements in the face of a cyber attack

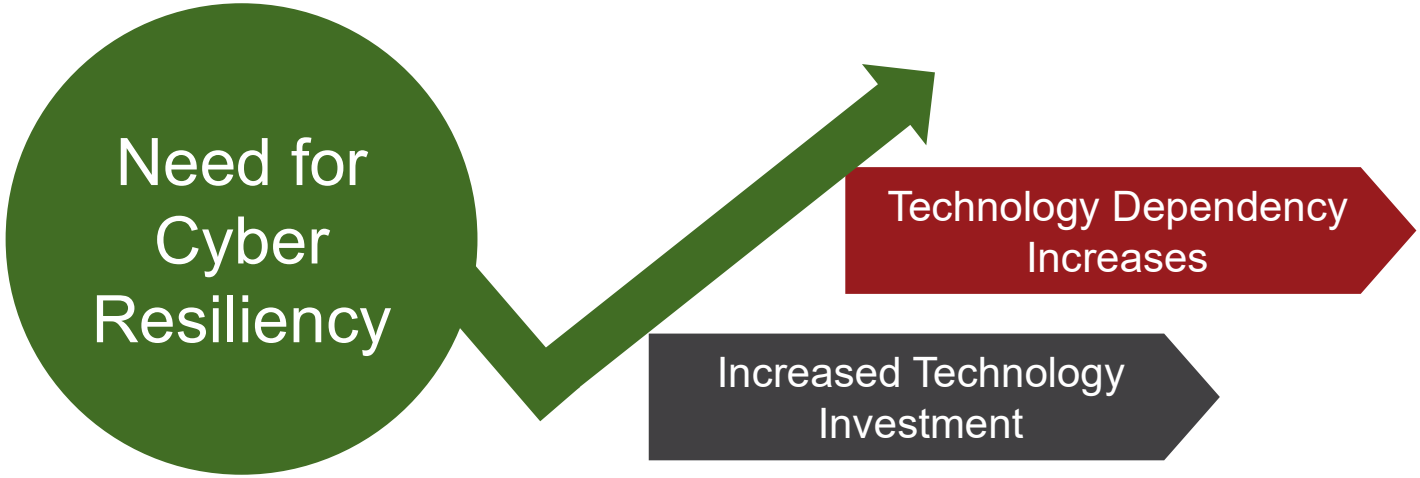
Why Model for Cyber Resiliency?

Today's increasingly complex capability needs for embedded systems are driving an increased investment in innovative technology



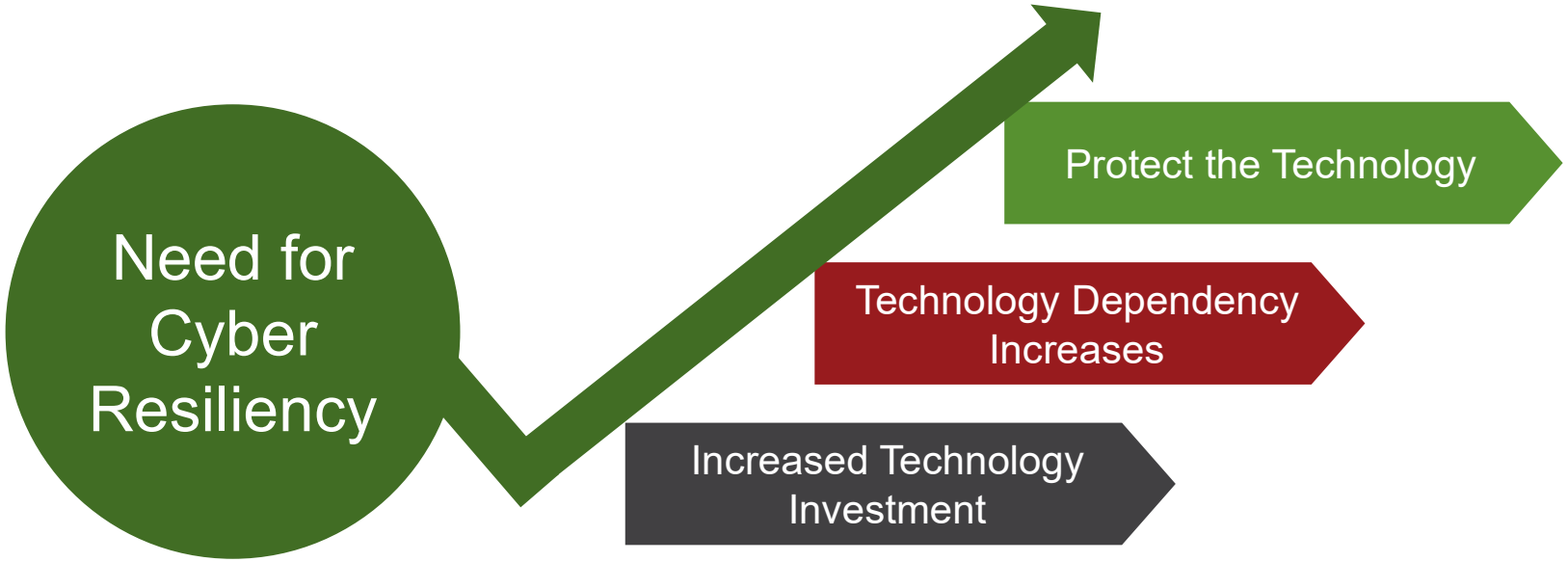
Why Model for Cyber Resiliency?

As the functionality of embedded systems increases, the systems become more dependent on the technology operating as intended



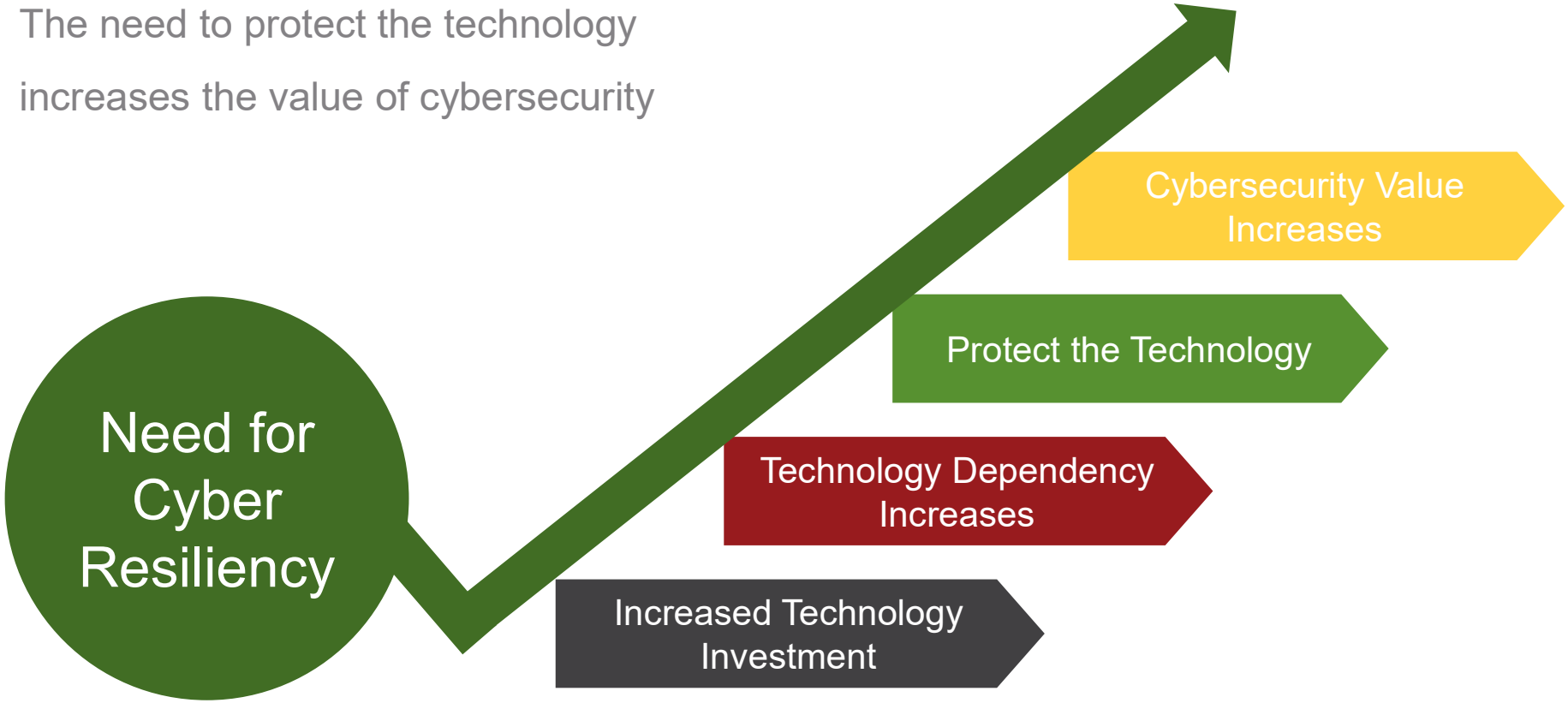
Why Model for Cyber Resiliency?

The increased dependency on technology increases the need to protect that technology



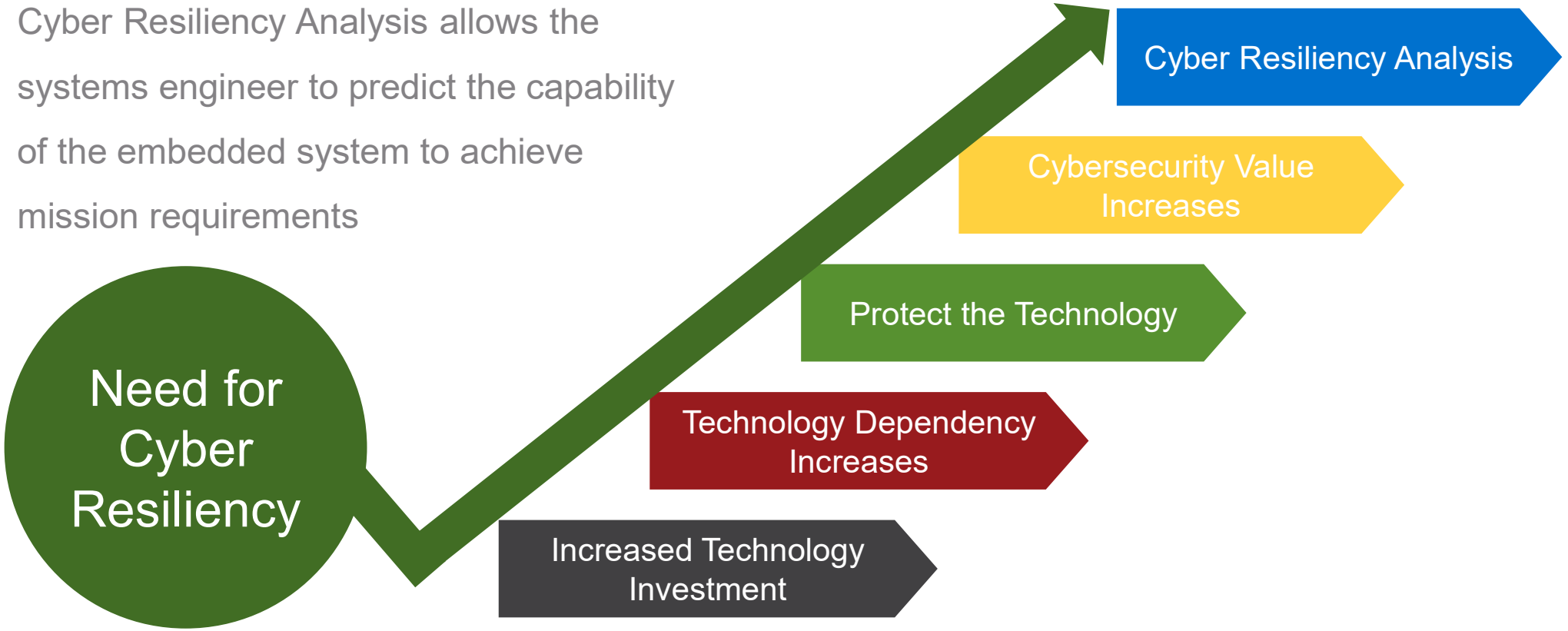
Why Model for Cyber Resiliency?

The need to protect the technology increases the value of cybersecurity



Why Model for Cyber Resiliency?

Cyber Resiliency Analysis allows the systems engineer to predict the capability of the embedded system to achieve mission requirements



Cyber Assured Systems Engineering (CASE)

- Main Objective
  - Develop open source tools that enable system engineers to design for cyber resiliency
  - Model-based architecture synthesis function generates solutions that satisfy both safety and security requirements
- Innovations
  - Synthesis of cyber resilient architectures considering both safety and security
  - Localized feedback of components responsible for cyber property violation
  - Highly automated threat/design model instrumentation
  - Ability to reason about future attacks

31st Annual INCOSE international symposium

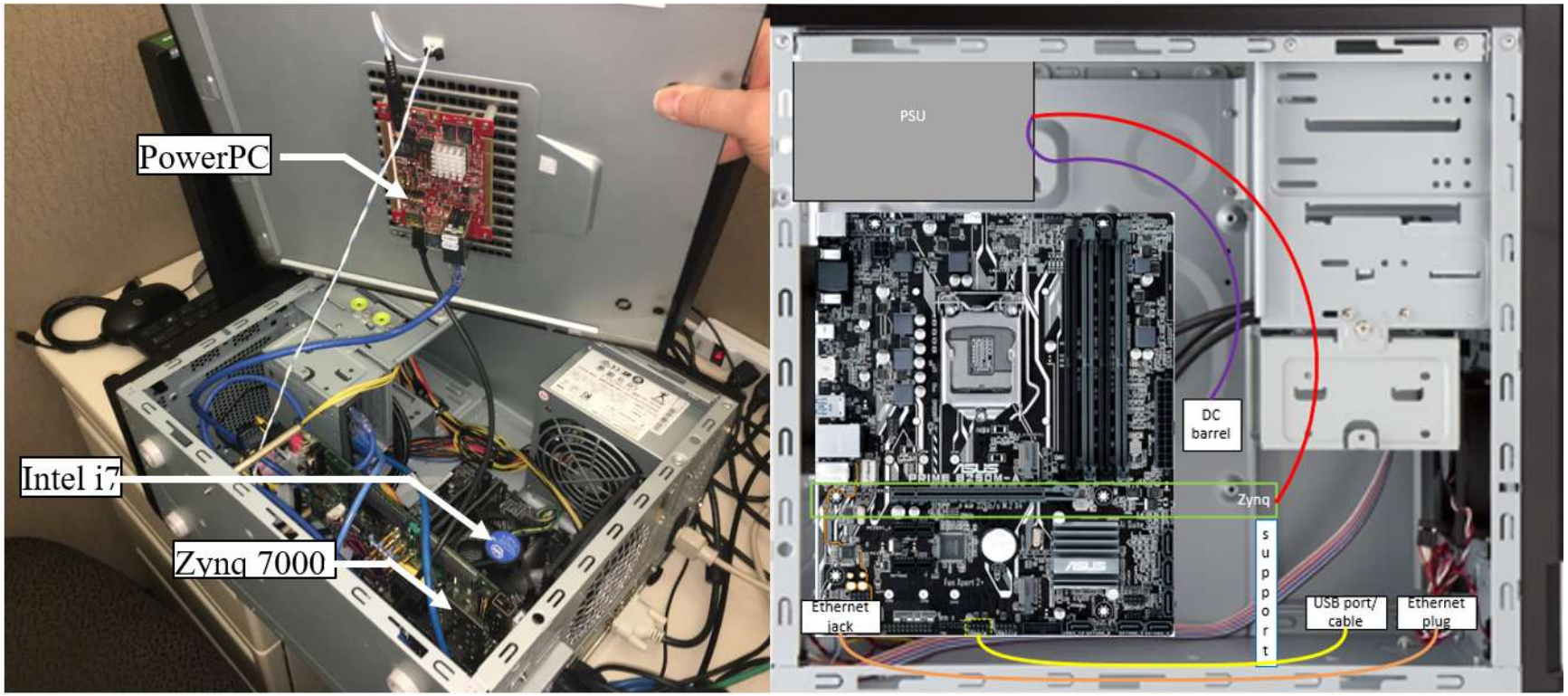
virtual event

July 17 - 22, 2021

Experimental Platform (EXP)

www.incose.org/symp2021

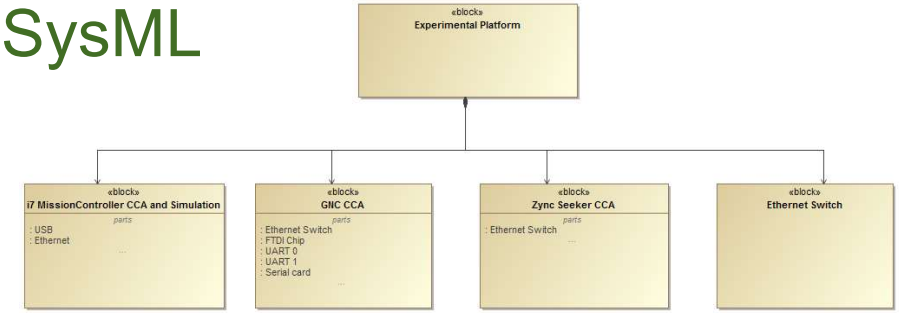
Experimental Platform (EXP)



	Component	Prior Program	HW	OS
Legacy	GNC	SLLM	PowerPC	VxWorks
Modified	MM	CODE	Intel i7	CentOS
New	Seeker	--	Zynq-7000	VxWorks

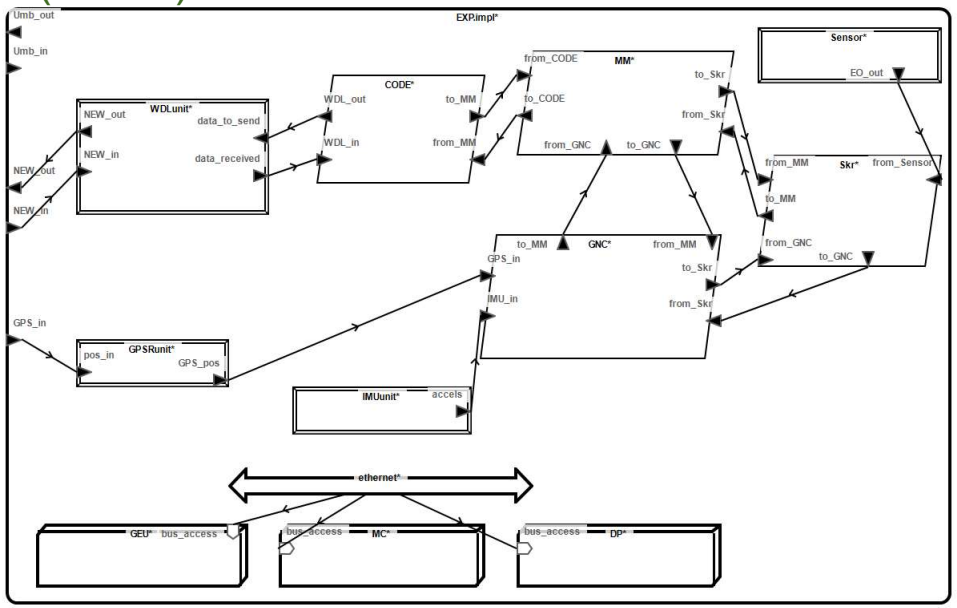
Systems Engineering Modeling

SysML



- Has been used on many previous programs
- Provides functional view of the system
  - Sequence Diagrams
  - State Machine Diagrams
  - Use Cases
  - Requirements Diagrams
- Lacks the specific connection information required for cyber resiliency analysis

Architecture Analysis and Design Language (AADL)

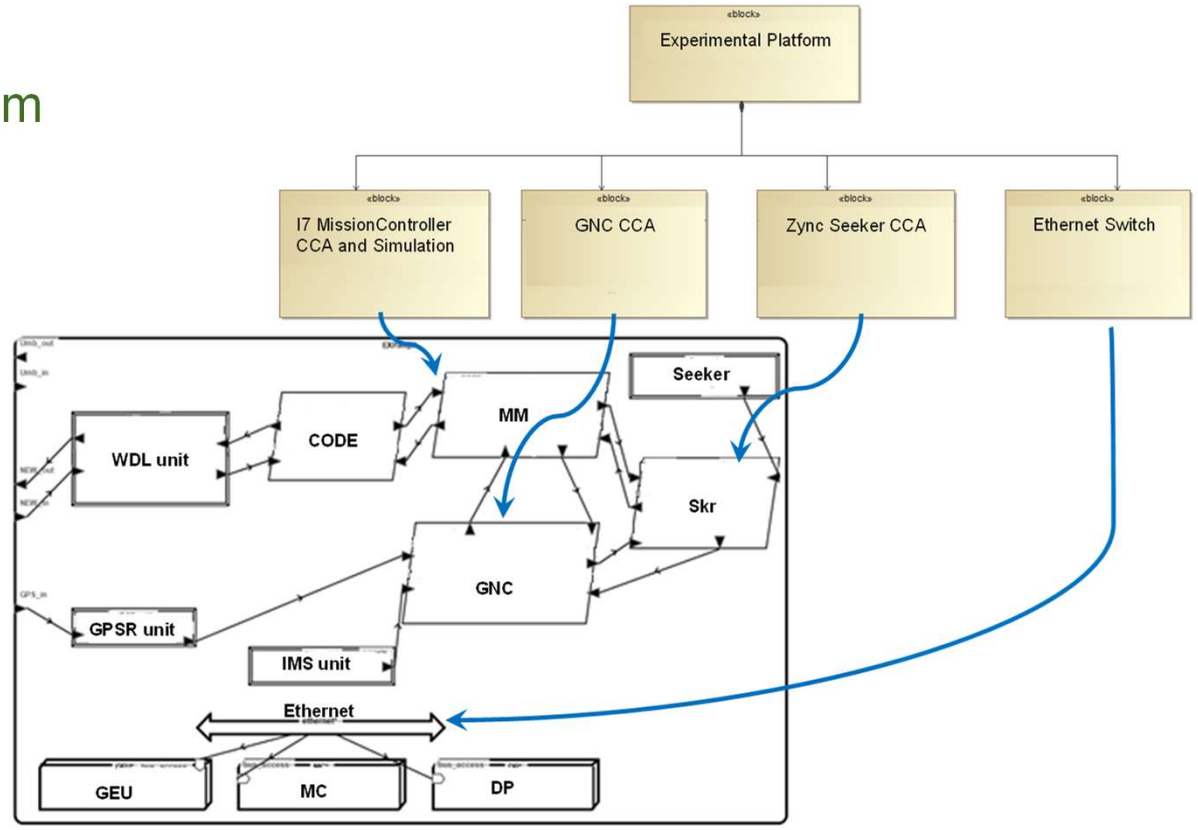


- Provides component and interface models – see next slides

SysML and AADL Comparison for EXP

Two distinct views of the same system

- SysML for high-level modeling
- AADL for lower-level implementation
- SysML for upfront System Engineering, AADL for design and analysis
- Map SysML model elements onto actual implementation blocks
- AADL provides the relevant connection properties and features for an analysis of the cyber resiliency potential of the system



31st Annual INCOSE international symposium

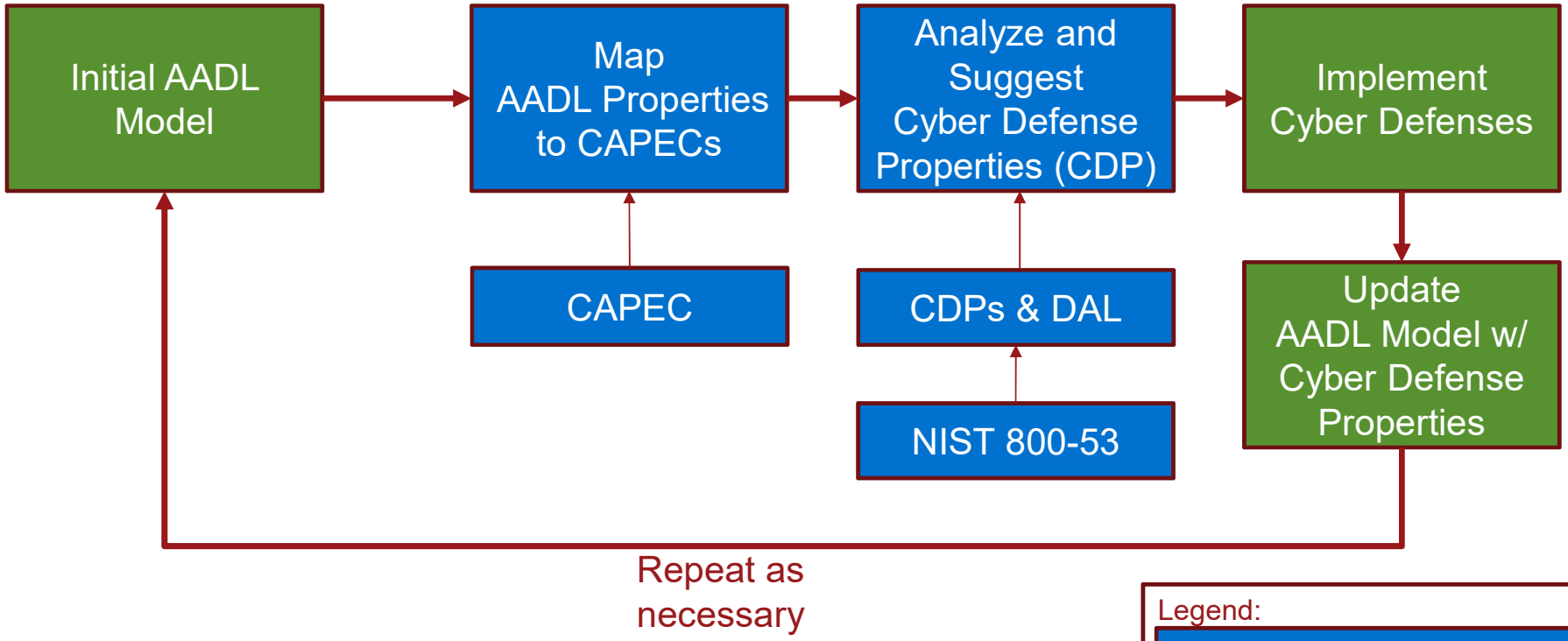
virtual event

July 17 - 22, 2021

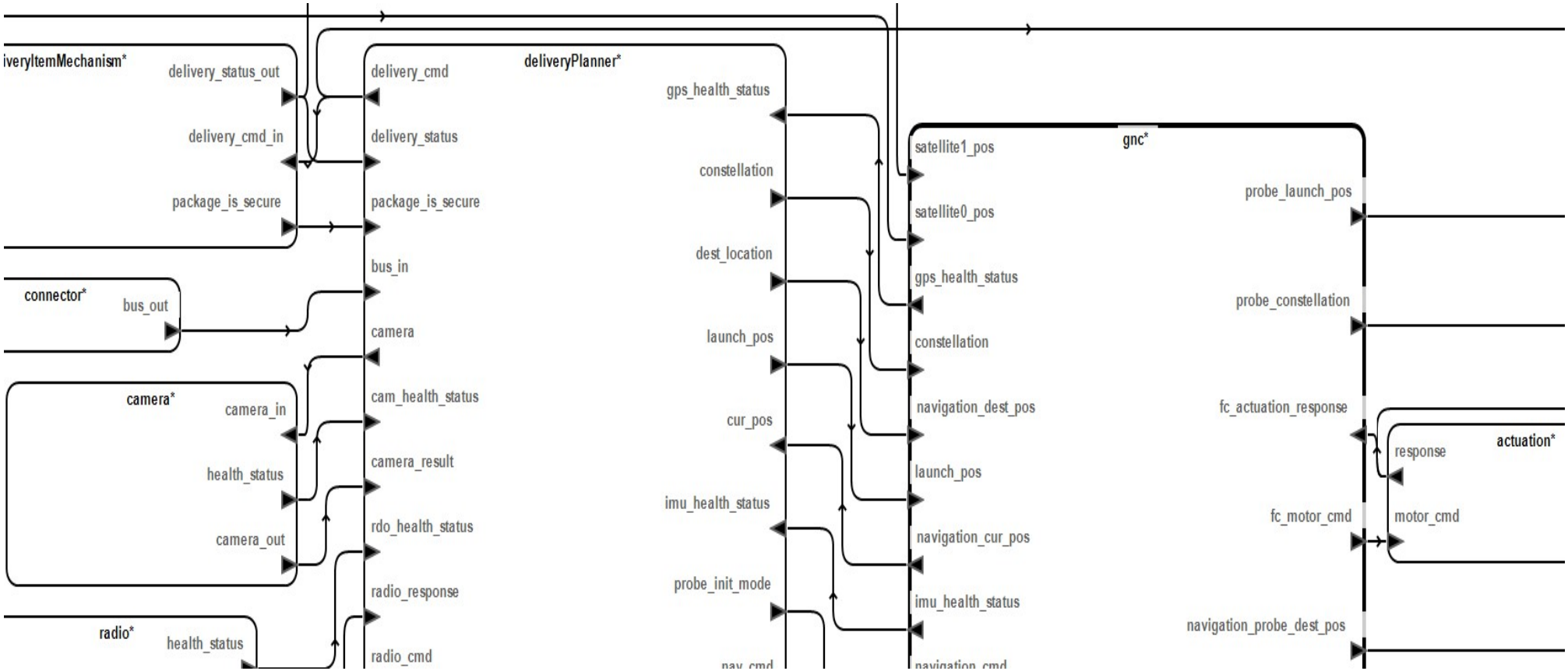
Verification Evidence and Resilient Design In anticipation of Cybersecurity Threats (VERDICT)

www.incose.org/symp2021

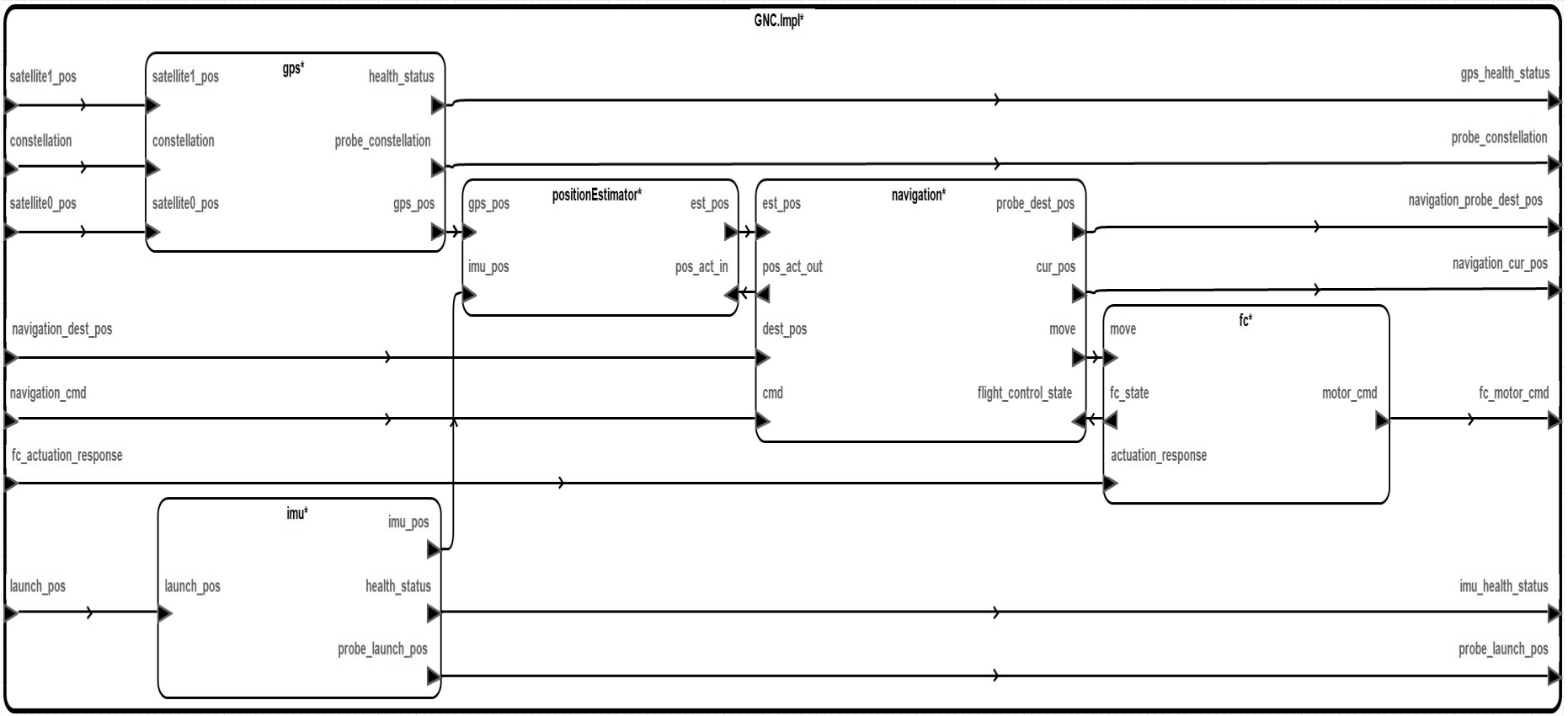
Cyber Resiliency Analysis Workflow



EXP Architecture Example



GNC Subcomponent



AADL Model Annotation with Cyber Requirements

```
annex verdict{**
    CyberReq {
    id = "CyberReq01"
    description = "The drone shall be resilient to loss of ability to deliver a package to
                  the appropriate consumer location"
    condition = actuation_out:I or actuation_out:A or delivery_status:I or delivery_status:A
    cia = I
    severity = Hazardous
        };
    CyberReq {
    id = "CyberReq02"
    description = "The drone shall be resilient to maliciously commanded improper delivery of a package"
    condition = delivery_status:I
    cia = I
    severity = Major
    };
    MissionReq {
        id ="MReq01"
        description = "Deliver a package to the intended location."
        reqs = "CyberReq01","CyberReq02"
    };
**};
```

AADL Model Annotation with Cyber Relationships

```
system Navigation
    features
        -- inputs
        est_pos: in data port Data_Types::Position.impl;
        dest_pos: in data port Data_Types::Position.impl;
        cmd: in data port Base_Types::Boolean;
        flight_control_state: in data port Base_Types::Boolean;

        -- outputs
        move: out data port Base_Types::Boolean;
        cur_pos: out data port Data_Types::Position.impl;
        pos_act_out: out data port Data_Types::Position.impl;
        probe_dest_pos: out data port Data_Types::Position.impl
        {CASE_Consolidated_Properties::probe => true; };

    annex verdict {**
        CyberRel "move_out_I"         = est_pos:I or cmd:I or flight_control_state:I => move:I;
        CyberRel "move_out_A"         = est_pos:A or cmd:A or flight_control_state:A => move:A;
        CyberRel "nav_location_out_I" = est_pos:I or cmd:I or flight_control_state:I => cur_pos:I;
        CyberRel "nav_location_out_A" = est_pos:A or cmd:A or flight_control_state:A => cur_pos:A;
        CyberRel "pos_act_out_I"      = est_pos:I or cmd:I or flight_control_state:I => pos_act_out:I;
        CyberRel "pos_act_out_A"      = est_pos:A or cmd:A or flight_control_state:A => pos_act_out:A;
    **};
end Navigation;
```

AADL Model Annotation with Component Properties

```
system implementation GNC.Impl
    subcomponents
        gps: system GPS
        {
            -- VERDICT Component Properties
            CASE_Consolidated_Properties::insideTrustedBoundary => true;
            CASE_Consolidated_Properties::componentType => Hybrid;
            CASE_Consolidated_Properties::pedigree => COTS;
        };

system implementation DeliveryDroneSystem.Impl
    subcomponents
        gnc: system GNC::GNC.Impl
        {
            -- VERDICT Component Properties
            CASE_Consolidated_Properties::insideTrustedBoundary => true;
            CASE_Consolidated_Properties::componentType => Software;
            CASE_Consolidated_Properties::pedigree => InternallyDeveloped;
            CASE_Consolidated_Properties::hasSensitiveInfo => true; --NOTE: this system may contain Waypoints
            CASE_Consolidated_Properties::canReceiveSWUpdate => false;
        };
```

VERDICT Analysis Results

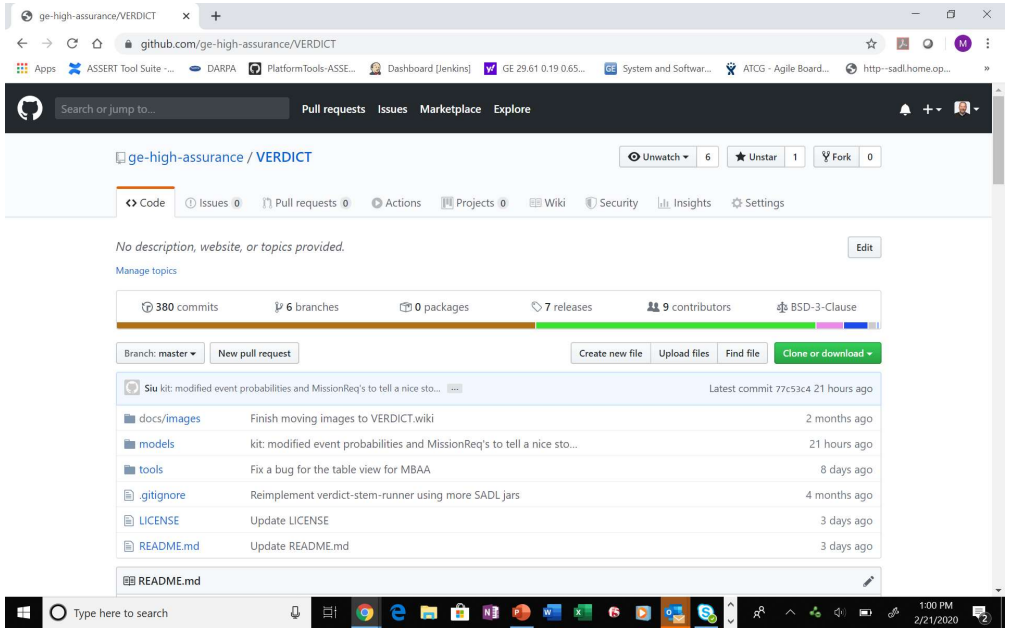
Problems | Properties | AADL Property Values | Classifier Information | Error Log | Console | MBAA Result | Search | Security Failure Paths

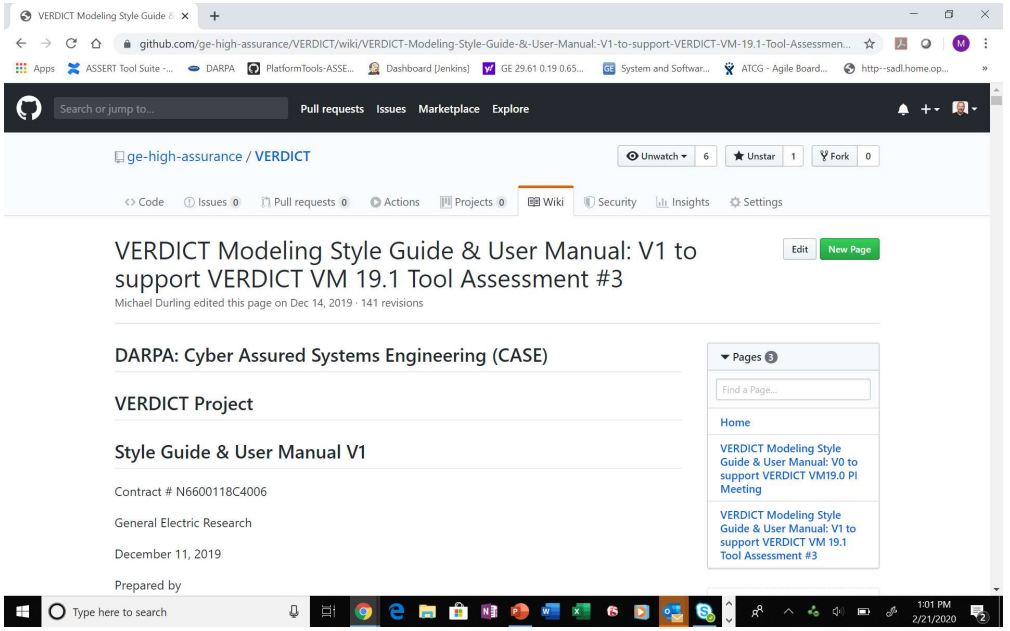
Minimal Failure Path	Path Likelihood	Attack Type	Suggested Defenses	Suggested Defenses Profile
Path # 61	1.	gnc:CAPEC-176	gnc:(MemoryProtection and RemoteAttestation and SecureBoot)	gnc:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7
Path # 62	1.	gnc:CAPEC-184	gnc:(MemoryProtection and RemoteAttestation and SecureBoot)	gnc:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7
Path # 63	1.	gnc:CAPEC-624	gnc:PhysicalAccessControl or SystemAccessControl	gnc:PE-3 or (PE-3 and PE-3-1
Path # 64	1.	gps:CAPEC-176	gps:(MemoryProtection and RemoteAttestation and SecureBoot)	gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7
Path # 65	1.	gps:CAPEC-184	gps:(MemoryProtection and RemoteAttestation and SecureBoot)	gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7
Path # 66	1.	gps:CAPEC-438	gps:(SupplyChainSecurity and TamperProtection)	gps:(SA-12 and SA-18-1)
Path # 67	1.	gps:CAPEC-439	gps:(SupplyChainSecurity and TamperProtection)	gps:(SA-12 and SA-18-1)
Path # 68	1.	gps:CAPEC-440	gps:PhysicalAccessControl or SystemAccessControl or TamperProtection	gps:PE-3 or SA-18-1 or (PE-3 and F
Path # 69	1.	gps:CAPEC-507	gps:PhysicalAccessControl or SystemAccessControl	gps:PE-3 or (PE-3 and PE-3-1
Path # 70	1.	gps:CAPEC-549	gps:(MemoryProtection and RemoteAttestation and SecureBoot)	gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7
Path # 71	1.	gps:CAPEC-624	gps:PhysicalAccessControl or SystemAccessControl	gps:PE-3 or (PE-3 and PE-3-1
Path # 117	1e-07	navigation:CAPEC-242	navigation:(InputValidation and Logging)	navigation:(AU-12 and AU-12-1 and AU-12-3 and AU-9 and
Path # 118	1e-07	navigation:CAPEC-248	navigation:(InputValidation and Logging)	navigation:(AU-12 and AU-12-1 and AU-12-3 and AU-9 and

Classifier Information | Error Log | Console | MBAA Result | Search | Security Failure Paths

Suggested Defenses Profile	Implemented Defenses
gnc:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7-5 and SI-7-6 and SI-7-9)	
gnc:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7-5 and SI-7-6 and SI-7-9)	
gnc:PE-3 or (PE-3 and PE-3-1)	
gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7-5 and SI-7-6 and SI-7-9)	
gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7-5 and SI-7-6 and SI-7-9)	
gps:(SA-12 and SA-18-1)	
gps:(SA-12 and SA-18-1)	
gps:PE-3 or SA-18-1 or (PE-3 and PE-3-1)	
gps:PE-3 or (PE-3 and PE-3-1)	
gps:(IA-3-4 and SI-16 and SI-7-1 and SI-7-15 and SI-7-5 and SI-7-6 and SI-7-9)	
gps:PE-3 or (PE-3 and PE-3-1)	
navigation:(AU-12 and AU-12-1 and AU-12-3 and AU-9 and AU-9-3 and SI-10 and SI-10-5)	navigation:(inputValidation and logging)
navigation:(AU-12 and AU-12-1 and AU-12-3 and AU-9 and AU-9-3 and SI-10 and SI-10-5)	navigation:(inputValidation and logging)

VERDICT Open Source on GitHub





https://github.com/ge-high-assurance/VERDICT

31st Annual INCOSE international symposium

virtual event

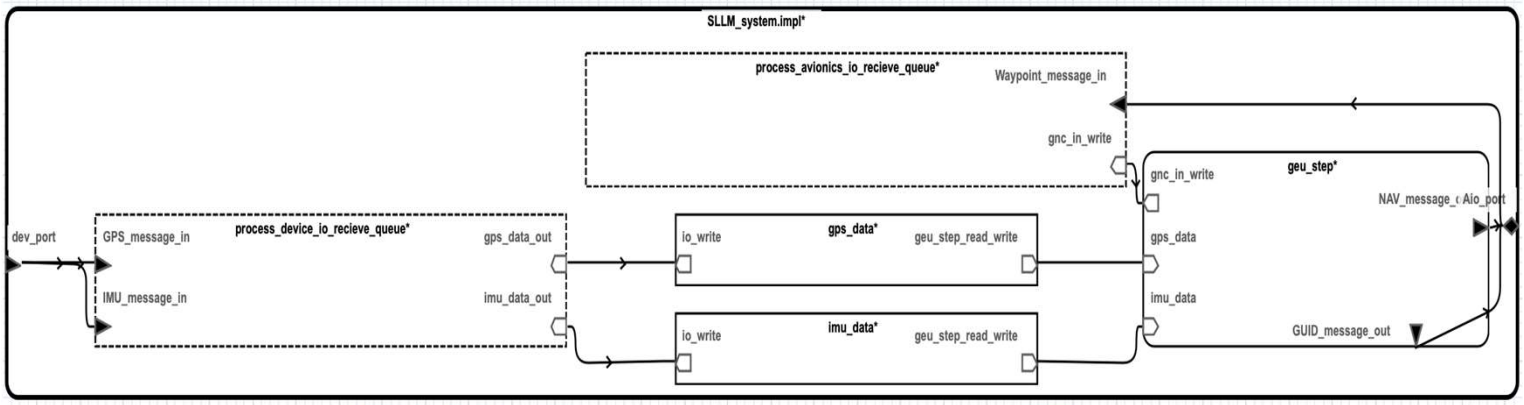
July 17 - 22, 2021

Conclusions

www.incose.org/symp2021

Initial Results from VERDICT/EXP

- Initial model created ~3 weeks (GNC module)
- Identified over 30 requirements
- Immediately able to identify…
  - 243 potential attacks over 13 components covering ~60% of the known attack surface
  - 19 Common Attack Pattern Enumeration and Classifications (CAPECs) from one component



Conclusion

- This paper described using cyber analysis tools on a MBSE AADL model based on a notional industry example, generating more than 30 cyber requirements specific to the system
- Engineering for Cyber Resiliency promises the most success if it is integrated as part of the requirements, design, and development process (i.e., not as a post-integration afterthought)
- Model-Based Systems Engineering as part of the development process can significantly improve cyber resiliency analysis because it includes connection properties and relevant features
- CASE tools such as VERDICT automate cyber resiliency tasks and realize the power of Model-Based Systems Engineering through AADL

31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021