CADA:
CyManII Attack-Defense Annex

Matthew Jablonski
George Mason University
CyManII

Dr. Duminda Wijesekera
George Mason University
CyManII

Dr. Gabriela Ciocarlie
University of Texas at San Antonio
CyManII

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under the Advanced Manufacturing Office Award Number DE-EE0009046

Agenda

- Project goals
- CADA data models and analysis
- Risk scenario: Network attacks and incidence response
- Closing remarks

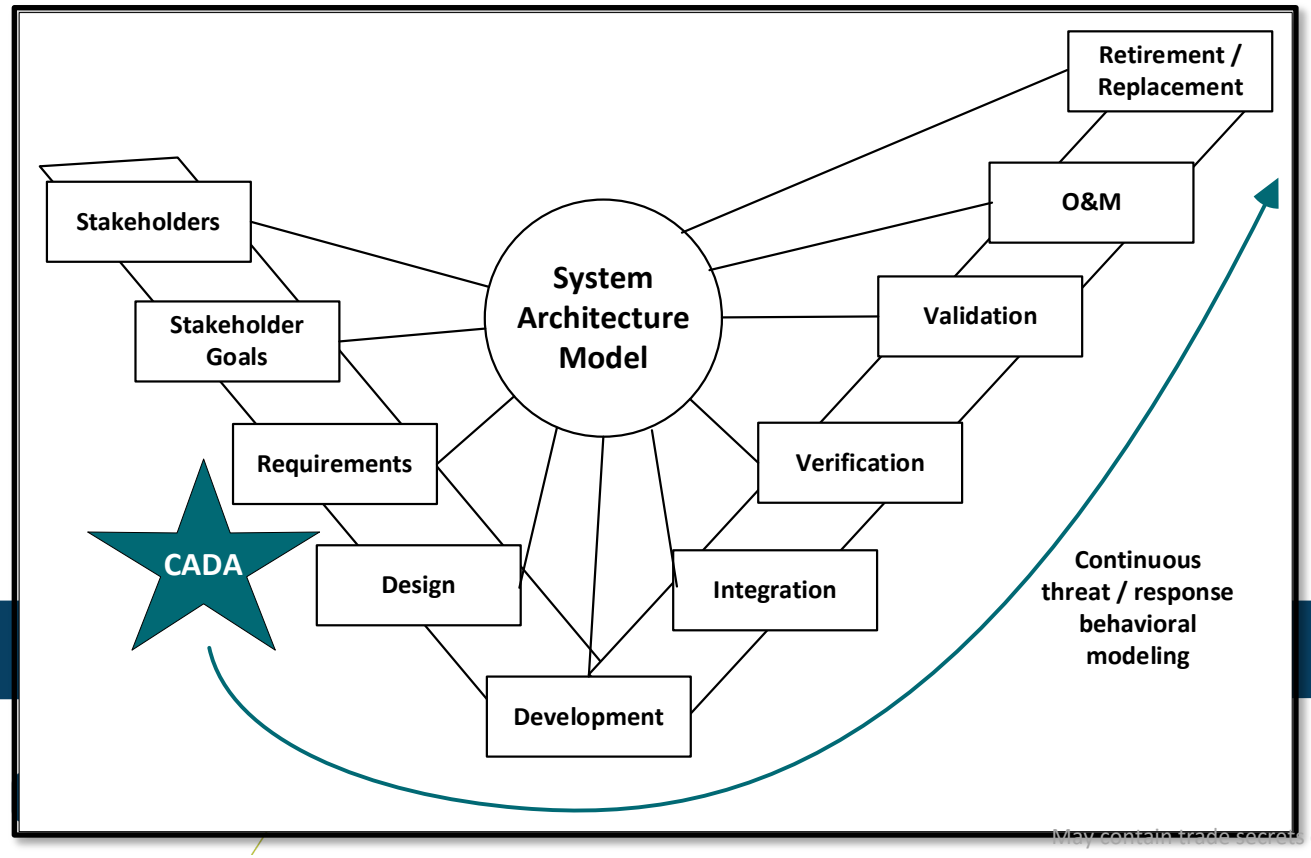
CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

CADA Goals

SN-3	DEVELOP THE SECURITY ASPECTS OF OPERATIONAL AND OTHER LIFE CYCLE CONCEPTS
SN-3.1	Define a representative set of scenarios to identify all required protection capabilities and security measures that correspond to anticipated operational and other life cycle concepts.
SN-3.2	Identify the security-relevant interaction between users and the system.

Stakeholder Needs (SN-3) from [NIST 800-160 Vol. 1]



- **Characterize** security throughout the SDLC
- **Visualize** security risks within system context as it evolves
- **Develop** behavioral models
- **Demonstrate** impacts on control
- **Analyze** behaviors using formal methods
- **Identify** design tradeoff costs
- **Open-Source** CADA

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

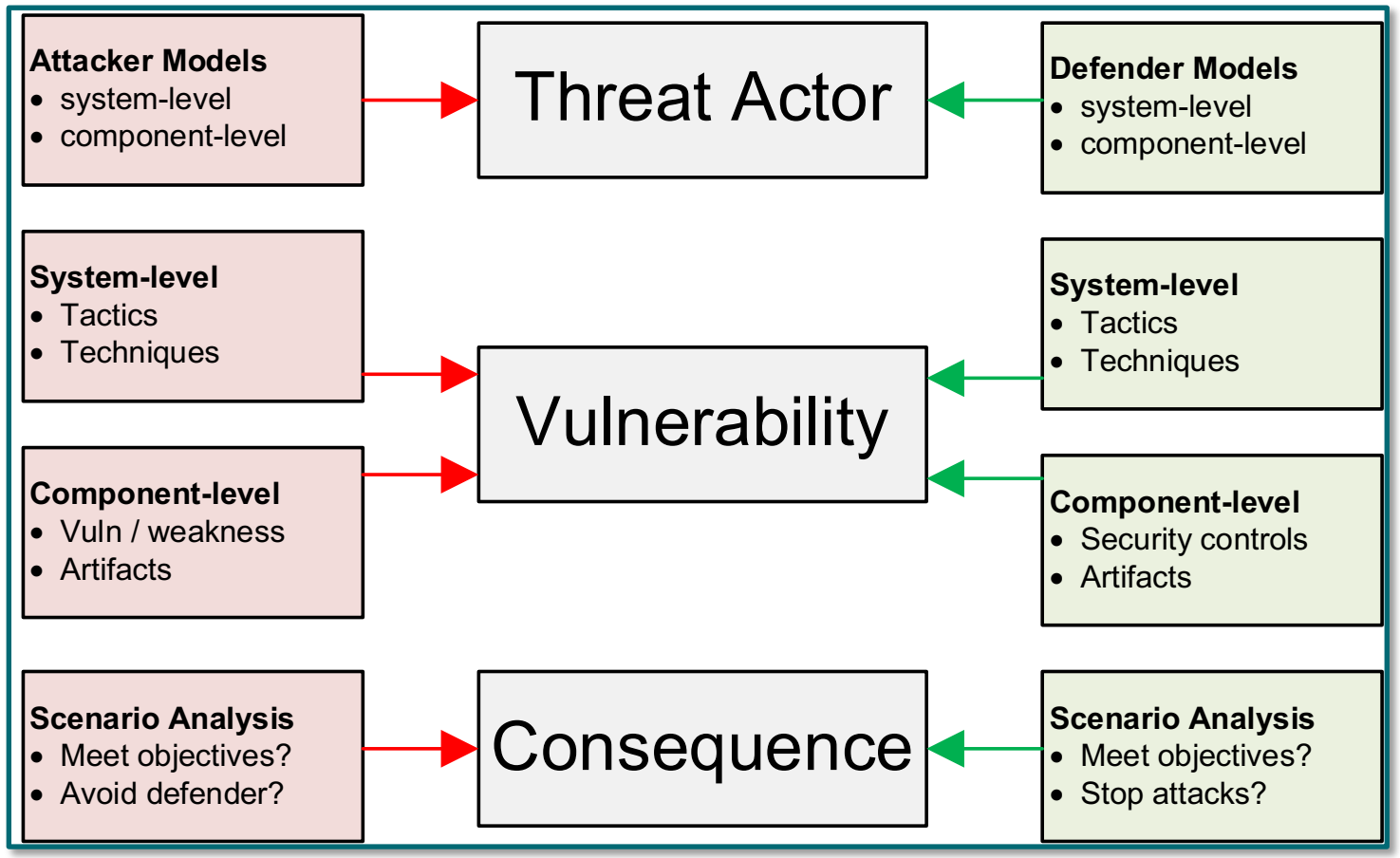
Risk Analysis with CADA

CADA:

- Behavioral data models
- Security risk analysis
- Define realistic attack and response scenarios

Core analytical engines:

- AGREE [AGREE Github]
- Safety Annex [Stewart et. al]



CYMANII

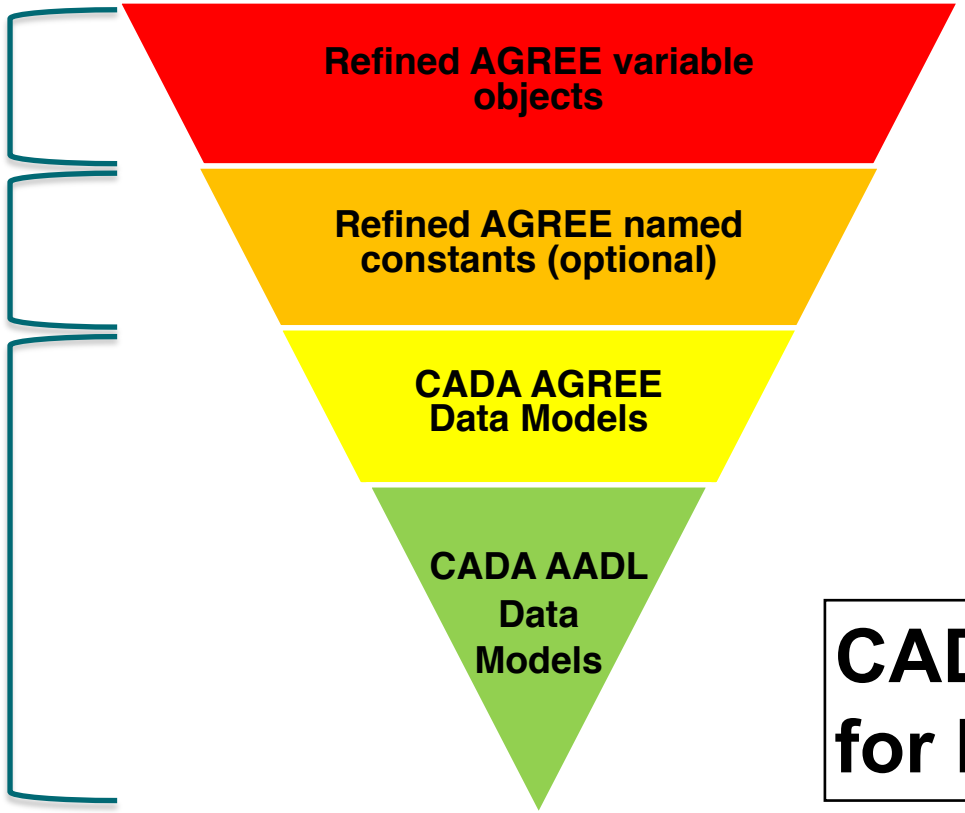
May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

CADA Data Modeling and Analysis In AGREE

Interactions via AGREE statements, CADA nodes, and Safety Annex

Based on system architecture & reqs

Base CADA models



CADA object structure for behavioral analysis

NOTE: we include the above triangle at the top of the next four slides

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

CADA AADL Data Models

Data models for attackers and defenders

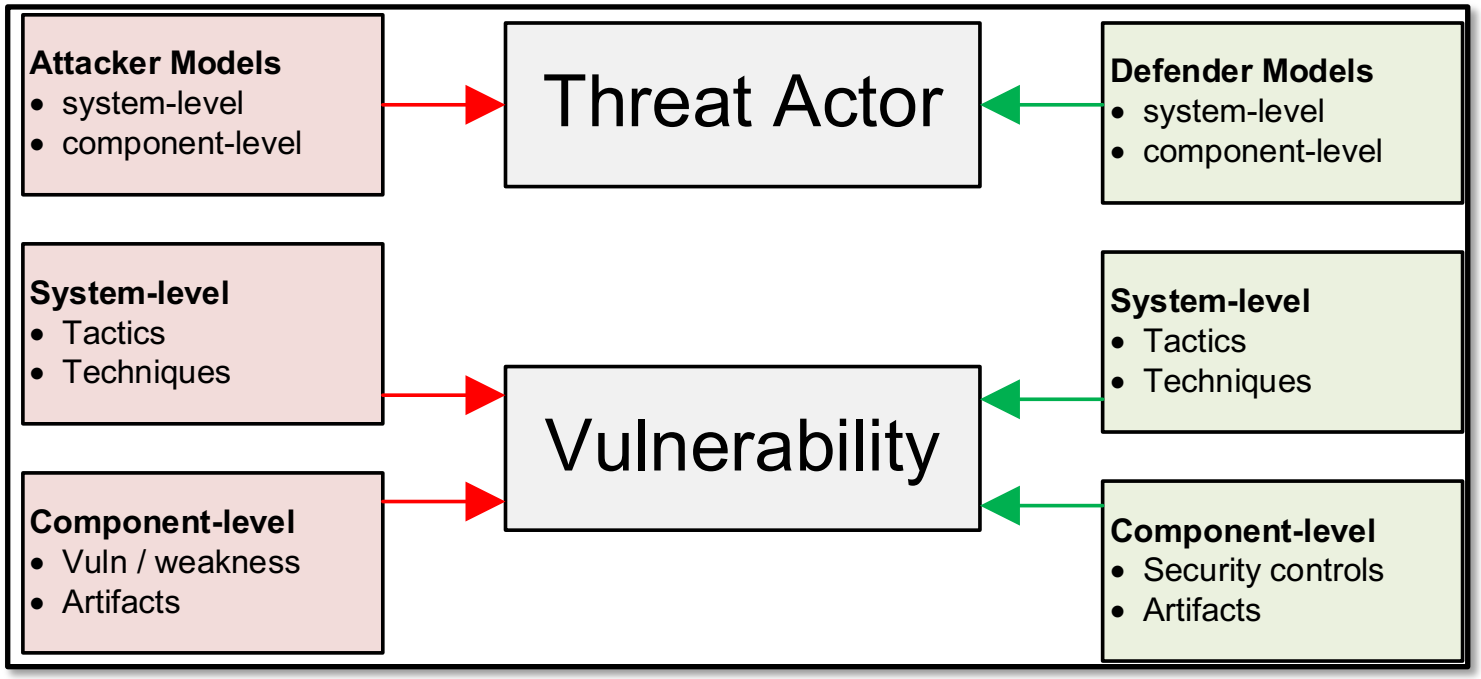
- [Rochetto & Tippenhauer]

Category	Name	A/D	Type	Possible Values
Knowledge	[Off/Def]_Knowledge_Int	AD	Integer	[0-100]
	Physical_[Off/Def]_Knowledge_Int	AD	Integer	[0-100]
	Network_[Off/Def]_Knowledge_Int	AD	Integer	[0-100]
	Software_[Off/Def]_Knowledge_Int	AD	Integer	[0-100]
	Component_Knowledge_Int	AD	Integer	[0-100]
	Protocol_Component_Knowledge_Int	AD	Integer	[0-100]
	Source_Code_Component_Knowledge_Int	AD	Integer	[0-100]
	Credentials_Component_Knowledge_Enum	AD	enum	none, user, administrator, SYSTEM_access, remote_desktop_users, root, any
Resource	Distance_Resource_Enum	AD	enum	none, far, near, physicalaccess, any
	Manpower_Resource_Enum	AD	enum	low, medium, high
	[Off/Def]_Tools_Resource_Enum	AD	enum	basic, intermediate, advanced
	Financial_Resource_Int	AD	Integer	[0-1000000]
	Effort_Resource_Enum	AD	enum	low, medium, high
Psychology	Off_Aim_Psych_Enum	A	enum	knowledge, manipulation, disrupt, damage
	Def_Aim_Psych_Enum	D	enum	none, confidentiality, integrity, availability, all
	[Off/Def]_Physical_Sec_Aim_Psych_Enum	AD	enum	none, confidentiality, integrity, availability, all
	[Off/Def]_Virtual_Sec_Aim_Psych_Enum	AD	enum	none, confidentiality, integrity, availability, all
	Periodicity_Psych_Enum	AD	enum	once, anytime, continuous
	Determination_Psych_Enum	AD	enum	first_attempt, several_attempts, untiring
	Honesty_Psych_Enum	A	enum	malicious, benign
	Camouflage_Psych_Enum	AD	enum	visible, stealthy, invisible
	Off_Strategy_Psych_Enum	AD	enum	random, brute_force, structured
	Def_Strategy_Psych_Enum	D	enum	random, monitor, investigate, evict

CYMANII

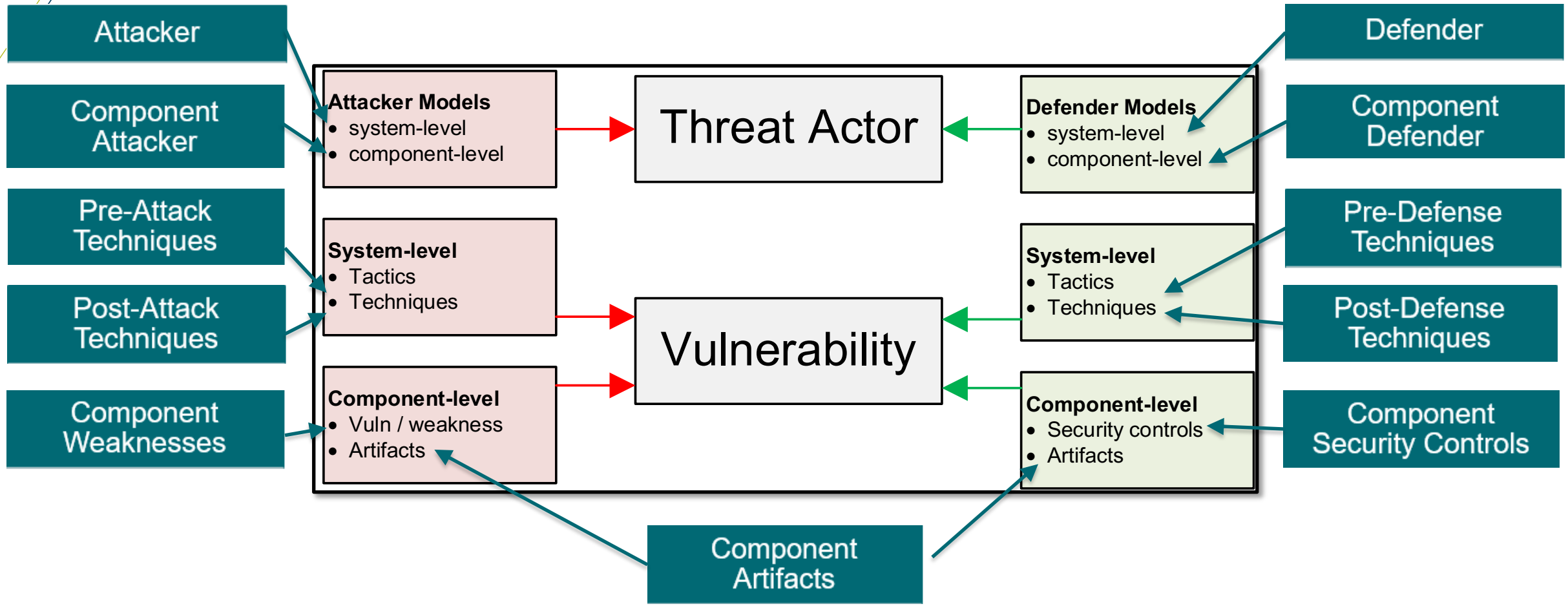
May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

CADA AGREE Data Models



May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

CADA AGREE Data Models



CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Refined AGREE Named Constants

- **Optionally refine** the CADA AGREE Data Models using named constants with **actual values**
  - Standards
  - Models
  - Domain experts
  - Best practice
  - etc.
- Refinements **specific to the system or organization**

Attacker

- Nation State
- Insider Threat
- Penetration Tester

Defender

- Incidence Response Team
- Security Engineering
- Physical Security

Attack Techniques

- [MITRE ATT&CK®]
- [MITRE CAPEC]

Defense Techniques

- [MITRE D3FEND™]

Component Weaknesses

- [MITRE CVE®]
- [MITRE CWE™]

Component Security Controls

- [NIST 800-53 Rev. 5]

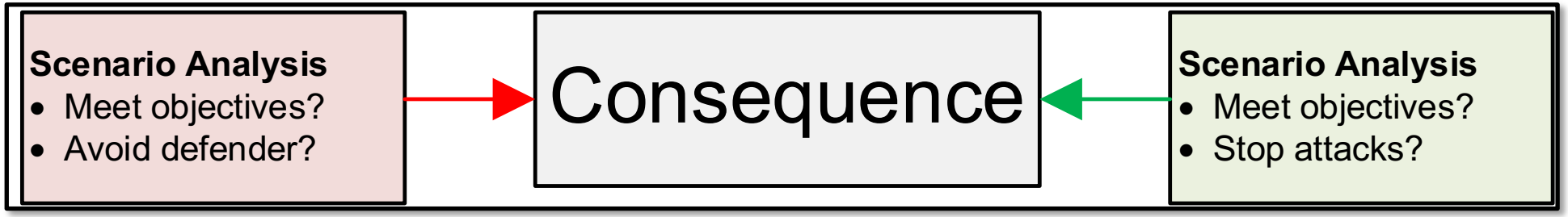
Component Artifacts

- MITRE D3FEND™ Digital Artifact Ontology [MITRE D3FEND]

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

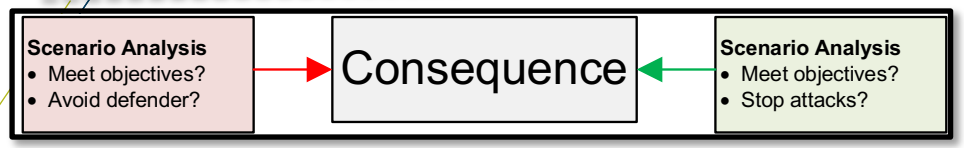
Refined AGREE Variable Objects



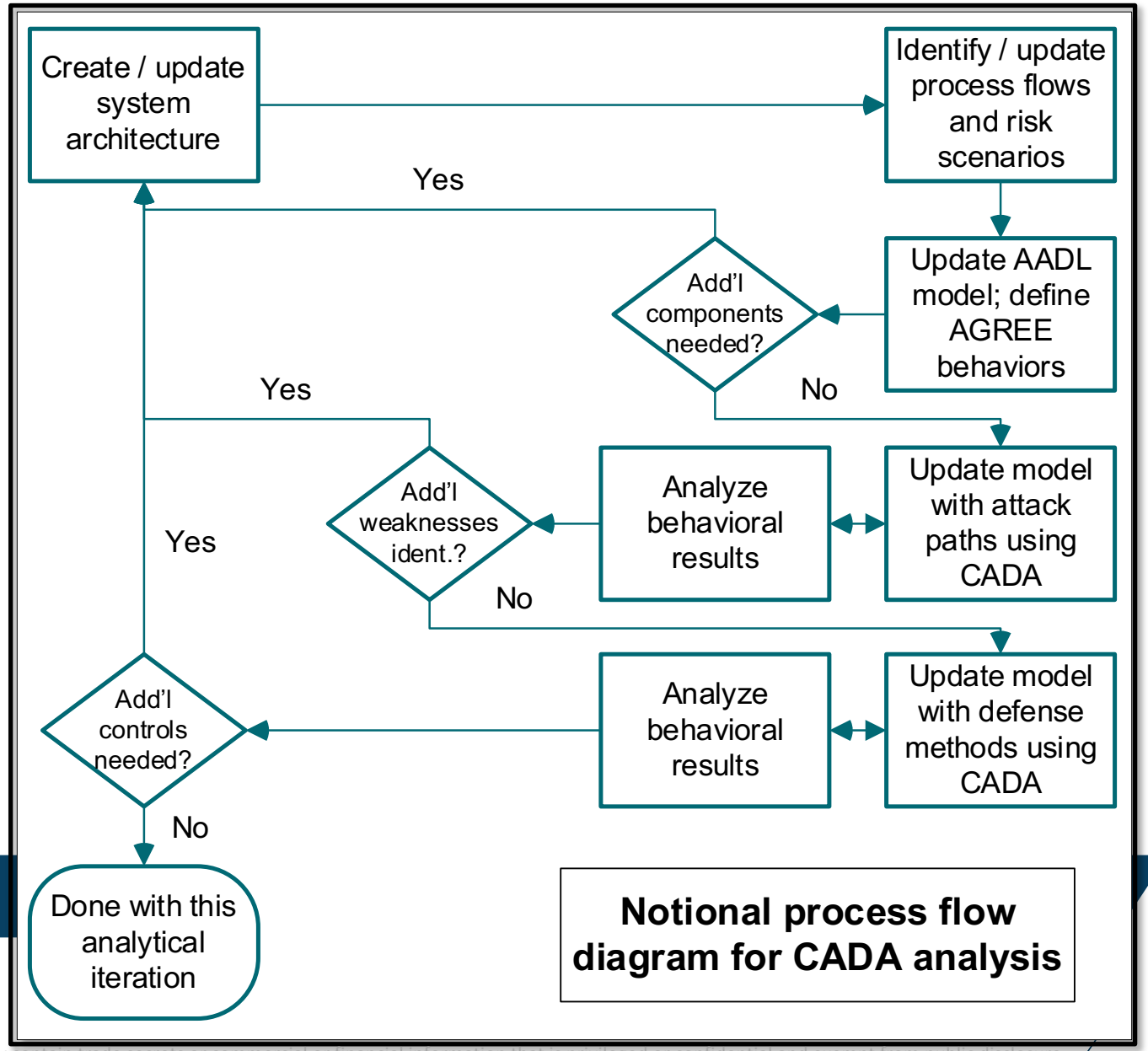
- **Analysis** should match perceived and actual real-world conditions
  - **AGREE** and **Safety Annex**
  - **CADA Nodes**
  - **Domain expertise**
  - **Notional process flow**

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Refined AGREE Variable Objects



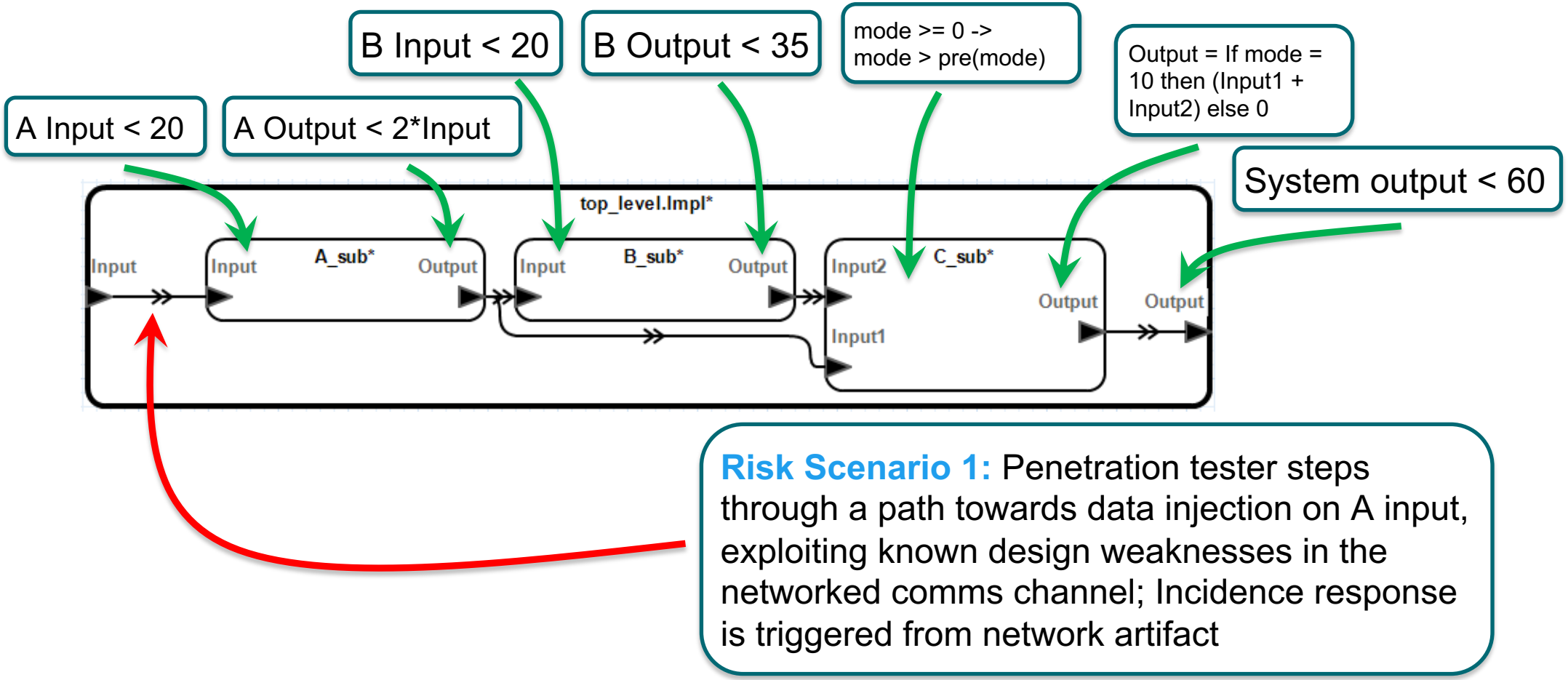
- **Analysis** should match perceived and actual real-world conditions
  - **AGREE** and **Safety Annex**
  - **CADA Nodes**
  - **Domain expertise**
  - **Notional process flow**



CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Toy Model Example System Risk Scenario 1



Risk Scenario 1: Penetration tester steps through a path towards data injection on A input, exploiting known design weaknesses in the networked comms channel; Incidence response is triggered from network artifact

NOTE: enhanced from AGREE and Safety Annex toy models for CADA example

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Risk Scenario 1 – Network Attack on System Input

Top-level AGREE Annex:

```
annex agree {**

    eq mode : int;
    assume "System input range " : if A_CWE_77_fail then Input = 100 else Input < 10;
    guarantee "mode is always positive" : mode >= 0;
    guarantee "System output range" : Output < 60;

    --------------
    --Attacker
    --------------
    eq attacker : Attack_AGREE_Models::AD001_ATTACKER = Attacker_AGREE_Types::A003_PENETRATION_TESTER;
    --------------
    --Attacks on A
    --------------
    eq attacker_A : Attack_AGREE_Models::AD001_ATTACKER = (attacker ->
        if A_CWE_200_ud = 1 then
            CADA_Nodes::Adapt_Attacker_From_Weakness(
                prev(attacker_A, attacker),
                Weakness_AGREE_Types::CWE200_EXPOSURE_OF_SENS_INFO
            )
        else if A_CWE_77_ud = 1 then
            CADA_Nodes::Adapt_Attacker_From_Weakness(
                prev(attacker_A, attacker),
                Weakness_AGREE_Types::CWE77_COMMAND_INJECTION
            )
        else prev(attacker_A, attacker)
    );
```

4

1

2

3

Attack Results

Property	Result
Verification for top_level.Impl	4 Invalid, 9 Valid
Contract Guarantees	4 Invalid, 4 Valid
A_sub assume: A input range	Invalid (1s)
B_sub assume: B input range	Invalid (1s)
Subcomponent Assumptions	Invalid (1s)
mode is always positive	Valid (3s)
System output range	Invalid (1s)
eq attacker : AD001_ATTACKER	Valid (1s)

	A	B	C	D	E
1	**Step**	0	1	2	3
2					
3	**A_sub**				
4	A_sub..ASSUME.HIST	TRUE	TRUE	TRUE	FALSE
5	A_sub.CWE_77_Present	TRUE	TRUE	TRUE	TRUE
6	A_sub.CWE_200_Present	TRUE	TRUE	TRUE	TRUE
7	A_sub.Input	0	0	0	100
8	A_sub.Output	-1	-1	-1	200
9					
10	**B_sub**				
11	B_sub..ASSUME.HIST	TRUE	TRUE	TRUE	FALSE
12	B_sub.Input	-1	-1	-1	200
13	B_sub.Output	0	0	0	35
14					
15	**C_sub**				
16	C_sub..ASSUME.HIST	TRUE	TRUE	TRUE	TRUE
17	C_sub.Input1	-1	-1	-1	200
18	C_sub.Input2	0	0	0	35
19	C_sub.Output	0	0	0	235
20	C_sub.mode	0	8	9	10
21					
22					
23	A_CWE_77	FALSE	FALSE	TRUE	TRUE
24	A_CWE_77_Present	TRUE	TRUE	TRUE	TRUE
25	A_CWE_77_fail	FALSE	FALSE	FALSE	TRUE
26	A_CWE_77_ud	0	0	1	2
27	A_CWE_77_ud_sp	TRUE	FALSE	TRUE	TRUE
28	A_CWE_200	FALSE	TRUE	TRUE	TRUE
29	A_CWE_200_Present	TRUE	TRUE	TRUE	TRUE
30	A_CWE_200_ud	0	1	2	3
31	A_CWE_200_ud_sp	TRUE	TRUE	FALSE	TRUE
32	A_sub assume: A input range	TRUE	TRUE	TRUE	FALSE
33	B_sub assume: B input range	TRUE	TRUE	TRUE	FALSE
34	Input	0	0	0	100
35	Output	0	0	0	235

Response analysis:
Exploit CWE-200 ->
Exploit CWE-77 -> A's input changes which cascades through to system output to complete attack path

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Risk Scenario 1 – Defensive Response 1

Top-level AGREE Annex:

```
--------------
--Defender
--------------

eq defender : Defend_AGREE_Models::DD001_DEFENDER = Defender_AGREE_Types::D001_INCIDENCE_RESPONSE_TEAM;

--------------
--Defense of A
--------------

--A Defender
eq defender_A : Defend_AGREE_Models::DD001_DEFENDER = defender ->
    if (A_D3_CAA and A_D3_CAA_ud = 1) then
        CADA_Nodes::Adapt_Defender_From_Technique(
            prev(defender_A, defender),
            Defend_Technique_AGREE_Types::D3_CAA_CONN_ATTEMPT_ANALYSIS_POST
        )
    else if (A_D3_ITF and A_D3_ITF_ud = 1) then
        CADA_Nodes::Adapt_Defender_From_Technique(
            prev(defender_A, defender),
            Defend_Technique_AGREE_Types::D3_ITF_IN_TRAFFIC_FILTER_POST
        )
    else if (A_D3_BDI and A_D3_BDI_ud = 1) then
        CADA_Nodes::Adapt_Defender_From_Technique(
            prev(defender_A, defender),
            Defend_Technique_AGREE_Types::D3_BDI_BROADCAST_DOM_ISO_POST
        )
    else prev(defender_A, defender);
```

1

2

3

4

Defense Results

Property	Result
Contract Guarantees	5 Invalid, 10 Valid
A_sub assume: A input range	Invalid (1s)
B_sub assume: B input range	Invalid (1s)
Subcomponent Assumptions	Invalid (1s)
mode is always positive	Valid (20s)
System output range	Invalid (1s)
System A response has not occurred	Invalid (2s)
System A defense not monitoring	Valid (2s)

Response analysis:

- Attack was still successful before defender could respond to bypassed network security controls
- Failure for “System A response has not occurred” check means that the defender did respond to attacker’s events
- Success for “System A defense not monitoring” check means that the defender was always monitoring the system

Question: How can we prevent this traffic injection attack from occurring in the first place?

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Risk Scenario 1 – Defensive Response 2

System A AGREE Annex:

```
--------------
--Defender
--------------

eq defender : Defend_AGREE_Models::DD001_DEFENDER = Defender_AGREE_Types::D002_SECURITY_ENGINEERING;

--------------
--Defense of A
--------------

--A Defender
eq defender_A : Defend_AGREE_Models::DD001_DEFENDER = defender ->
    if (A_D3_MAN and A_D3_MAN_ud = 1) then
        CADA_Nodes::Adapt_Defender_From_Technique(
            prev(defender_A, defender),
            Defend_Technique_AGREE_Types::D3_MAN_MESSAGE_AUTH_POST
        )
    else prev(defender_A, defender);
```

1

2

Defense Results

Property	Result
✔ Contract Guarantees	16 Valid
✔ A_sub assume: A input range	Valid (46s)
✔ B_sub assume: B input range	Valid (46s)
✔ Subcomponent Assumptions	Valid (46s)
✔ mode is always positive	Valid (44s)
✔ System output range	Valid (46s)
✔ System A response has not occurred	Valid (47s)
✔ System A defense not monitoring	Valid (2s)

Response analysis:

- Traffic injection attack fails when Input data is signed and authenticated ☺
- Defender was monitoring throughout the scenario for signs of attack

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

Contributions

- **Introduced CyManII Attack-Defense Annex (CADA)**
  - Provides attack-defense data model
  - Pentest and mitigate attacks early in SDLC
  - Offers risk scenarios that span SDLC and evolve with system
- **CADA's generality**
  - Based on testing, CADA is extendable to all system models that leverage AGREE / Safety Annex
  - Similar data models may be derived to support other modeling languages
  - Intent to open source
- **Email Contact**: FIRST <dot> LAST <at> cymanii <dot> org

CYMANII

May contain trade secrets or commercial or financial information that is privileged or confidential and exempt from public disclosure.

References

- **[AADL Overview]** Peter Feiler, *SAE AADL V2: An Overview*, Software Engineering Institute, 2010. https://cs.gmu.edu/~rpettit/files/lectures/AADLV2Overview-AADLUserDay-Feb_2010.pdf
- **[AGREE Github]** Loonwerks AGREE Repository, 2021. https://github.com/loonwerks/AGREE
- **[Delange]** Julien Delange, *AADL In Practice*, Reblochan Development Company, 2017. (book) [Rochetto & Tippenhauer] Rochetto and Tippenhauer, "On attacker models and profiles for cyber-physical systems," ESORICS 2016, Springer International Publishing, Switzerland.
- **[Feiler & Gluch]** Peter H. Feiler and David P. Gluch, *Model-Based Engineering with AADL*, Addison-Wesley, 2012. (book)
- **[Meng]** Baoluo Meng et al., *VERDICT: A Language and Framework for Engineering Cyber Resilient and Safe System*, in Systems, Vol.9 (1), p.18.
- **[MITRE ATT&CK]** MITRE, MITRE ATT&CK®, 2022. https://attack.mitre.org
- **[MITRE CVE]** MITRE, CVE® Program, 2022. https://cve.org
- **[MITRE CWE]** MITRE, Common Weakness Enumeration, 2022. https://cwe.mitre.org
- **[MITRE D3FEND]** Peter E. Kaloroumakis and Michael J. Smith, Toward a Knowledge Graphy of Cybersecurity Countermeasures, MITRE, Case 20-2034, 2021. https://d3fend.mitre.org/resources/D3FEND.pdf
- **[NIST 800-53 Rev. 5]**
- **[NIST 800-160 Vol. 1]** Ron Ross, Michael McEvilley, and Janet Carrier Oren, *Systems Security Engineering*, National Institute of Standards and Technology, NIST Special Publication 800-160 Volume 1, 2018.
- **[OSATE]** Welcome to OSATE, 2021. https://osate.org/
- **[Stewart et. al]** Danielle Stewart et. al, *Safety Annex for the Architecture Analysis and Design Language*, In ERTS 2020, 10th European Conference Embedded Real Time System.