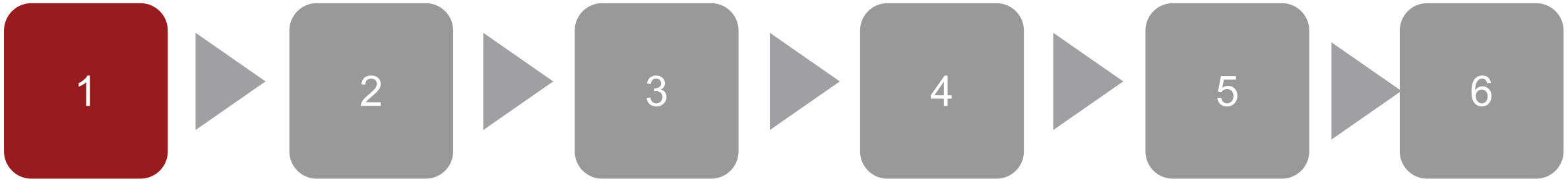
29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

Use of SysML for the Creation of FMEAs for Reliability, Safety, and Cybersecurity for Critical Infrastructure



introduction

Metamodel

Procedure

Example

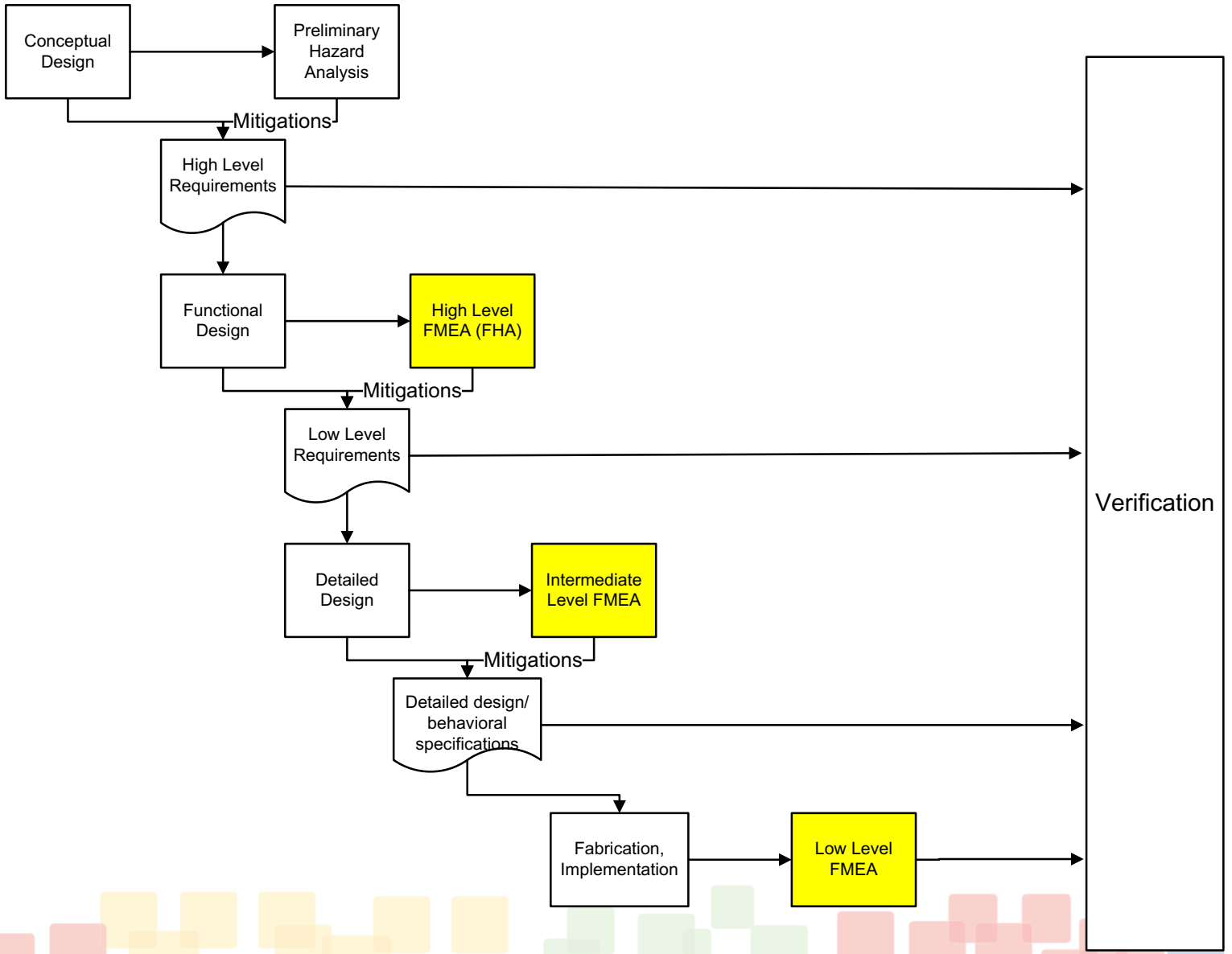
Outputs

Discussion and Conclusions

Failure Modes and Effects Analysis (FMEAs)

- Most important and labor intensive analysis for reliability and safety assurance
- Defined and required in multiple domains
  - Defense (MIL STD 1629A and MIL STD 882E)
  - Avionics (SAE ARP 4754, ARP 4761, and AARP 5580)
  - Automotive (SAE J1739)
  - Medical Devices (ISO 14971 risk management, ISO 60812 FMEA, FDA Guidance for Industry, Q9 Quality Risk Management)
  - Nuclear Power Reactors, Space Systems, Industrial Process Control, many others….

Ideal Use of FMEAs



Challenges in Reaching the Ideal

- FMEAs are Labor Intensive (Expensive)
  - Cost Schedule Impact
  - impact
- FMEAs require domain and technical expertise
  - Resources may be scarce during development
- Consequences
  - Immediate Consequence: Done once and late in the development process
  - Secondary consequence: marginal impact on the design
    - Primary motivation becomes regulatory or contractual compliance, not design

Conventional FMEA and its drawbacks

Traditional FMEA Example

Service Component	Failure Mode	Effect on Component	Next Level Effect	End Effect	Detection	Mitigation	Severity	Recommendations
BEM	Incorrect Result	BEM cannot send or receive data from JMS Database;	BEM may not be able to function correctly possibly effecting CAM, APS, CFM, and other services	User cannot get breakup data or retrieve data for breakup related messages	Errors are captured in breakup event processing log; JMS resources to detect; Errors are returned for	Failover for 2nd DB VM	5 - minor effect	Develop Infrastructure application to check logs and report failures to operator

There could be a lot happening between the next level and end effect that's not captured

On which propagation path and at what point do detection and mitigation occur ?

On which propagation path and at what point do detection and mitigation occur ?

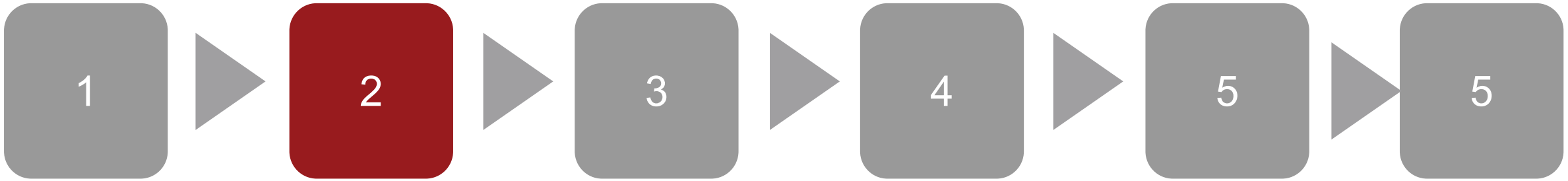
Solution: Automated SysML-based FMEA method

Components of the solution

- FMEA profile
- Model annotated with properties defined by FMEA profile
- SysML modeling tool (Cameo Systems Modeler)
- Plug-in (Java program) using Cameo System Modeler APIs to traverse annotated SysML Model, collect data, and generate output file
- Microsoft Excel Output File (consisting of 6 worksheets)

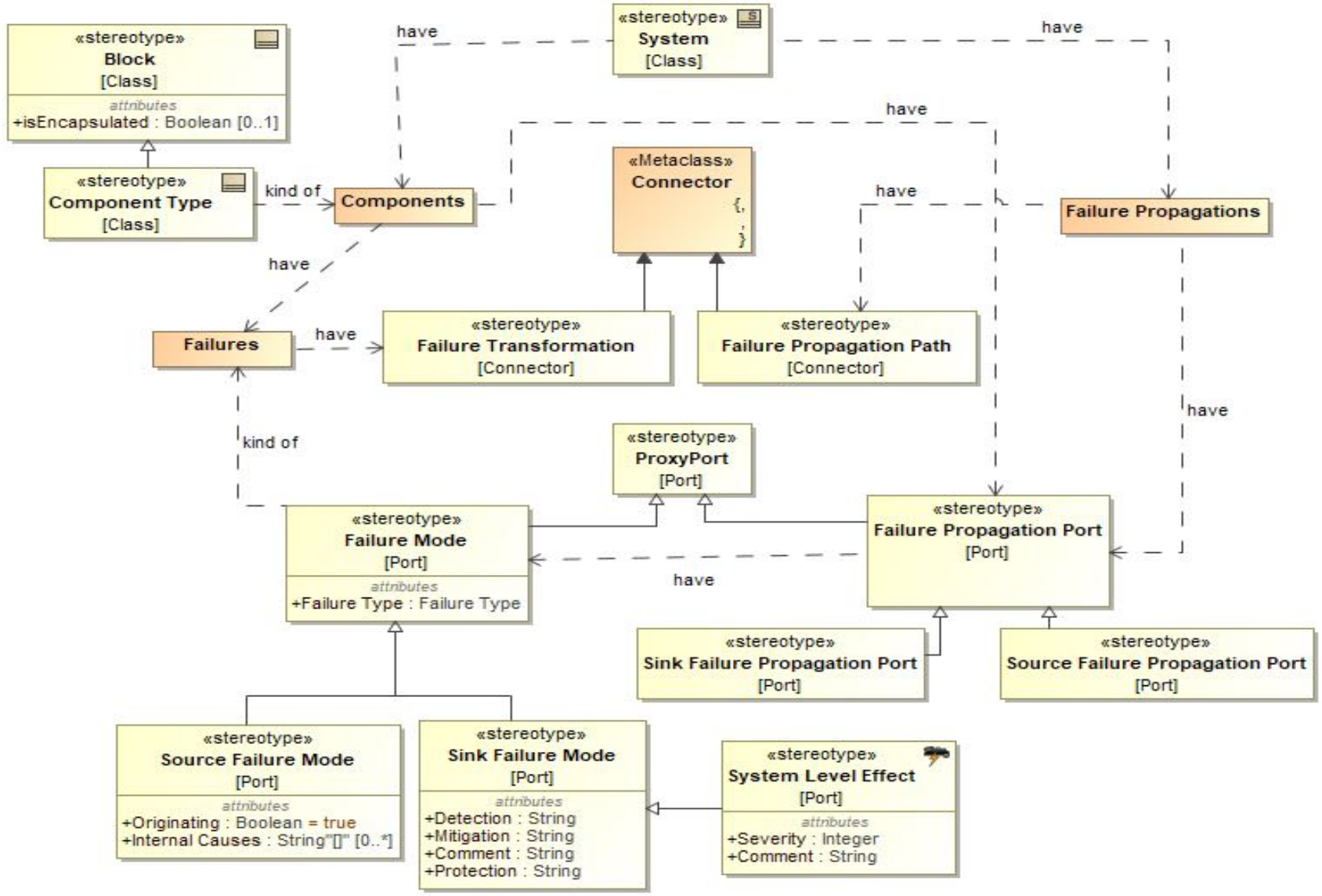
Advantages of the automated FMEA method

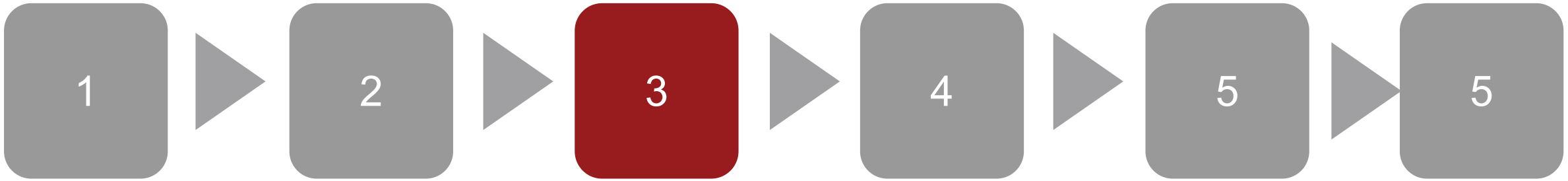
- Complete coverage: considers all propagation paths in detail
- More analytical information
  - Length of each propagation path
  - Earliest detection and mitigation
  - Components subject to the most propagating failures
  - Symptoms most likely to cause a specific failure mode
  - Complete listing of each propagation path
- Integrate cybersecurity analyses
  - Failure propagation and attack propagation paths can be integrated in a single model
  - Attack propagations, detections, and mitigations can be included in an integrated analysis or separated for a discipline unique artifact
- Reduce labor
  - Only component and propagation-to-nearest-neighbor parameters need to be defined; not the entire FMEA “row”; the algorithm integrates them
  - Facilitates reusable components and propagation paths
  - Automated – FMEA generated in seconds
- Integration into the development process
  - The primary value of the FMEA is during the design process; automation enables many iterations and considerations of alternatives most FMEAs are done when the design is complete because of the expense of a manual process



introduction Metamodel Procedure Example Outputs Discussion and Conclusions

Metamodel and Profile

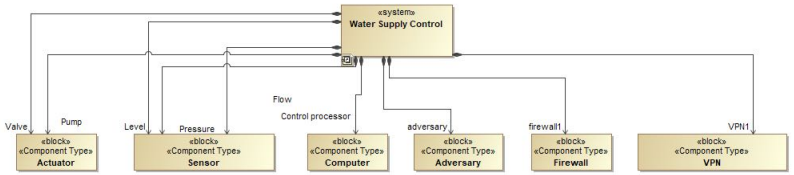




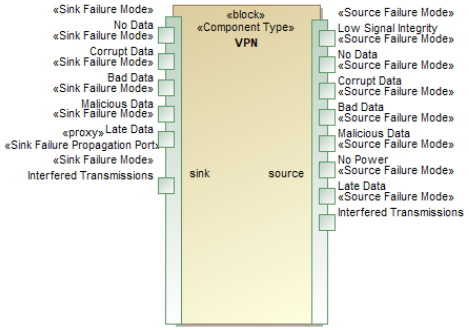
introduction Metamodel Procedure Example Outputs Discussion and Conclusions

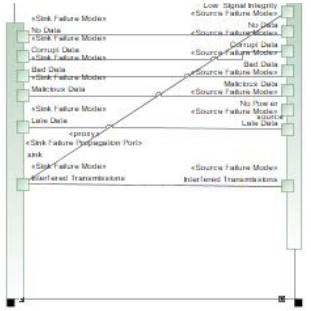
Automated FMEA Generation Procedure

- Define failure propagations and transformations in SysML
- System described using standard SysML constructs
- Once system is modeled, output is automatically produced

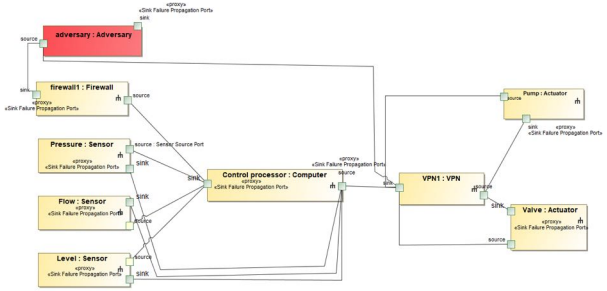


1. Defining the System with a Block Definition Diagram

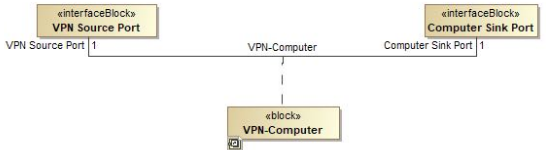


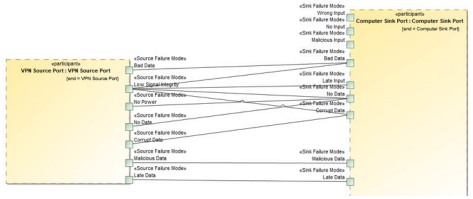


2. Defining the failure propagations and transformations within a component

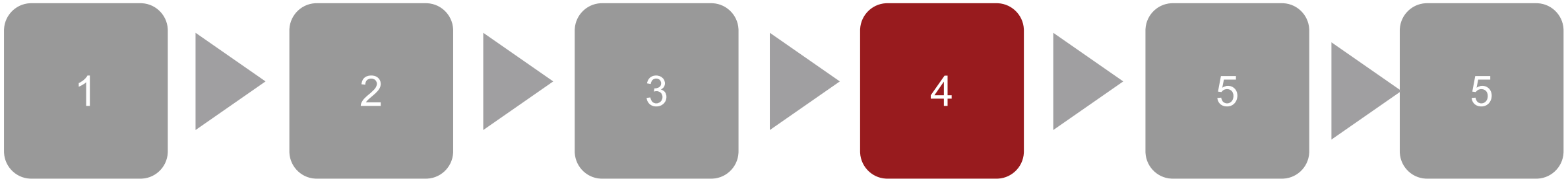


3. Defining the propagation paths with a System Internal Block Diagram



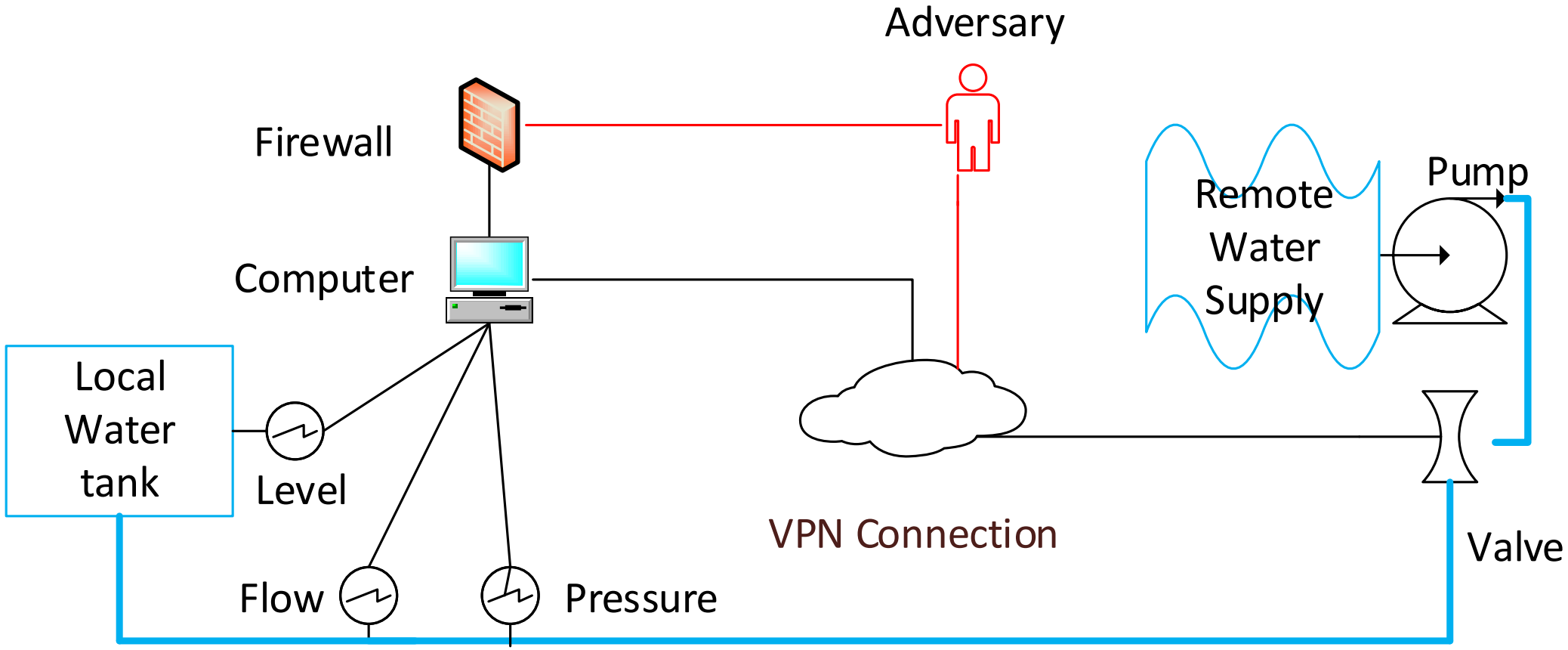


4. Defining Inter-component propagations and transformations

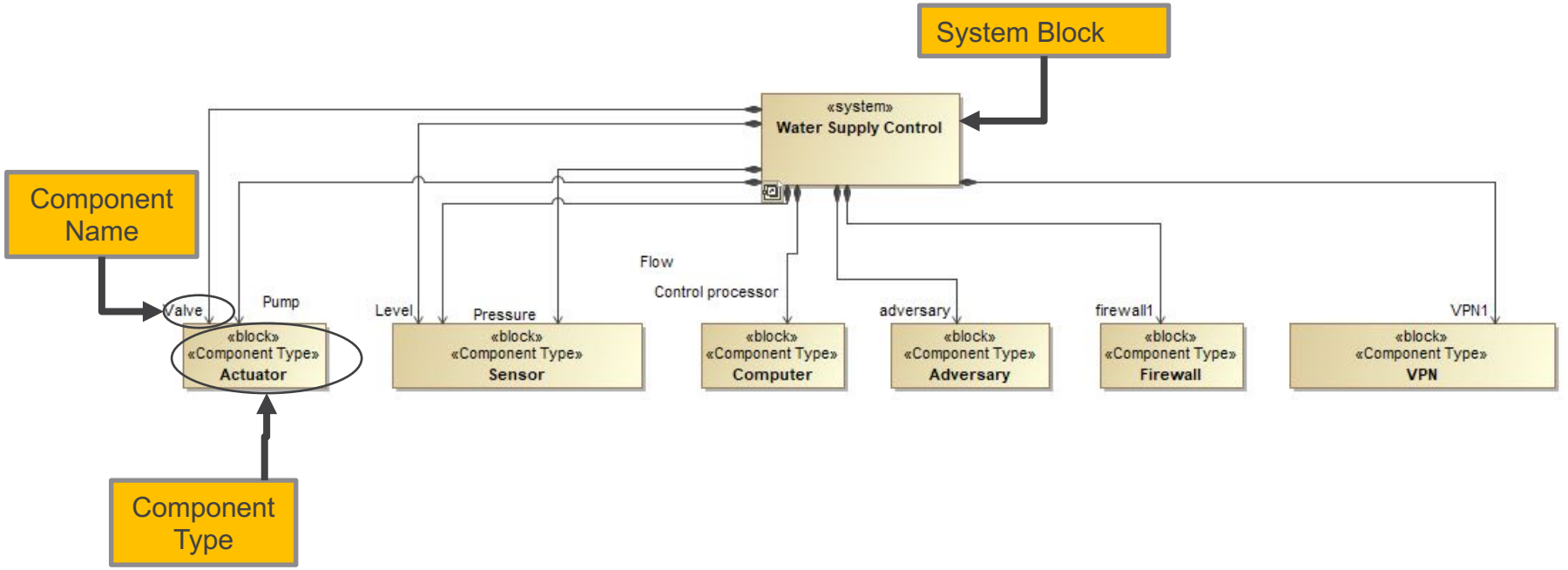


introduction Metamodel Procedure Example Outputs Discussion and Conclusions

Water Supply System Example

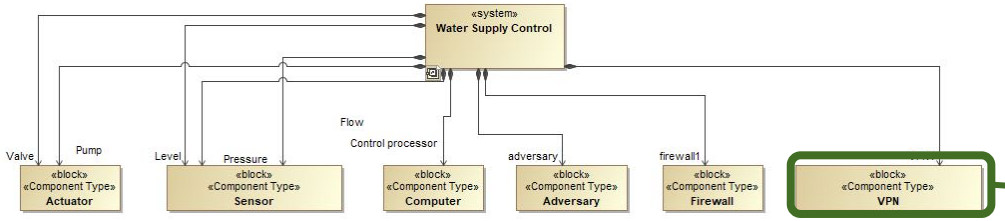


1.Defining the system components to be included in the analysis using a SysML Block Definition diagram

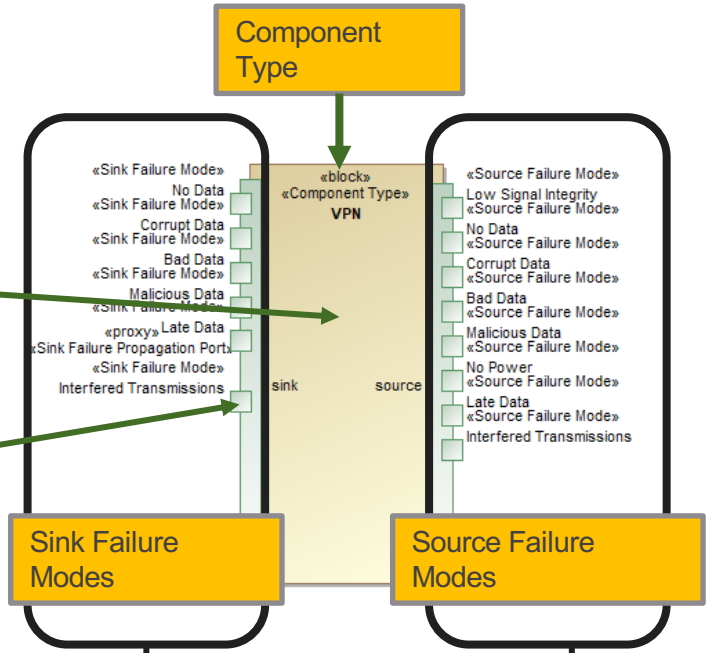


- System represented by top-level block
- Component types connected to subsystem through the directed composition relationship
- Components are instantiated from component types

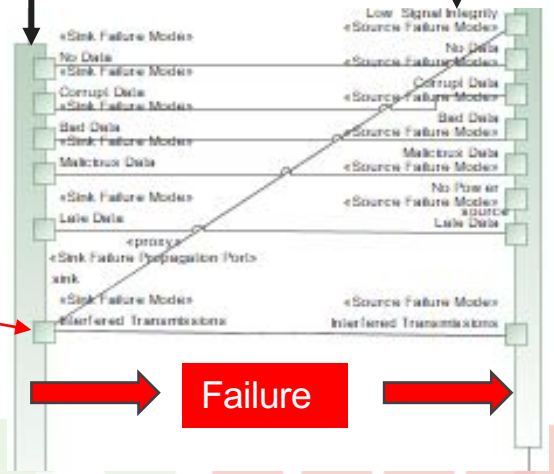
2. Defining the failure propagations and transformations within a component



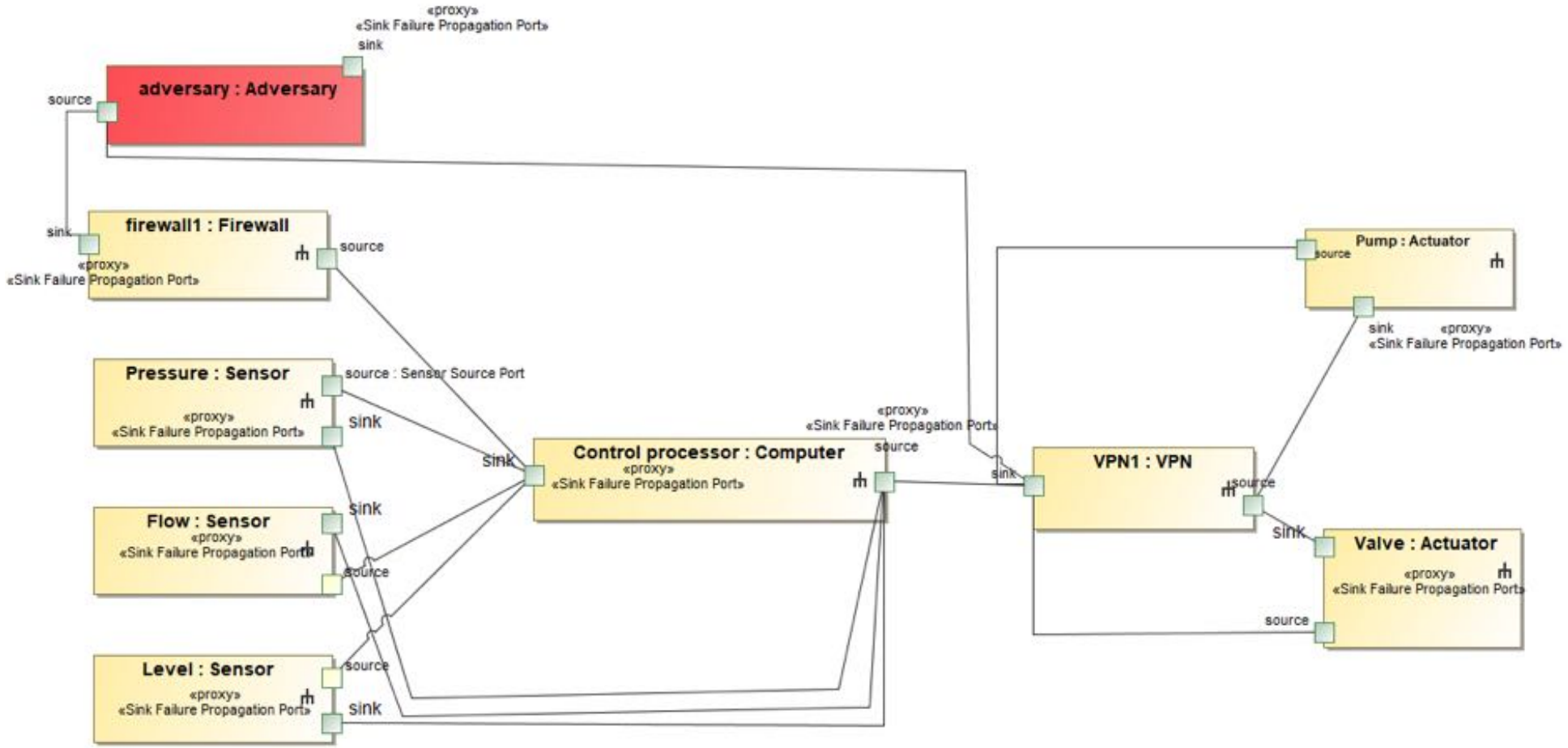
- Component types represented as blocks
- Failure modes represented as ports



- Internal failure propagations shown in component type IBD
- Single sink failure mode can transform into different source failure modes



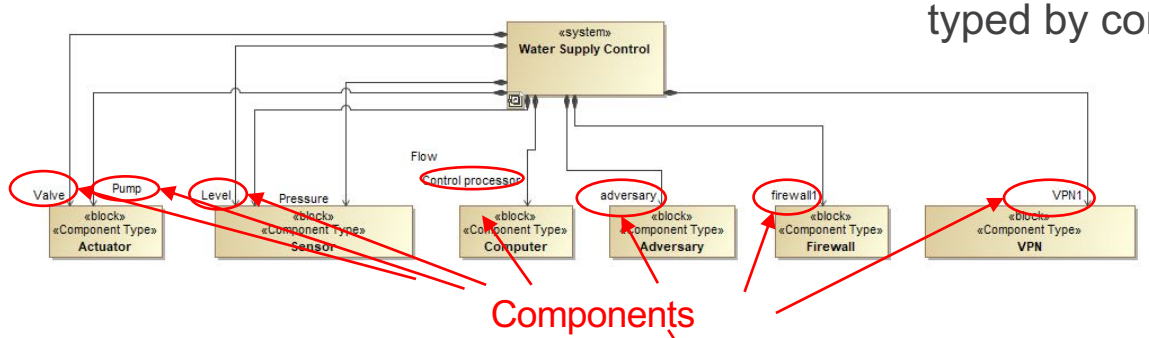
3. Defining the propagation paths with a System Internal Block Diagram



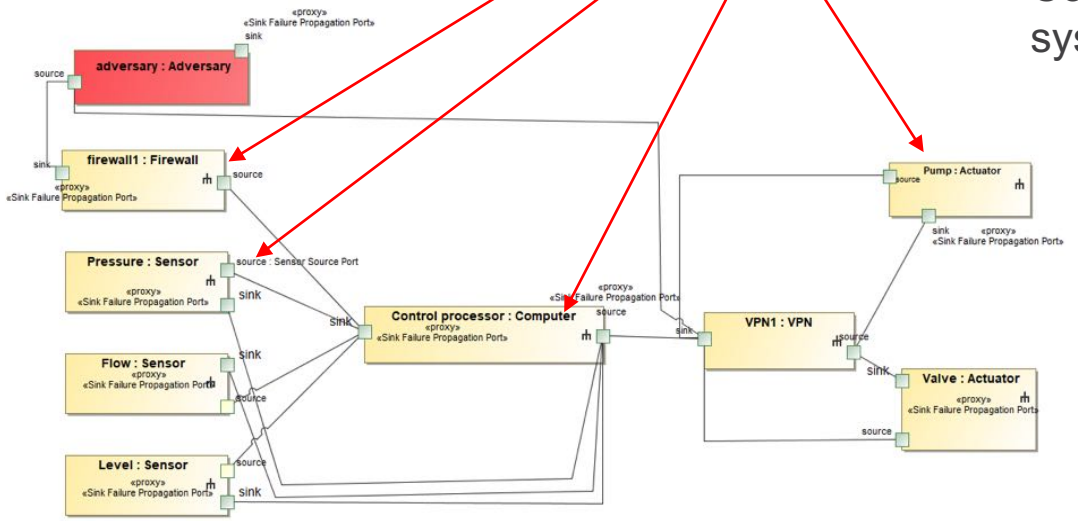
3. Defining the propagation paths with a System Internal Block Diagram

Development from BDD

Components defined as part properties typed by component type blocks

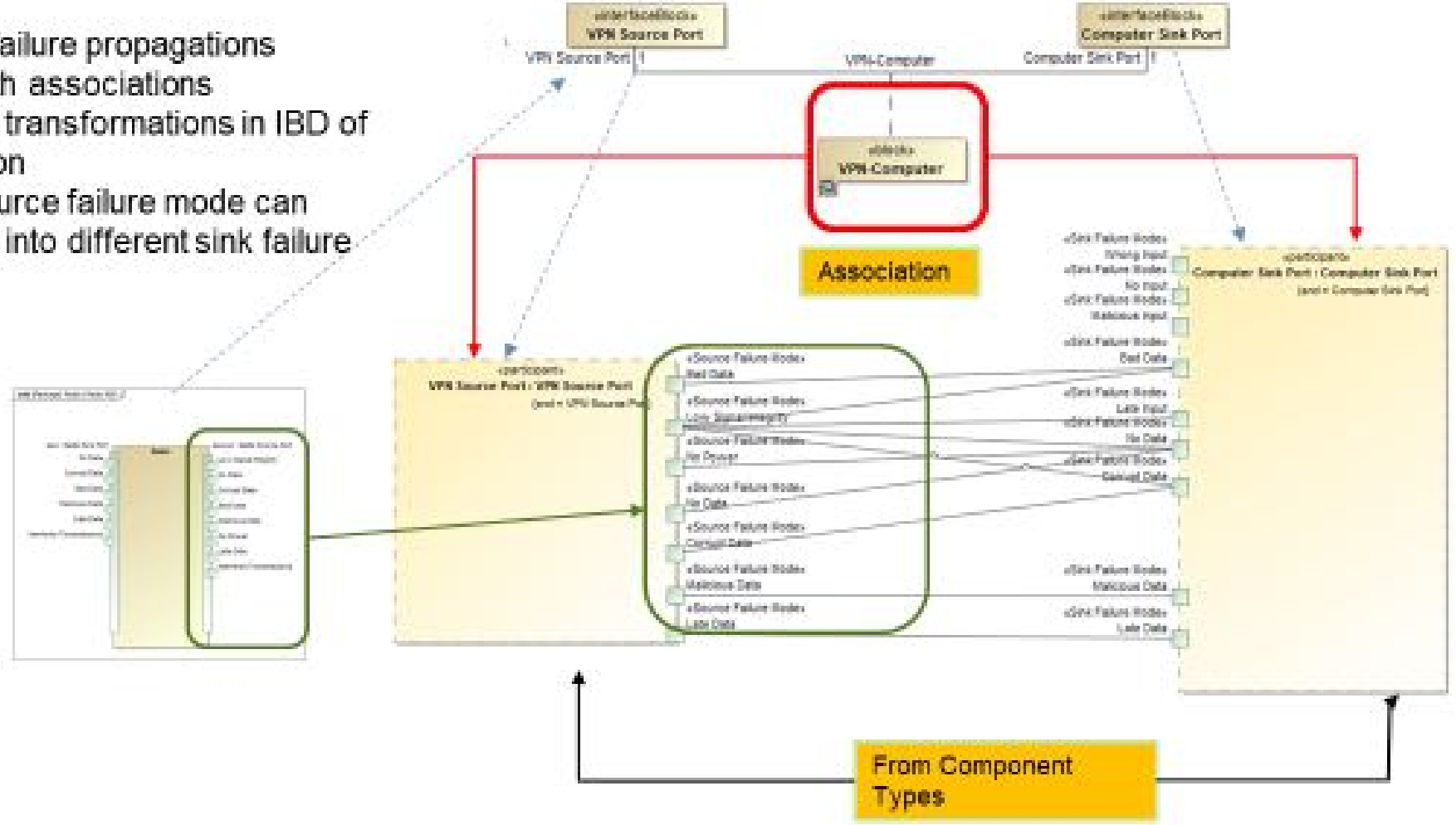


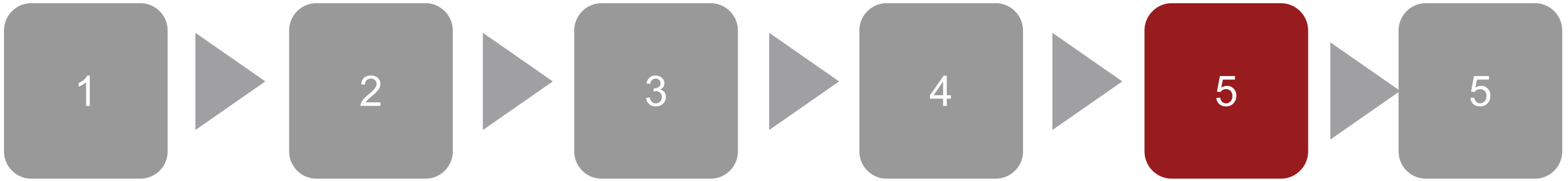
Connections between components made in system internal block diagram



4. Defining Inter-component propagations and transformations

- External failure propagations shown with associations
- Individual transformations in IBD of association
- Single source failure mode can transform into different sink failure modes





introduction Metamodel Procedure Example Outputs Discussion and Conclusions

FMEA Output

Table	Description and Use	Water Supply System Results
Full FMEA	List all FMEA information in SysML model Rows represent individual failure propagation paths	There are 1110 propagation paths with unique originating components, failure modes, causes, propagation steps, and end effects (with a conventional manually generated FMEA, there would be only 37 rows)
Failure Modes and Effects Summary	Provides both qualitative and quantitative data about each failure mode and effect Useful for prioritizing failure and cybersecurity resources by identifying system components with the highest number of failure modes, undetectable or unmitigated failure modes, and long propagation paths	The VPN is the component with the most failure modes, actuator failure modes have the highest proportion of severity 1 events, CRCs and redundancy checks are the most often used detection mechanism, Retry is the most common recovery mechanism. Malicious Data is the failure mode that is most often not detected and has the greatest severity effects
System Effects Summary	Provides analysis of all system effects in system Useful for determining undetected, unmitigated, or unprotected system effects	The VPN is the component with the largest number of severity 1 failure modes Actuators (pump and value) and the control processor are also significant contributors to Severity 1 failure modes
Diagnostics	Matrix of system effects versus their causes Capable of determining probably causes of system effects	The VPN is the single component most likely to be the cause of malfunctions in the actuators The control processor can be a cause of all system level effects identified thus far
Propagation Description	Rows represent individual failure propagation paths Each cell in a row lists detailed information about a single failure propagation hop	There are multiple propagation paths for which there is no protection against a cyberattack; measures for failure detection and mitigation should be evaluated to determine if there is any effect

FMEA Output Excerpt

Full FMEA

Failed Component	Failure Mode	Cause	Intermediate Effects	Intermediate Causes	End Component	End Effect
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data; VPN1: Bad Data	Control processor: ; VPN1:	Valve:Actuator	Actuator Energizes incorrectly
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data; VPN1: Bad Data	Control processor: ; VPN1:	Valve:Actuator	Actuator engages without computer command
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data; VPN1: Bad Data	Control processor: ; VPN1:	Pump:Actuator	Actuator Fails to Perform When Commanded
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data; VPN1: Bad Data	Control processor: ; VPN1:	Pump:Actuator	Actuator Energizes incorrectly
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data; VPN1: Bad Data	Control processor: ; VPN1:	Pump:Actuator	Actuator engages without computer command
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data	Control processor:	Level:Sensor	Sensor receives bad data
Control processor:Computer	Malicious Input	Cyberattack, vulnerability	Control processor: Bad Data	Control processor:	Pressure:Sensor	Sensor receives bad data

Shows all Failure Modes, Causes, Effects, Detections, Mitigations, and recommendations/comments; propagations presented in a compressed form

Failure Modes and Effects Summary (FMES)

Component	Failure Mode	Primary Failure Mode	Intermediate Effects Occurrences	Unique Failure Modes and Effects	Total Failure Modes and Effects	Detection	Mitigation	Protection	Comment	Severity 1	Severity 2	Severity 3	Severity 4	Severity 5
VPN1	Corrupt Data	8	124	66	132	CRC	Retry	Unknown Protection	Requires CRC	132	0	0	0	0
Pump	Corrupt Data	16	62	26	78	CRC	Retry	Unknown Protection		78	0	0	0	0
Valve	Corrupt Data	16	62	26	78	CRC	Retry	Unknown Protection		78	0	0	0	0
VPN1	Malicious Data	4	80	21	84	None	None	Unknown Protection		84	0	0	0	0
Pump	Malicious Data	16	32	8	48	None	None	Unknown Protection		48	0	0	0	0
Valve	Malicious Data	16	32	8	48	None	None	Unknown Protection		48	0	0	0	0
VPN1	Late Data	6	126	66	132	Timer expiration	Retry	Unknown Protection	Requires timer	0	0	132	0	0
Pump	Late Data	4	56	20	60	Timer expiration	Retry	Unknown Protection	Requires timer	0	0	60	0	0
Valve	Late Data	4	56	20	60	Timer expiration	Retry	Unknown Protection	Requires timer	0	0	60	0	0
VPN1	Low Signal Integrity	250	100	7	350	Unknown Detection	Unknown Mitigation	Unknown Protection		294	0	56	0	0
Level	Fails to Output	21	0	3	21	Unknown Detection	Unknown Mitigation	Unknown Protection		12	0	9	0	0
Control processor	No Data	5	80	17	85	Timer expiration	Retry; switchover to redundant computer	Unknown Protection	Requires timer	34	0	51	0	0

Shows components and counts of internal failure modes, occurrences, detections, mitigations, and severity distributions – enables assessment of the importance and priority of detection and mitigation measures

System Effects Table

Component	System Effect	Total System Effect Occurrences	First Known Detection:Number of Occurrences	First Known Mitigation:Number of Occurrences	First Known Protection:Number of Occurrences	Severity
Valve	Actuator Fails to Perform When Commanded	221	CRC: 52, Reasonableness check: 56, Timer expiration: 65, CRC, reasonableness check: 26, Remote Monitoring: 16, None: 6,	Substitution of default value or retry: 52, Retry; switchover to redundant computer: 59, Use an alternate means of Control: 4, Retry: 58, Retry; use alternate actuation: 16, None: 32,	Unknown Protection: 180, Shielding, anti-tamper: 26, More rigorous defect avoidance: 12, Message authentication: 3,	1
Pump	Actuator Fails to Perform When Commanded	221	CRC: 52, Reasonableness check: 56, Timer expiration: 65, CRC, reasonableness check: 26, Remote Monitoring: 16, None: 6,	Substitution of default value or retry: 52, Retry; switchover to redundant computer: 59, Use an alternate means of Control: 4, Retry: 58, Retry; use alternate actuation: 16, None: 32,	Unknown Protection: 180, Shielding, anti-tamper: 26, More rigorous defect avoidance: 12, Message authentication: 3,	1
Valve	Actuator engages without computer command	90	Unknown Detection: 3, Reasonableness check: 56, CRC, reasonableness check: 13, None: 18,	Unknown Mitigation: 3, Substitution of default value or retry: 52, Use an alternate means of Control: 4, None: 31,	Unknown Protection: 49, Shielding, anti-tamper: 13, More rigorous defect avoidance: 12, Message authentication: 16,	1
Valve	Actuator Energizes incorrectly	90	Reasonableness check: 56, CRC, reasonableness check: 13, Remote Monitoring: 3, None: 18,	control operator intervention: 3, Substitution of default value or retry: 52, Use an alternate means of Control: 4, None: 31,	Unknown Protection: 49, Shielding, anti-tamper: 13, More rigorous defect avoidance: 12, Message authentication: 16,	1

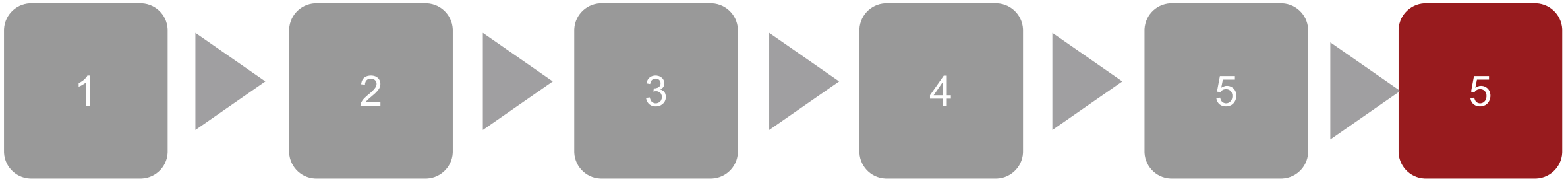
Diagnostics Table

Symptom	Control processor	Flow	Level	Pressure	Pump	VPN1	Valve	adversary	firewall1
Sensor receives bad data	27%	13%	13%	13%	0%	0%	0%	13%	20%
Sensor receives late data	43%	14%	14%	14%	0%	0%	0%	7%	7%
Actuator engages without compu	8%	4%	4%	4%	9%	39%	9%	18%	4%
Actuator Energizes incorrectly	8%	4%	4%	4%	9%	39%	9%	18%	4%
Sensor receives corrupt data	40%	0%	0%	0%	0%	0%	0%	20%	40%
Actuator Fails to Perform When	6%	5%	5%	5%	7%	47%	7%	14%	5%
Sensor receives malicious data	100%	0%	0%	0%	0%	0%	0%	0%	0%
Actuator Energizes Late	13%	6%	6%	6%	3%	47%	3%	15%	1%
Sensor receives no data	18%	18%	18%	18%	0%	0%	0%	12%	18%
Total	11%	6%	6%	6%	6%	37%	6%	15%	6%

Propagation Description Table (excerpt)

Original Failure Mode	Propagation Step 1	Propagation Step 2	Propagation Step 3	Propagation Step 4
VPN1:VPN Failure Mode: Interfered Transmissions Cause: Cyberattack	Valve:Actuator Failure Mode: Corrupt Data Cause: Unspecified Cause Detection: CRC Mitigation: Retry Comment: Protection: Unknown Protection	Pump:Actuator Failure Mode: Corrupt Data Cause: Unspecified Cause Detection: CRC Mitigation: Retry Comment: Protection: Unknown Protection	VPN1:VPN Failure Mode: Corrupt Data Cause: Unspecified Cause Detection: CRC Mitigation: Retry Comment: Requires CRC Protection: Unknown Protection	Pump:Actuator Failure Mode: Actuator Fails to Perform When Commanded Cause: Unspecified Cause Detection: Remote Monitoring Mitigation: Retry; use alternate actuation Comment: Recoverable from control station Protection: Unknown Protection Severity: 1 Severity Comment: Recoverable from control station
VPN1:VPN Failure Mode: Interfered Transmissions Cause: Cyberattack	Valve:Actuator Failure Mode: Malicious Data Cause: Unspecified Cause Detection: None Mitigation: None Comment: Protection: Message authentication	VPN1:VPN Failure Mode: Malicious Data Cause: Unspecified Cause Detection: None Mitigation: None Comment: Protection: Unknown Protection	Valve:Actuator Failure Mode: Actuator engages without computer command Cause: Unspecified Cause Detection: Unknown Detection Mitigation: Unknown Mitigation Comment: Could result in loss of control, instability, and loss of water system Protection: Unknown Protection Severity: 1 Severity Comment: Could result in loss of control, instability, and loss of water system	
VPN1:VPN Failure Mode: Interfered Transmissions Cause: Cyberattack	Valve:Actuator Failure Mode: Malicious Data Cause: Unspecified Cause Detection: None Mitigation: None Comment: Protection: Message authentication	VPN1:VPN Failure Mode: Malicious Data Cause: Unspecified Cause Detection: None Mitigation: None Comment: Protection: Unknown Protection	Valve:Actuator Failure Mode: Actuator Energizes incorrectly Cause: Unspecified Cause Detection: Remote Monitoring Mitigation: control operator intervention Comment: Could reuslt in loss of control, instability and loss of water system Protection: Unknown Protection Severity: 1 Severity Comment: Could reuslt in loss of control, instability and loss of water system	

Shows the details of the propagation of each failure mode (expands the condensed propagation information in the Full FMEA)



introduction Metamodel Procedure Example Outputs Discussion and Conclusions

Discussion

- FMEA approach described here enables integration of cybersecurity and traditional R&M/safety analysies
  - Cyberphysical system reliability, safety, and cybersecurity analyses should be integrated
    - Cyberattack intent and effects may be system failures that can be detected and mitigated using detection and recovery techniques
  - Application to cybersecurity discussed for more than a decade e.g., Gorbenko (2006), Raanan (2008) referenced in paper
    - Cause vs. vulnerability
    - Failure mode vs. exploit
    - Propagation, Detection, and Recovery (common)
- Next steps
  - Development of libraries of standardized failure modes and propagations
    - Failure modes for classes of components (e.g., sensors, computers, LANs, automobile tires, rocket engines, etc.)
    - Specialized to specific components through inheritance
    - CVEs and CWEs for software components
  - Propagations for common pairs of components (e.g., processor and USB port, motor and shaft, etc.)

Summary and Conclusions

- Tool Automates the manual FMEA process
  - Automated process much less arduous
  - Allows FMEAs to be generated iteratively throughout design and production phases
  - Libraries of components can be created to enable failure propagations, detections and mitigations attributes to be reused
- Automated FMEA output is more detailed and correct
  - Contains all steps in failure propagation paths
  - Important analysis performed automatically (e.g. Failure Modes and Effects Summary)
  - Validations and model editor exist to ensure proper modeling
- Process is model-based
  - FMEA produced from SysML architectural model
  - FMEA can be produced on demand (i.e., early and often) enabling early identification of deficiencies
- New applications of FMEA to cyber security
  - Malicious actors represented as components in system
  - Malicious actors can cause failure modes in other components

29th Annual INCOSE international symposium

Orlando, FL, USA

July 20 - 25, 2019

www.incose.org/symp2019