UNIVERSITY OF OXFORD

Models will not solve all of your problems

But they can help you understand…

Avi Shaked, PhD
Senior Research Associate

Why do we need model driven engineering?

- "To generate usable work products"
- "To organise, find, filter, retrieve, examine, and edit information about large systems"

But also:

- "To capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree on them"
- "To think about the design of a system"

Source for cited: Rumbaugh, Jacobson and Booch, 1999, The Unified Modeling Language reference manual

Does modelling really support the objectives?

- UML Ref Manual:
  - “Semantics and presentation”
    - Semantics (“often called *the model*”) – capture “the meaning of an application as a network of logical constructs”
    - Presentation – “shows semantic information in a form the can be seen, browsed and edited by humans”. “Presentation elements carry the visual presentation of the model – that is, they show it in a form directly apprehensible by humans.”

Let’s examine this in a real life application

Source for cited: Rumbaugh, Jacobson and Booch, 1999, The Unified Modeling Language reference manual

A model driven approach to systems security engineering

Trying to design security aspects of systems and assess security posture and risks

A model driven approach to systems security engineering: Semantics (capture "the meaning of an application as a network of logical constructs")

- UML
  - Actor:
    "characterizes and abstracts an outside user or related set of users that interact with a system of classifier"
  - Class:
    "the named description of both the data structure and the behavior of a set of objects"
- Real life:
  - System
  - Components
  - Threats, Risks
  - Security Controls
  - **Mitigation**

Source for cited: Rumbaugh, Jacobson and Booch, 1999, The Unified Modeling Language reference manual

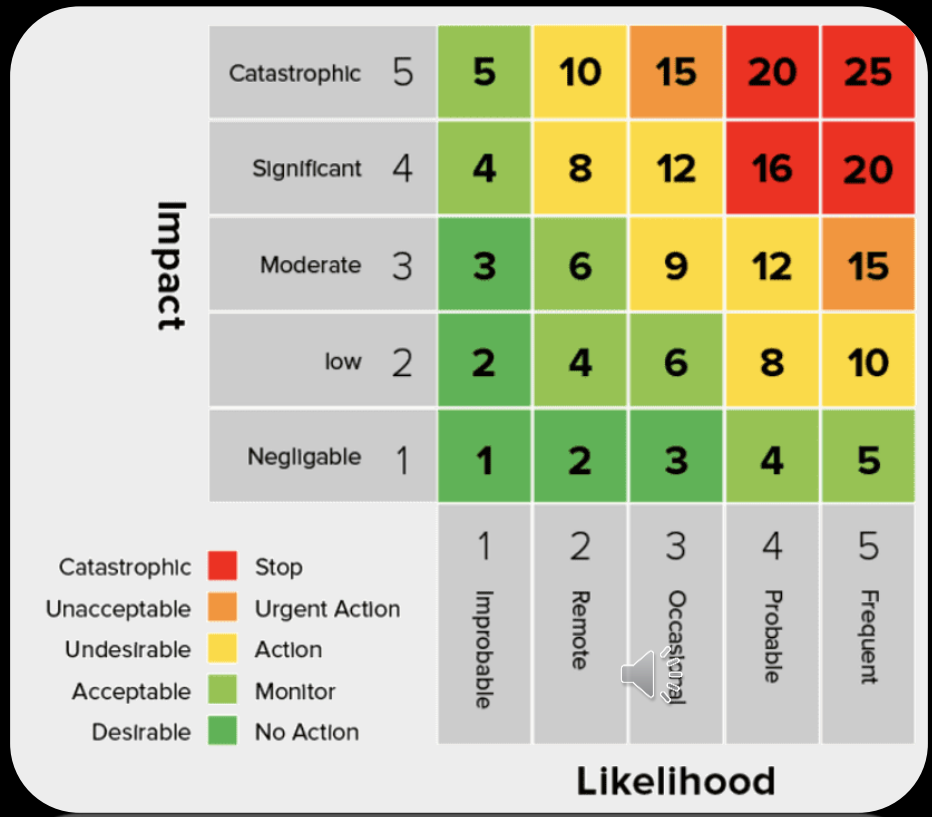
A model driven approach to systems security engineering: Presentation (show the model in a form directly apprehensible by humans)

- UML
  - Class diagram?
  - Use case diagram?
- Real life

So, what should we do?

	«Block» Radio	«ConstraintBloc Joule Effect	«Block» AlarmRadio	«Block» Alarm
<<Requirement>> 004 : Save				
<<Requirement>> 007 : Radio frequencies				
<<Requirement>> 008 : Dissipation				
<<Requirement>> 003 : Clock control				
<<Requirement>> 001 : Alarm				
<<Requirement>> 005 : Radio station control	s			
<<Requirement>> 002 : Radio control	s			
<<Requirement>> 006 : Volume radio contro				

Source: http://www.umldesigner.org/ref-doc/define-the-system.html



Source: https://www.balbix.com/insights/cyber-risk-heat-map/

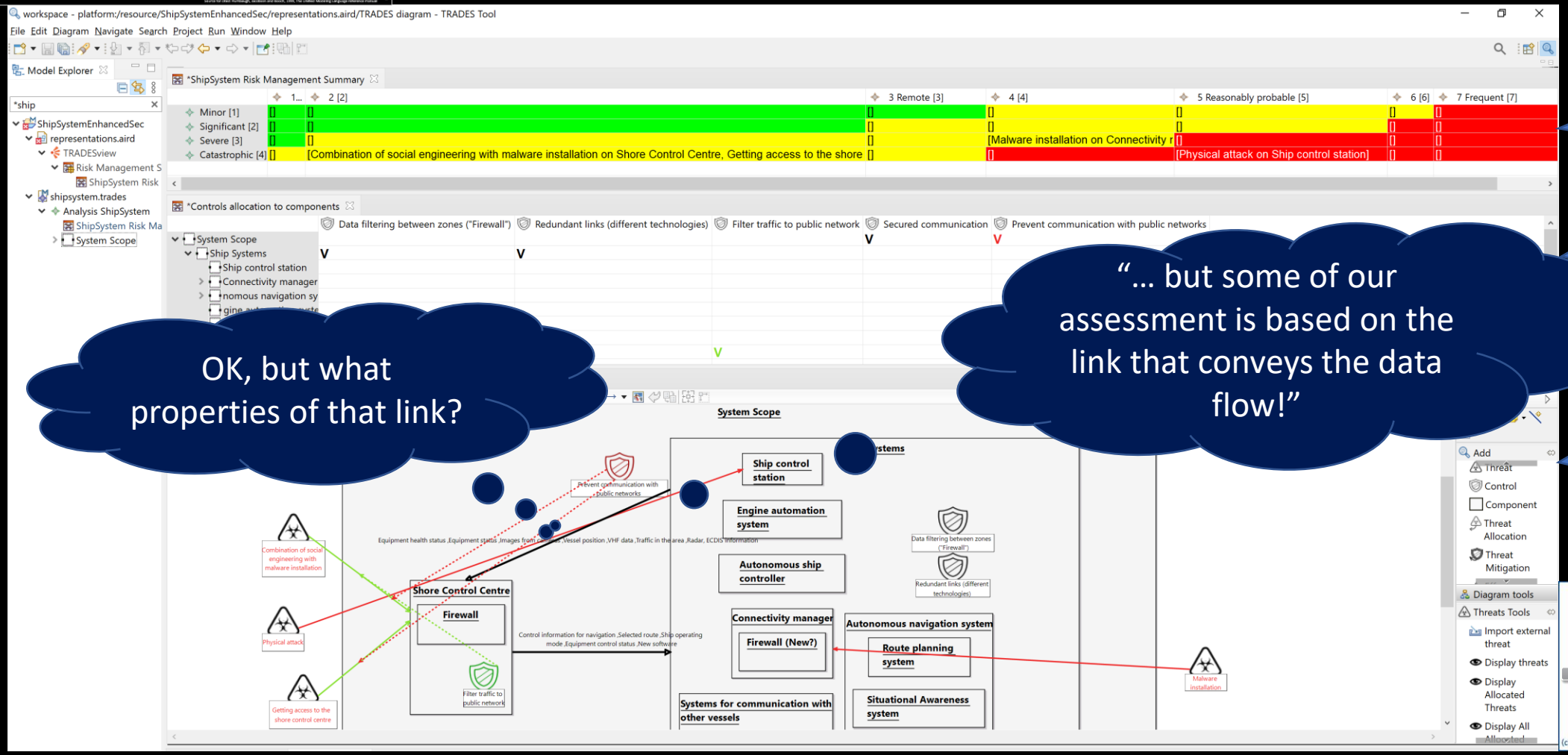
Why do we need model driven engineering?

- "To generate usable work products"
- "To organise, find, filter, retrieve, examine, and edit information about large systems"

But also:

- "To capture and precisely state requirements and domain knowledge so that all stakeholders may understand and agree on them"
- "To think about the design of a system"

A domain-specific, model driven approach to systems security engineering



Synchronised risk matrix

Function allocations

Formalised security assessment

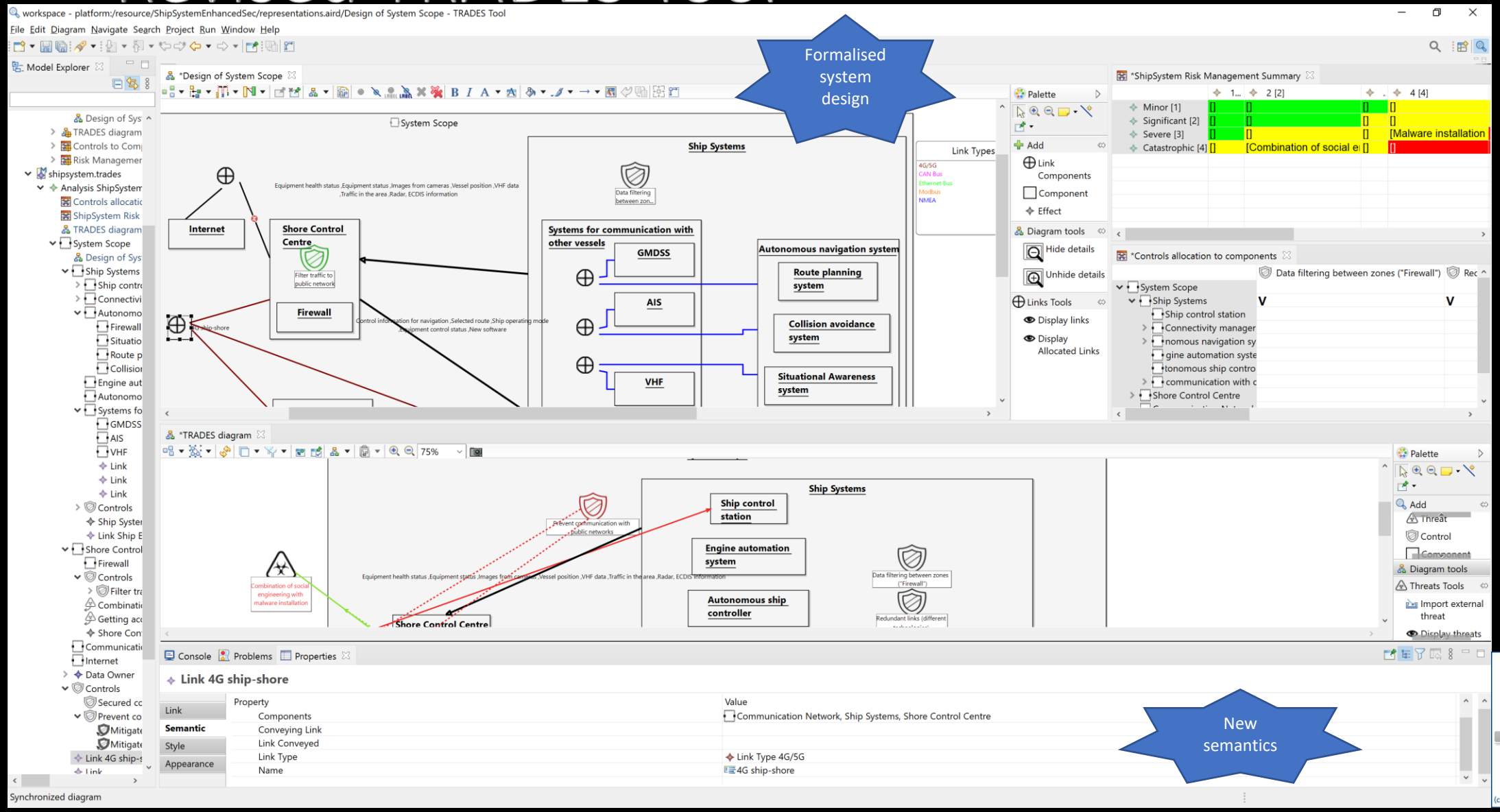
"… but some of our assessment is based on the link that conveys the data flow!"

OK, but what properties of that link?

TRADES Tool

https://github.com/IAI-Cyber/TRADES

Revised TRADES Tool

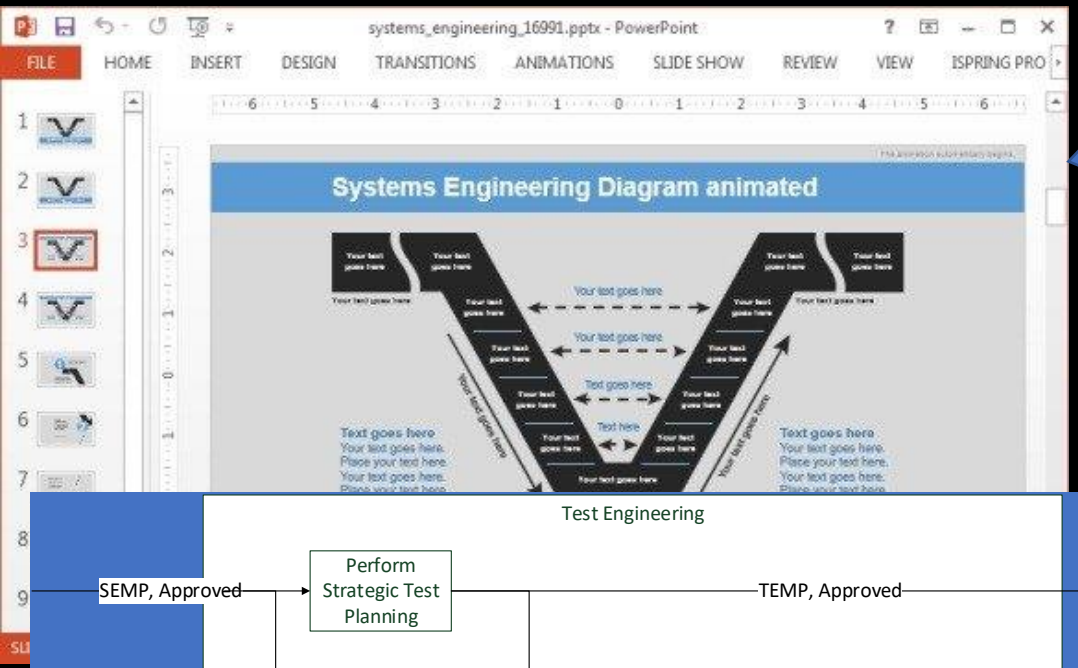


https://github.com/IAI-Cyber/TRADES

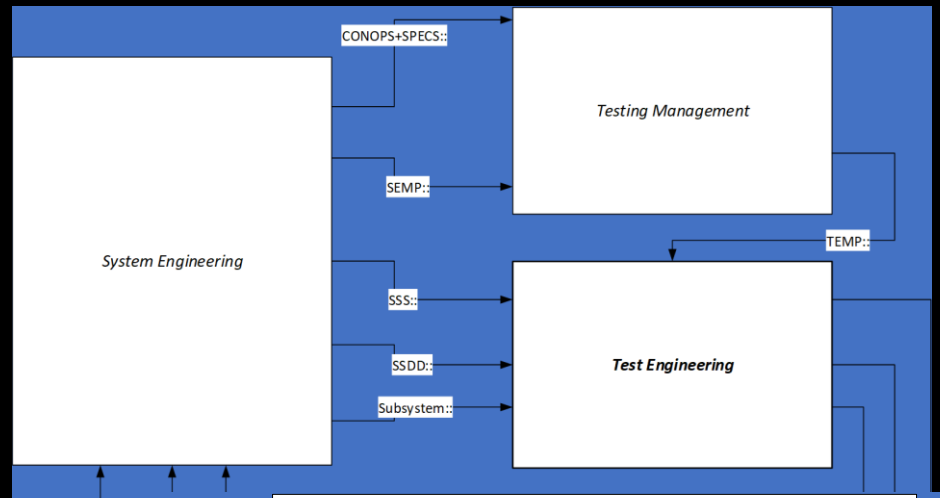
Restructuring the development process definitions

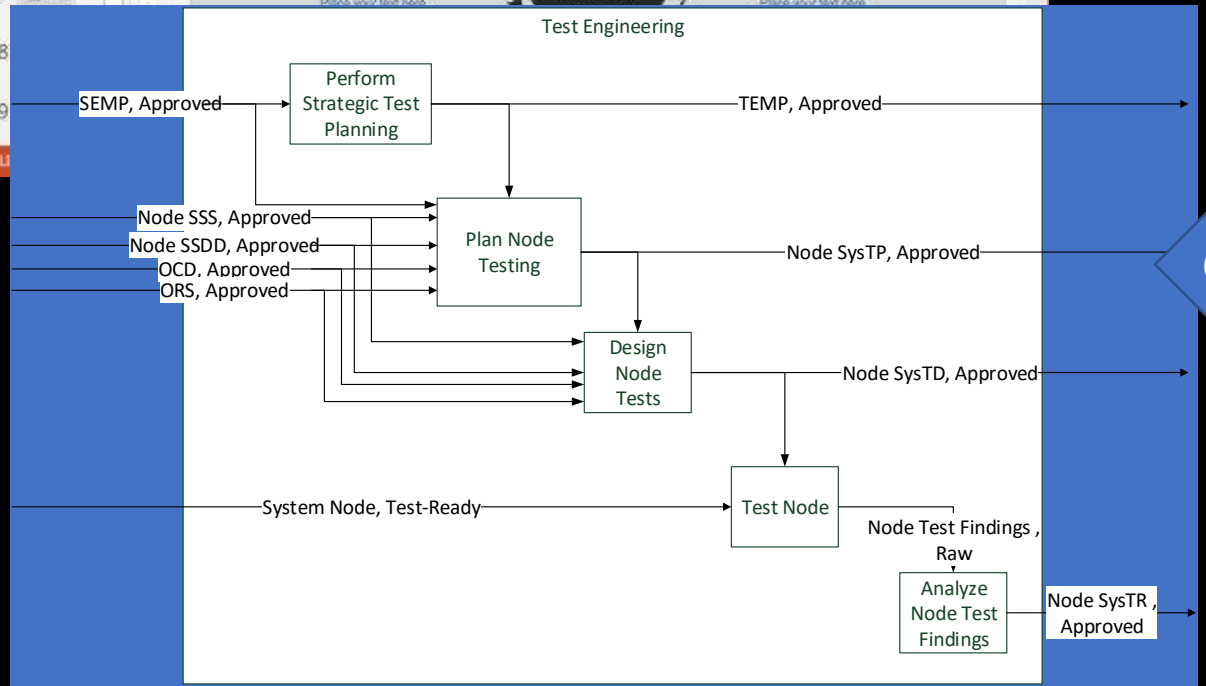
PROVE Tool

https://github.com/TAU-SERI/PROVE

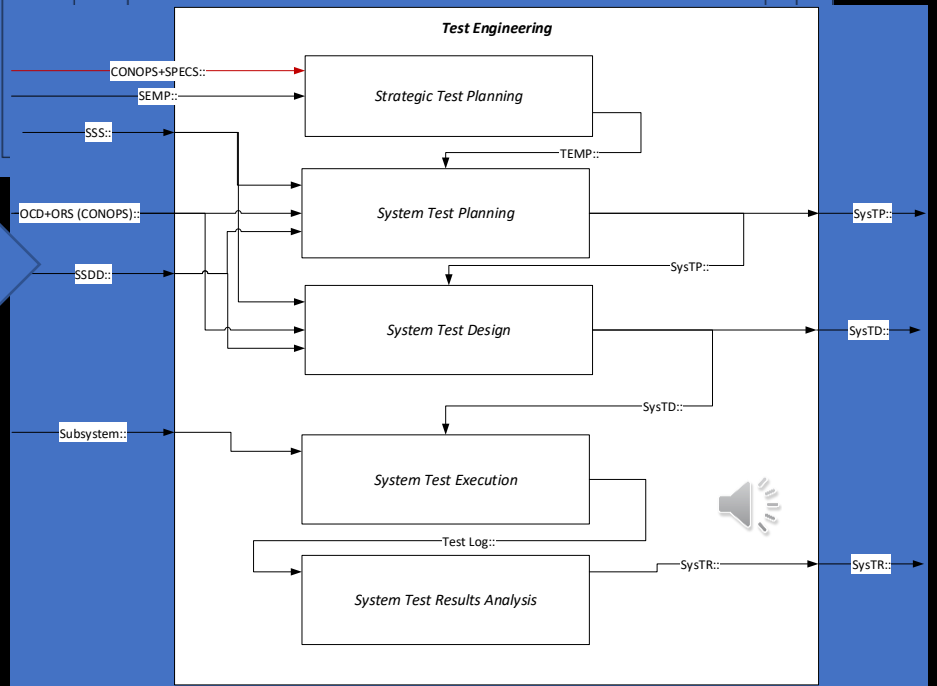


Agreed semantics and presentation



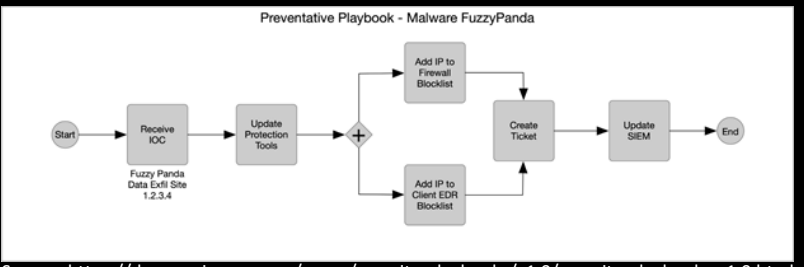


Comparable*



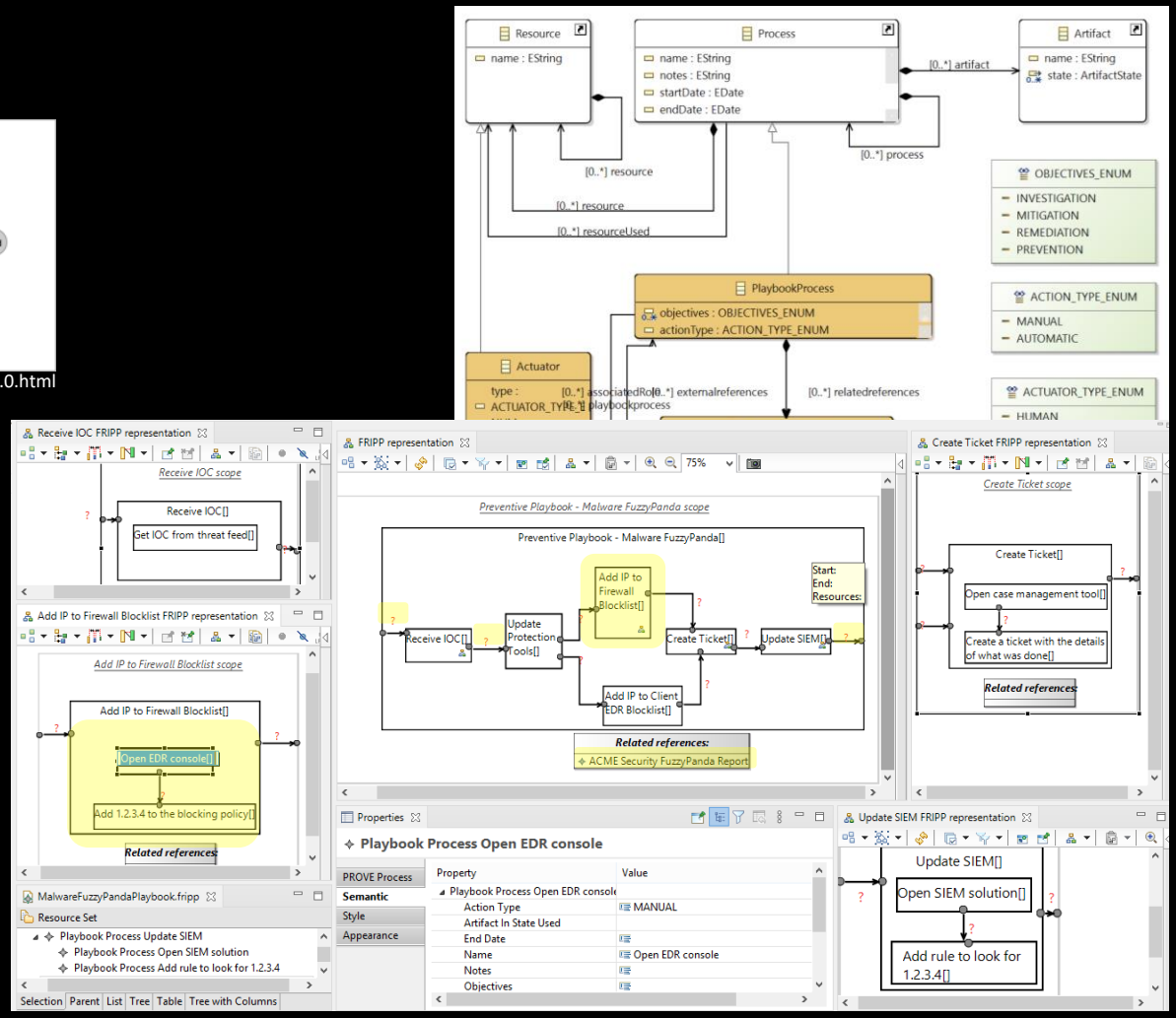
* Compare, for example, with Sharon & Dori, 2017. Model-Based Project-Product Lifecycle Management and Gantt Chart Models: A Comparative Study.

Designing Cyber Security Incident Response: Restructuring the process playbook



Source: https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html


```
{
  "type": "playbook",
  "spec_version": "1.0",
  "id": "playbook--6b74199d-42a6-43a1-99cb-75d52207a778",
  "name": "Prevent FuzzyPanda Malware",
  "description": "This playbook will block traffic to the FuzzyPanda data exfil site",
  "playbook_types": [ "prevention" ],
  "external_references": [ { "name": "ACME Security FuzzyPanda Report", } ],
  "features": { "parallel_processing": true, "data_markings": true },
  "markings": [ "marking-statement--16a48f6b-ab42-4f99-ba9b-8b21e1225836", "marking-tlp--a099a2eb-1113-4368-9b17-d7ef75841239" ],
  "workflow_start": "start--7269bda2-e651-44d3-9fe5-aa7e88484b93", "workflow": { "start--7269bda2-e651-44d3-9fe5-aa7e88484b93": { "type": "start", "on_completion": "single--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb" },
    "single--8c46cab0-46a3-48f4-b4bb-9643dcfaf642": { "type": "single", "name": "Add IP to Firewall Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the firewall", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open firewall console and add 1.2.3.4 to the firewall blocking policy" } ] },
    "single--3d930f08-e22c-4dd4-996f-61f2d022121c": { "type": "single", "name": "Add IP to Client EDR Blocklist", "description": "This step will add the IP address of the FuzzyPanda data exfil site to the client EDR solution", "on_completion": "single--d5780323-5107-4cd0-bac4-6553c9d90c8e", "commands": [ { "type": "manual", "command": "Open EDR console and add 1.2.3.4 to the blocking policy" } ] },
    "single--d5780323-5107-4cd0-bac4-6553c9d90c8e": { "type": "single", "name": "Create Ticket", "description": "This step will create a ticket for this issue", "on_completion": "single--33dc512c-263d-4f8a-a07d-cfe9f6d6ed26", "commands": [ { "type": "manual", "command": "Open case management tool and create a ticket with the details of what was done" } ] },
```

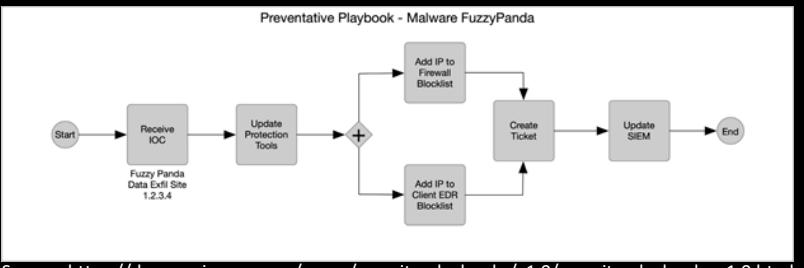



Formalised Incident Response Semantics

Formalised Incident Response Presentation

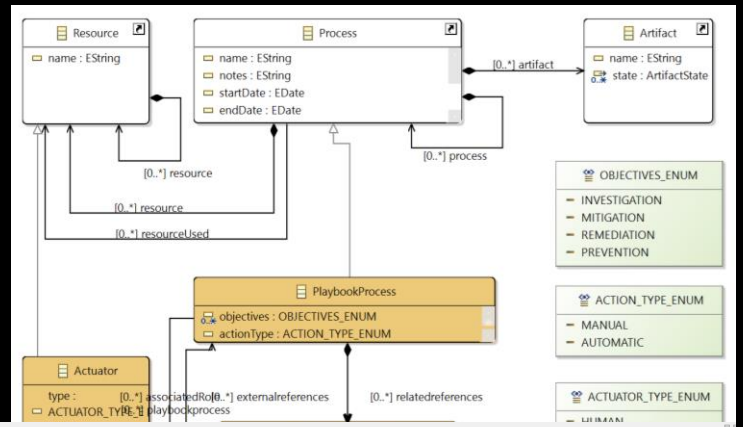
Source: Shaked, Cherdantseva, and Burnap, 2022. Model-Based Incident Response Playbooks. In Proceedings of the 17th International Conference on Availability, Reliability and Security.

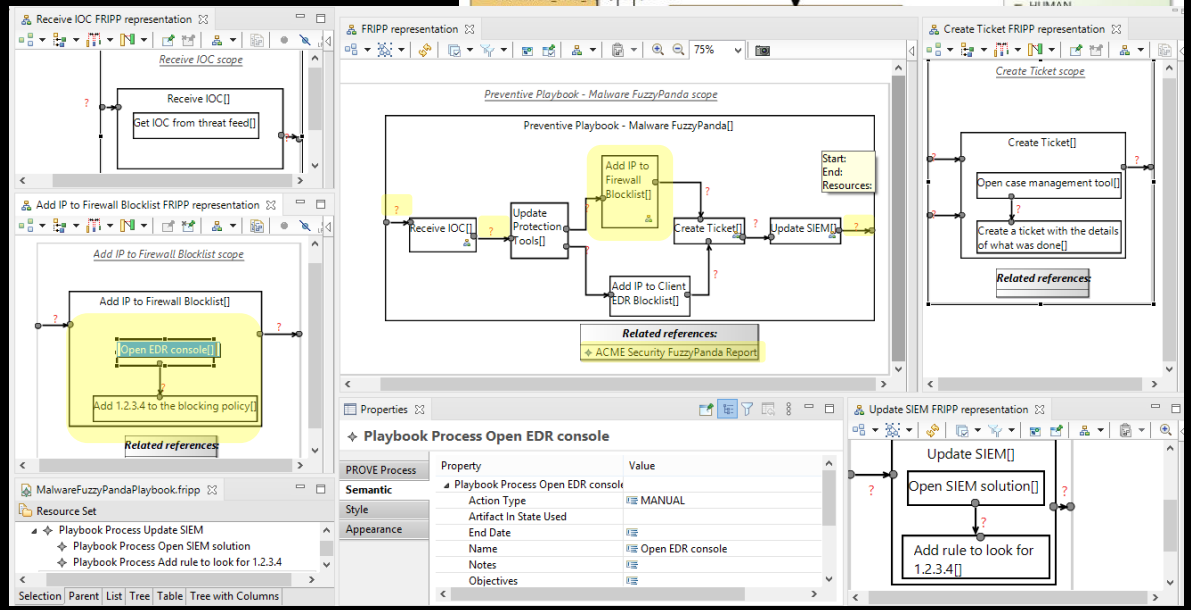
Designing Cyber Security Incident Response: Restructuring the process playbook is insufficient!



Source: https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html

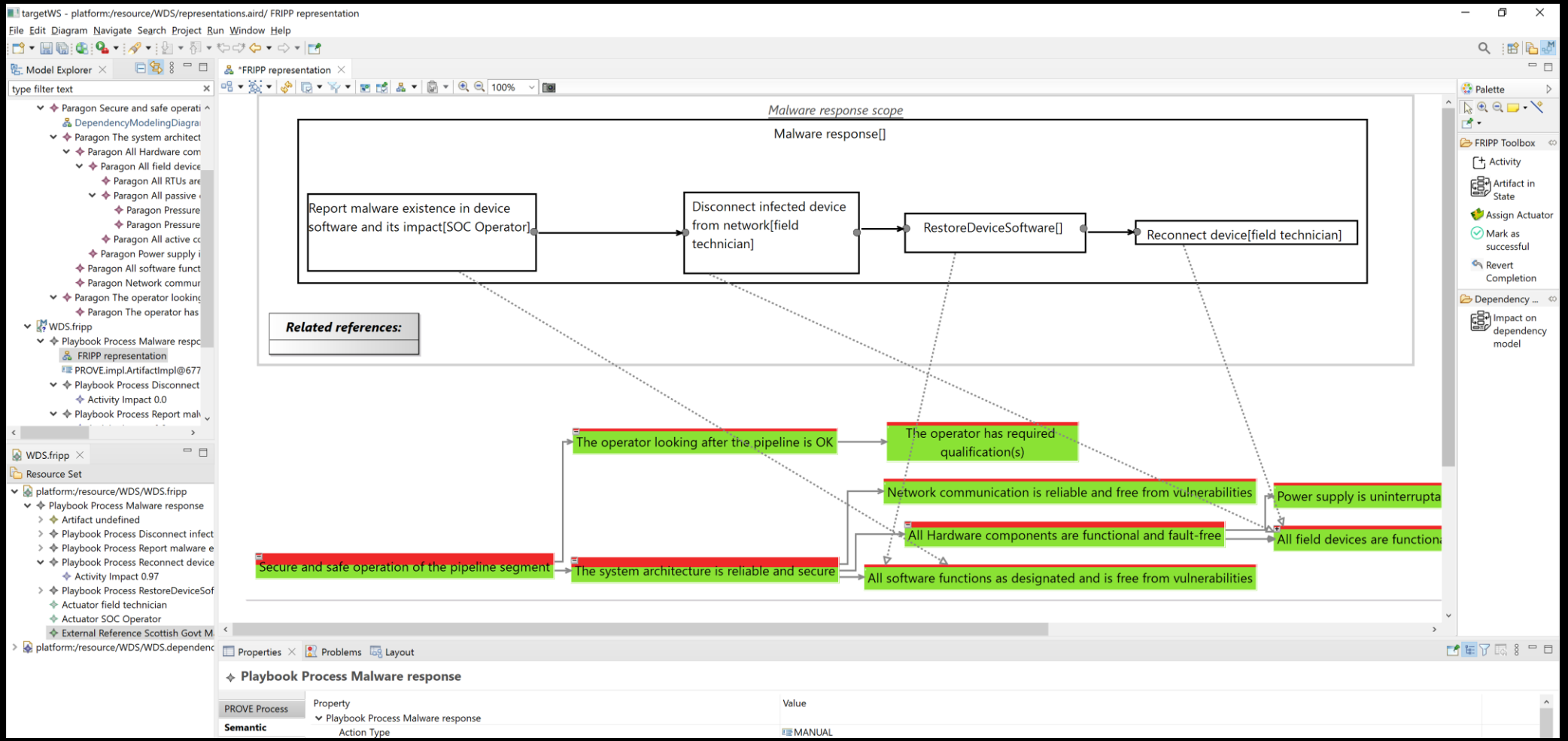

```
{
  "type": "playbook",
  "spec_version": "1.0",
  "id": "playbook--6b74199d-42a6-43a1-99cb-75d52207a778",
  "name": "Prevent FuzzyPanda Malware",
  "description": "This playbook will block traffic to the
FuzzyPanda data exfil site",
  "playbook_types": [ "prevention" ],
  "external_references": [ { "name": "ACME Security
FuzzyPanda Report", … } ],
  "features": { "parallel_processing":
true, "data_markings": true },
  "markings": [ "marking-statement--16a48f6b-ab42-4f99-ba9b-
8b21e1225836", "marking-tlp--a099a2eb-1113-4368-9b17-
d7ef75841239" ],
  "workflow_start": "start--7269bda2-e651-44d3-9fe5-
aa7e88484b93", "workflow": { "start--7269bda2-e651-44d3-9fe5-
aa7e88484b93": { "type": "start", "on_completion":
"single--a13c8450-2bd1-4a2b-9241-cf4f7e9f48cb" },
    "single--8c46cab0-46a3-48f4-b4bb-9643dcfaf642": { "type":
"single", "name": "Add IP to Firewall
Blocklist", "description": "This step will add the IP address
of the FuzzyPanda data exfil site to the
firewall", "on_completion": "single--d5780323-5107-4cd0-bac4-
6553c9d90c8e", "commands": [ { "type":
"manual", "command": "Open firewall console and add
1.2.3.4 to the firewall blocking policy" } ] },
    "single--3d930f08-e22c-4dd4-996f-61f2d022121c": { "type":
"single", "name": "Add IP to Client EDR Blocklist",
    "description": "This step will add the IP address of the
FuzzyPanda data exfil site to the client EDR solution",
    "on_completion": "single--d5780323-5107-4cd0-bac4-
6553c9d90c8e", "commands": [ { "type":
"manual", "command": "Open EDR console and add 1.2.3.4 to
the blocking policy" } ] },
    "single--d5780323-5107-4cd0-bac4-6553c9d90c8e": { "type":
"single", "name": "Create Ticket", "description": "This
step will create a ticket for this issue", "on_completion":
"single--33dc512c-263d-4f8a-a07d-cfe9f6d6ed26", "commands":
[ { "type": "manual", "command": "Open
case management tool and create a ticket with the details of what
was done" } ] },
```



Source: Shaked, Cherdantseva, and Burnap, 2022. Model-Based Incident Response Playbooks. In Proceedings of the 17th International Conference on Availability, Reliability and Security.

Designing Cyber Security Incident Response: Restructuring the process playbook is insufficient!



Improved semantics and presentation

Operational model – based on Cherdantseva et al., 2022. A configurable dependency model of a SCADA system for goal-oriented risk assessment.

https://github.com/ASH-SYSTEMS/SecMOF

Conservation of enterprise energy applies to Model-Driven Engineering

- Modelling requires significant effort
  - Develop meaningful semantics and representations
- Efficiency
  - Distributed “semantics” vs. governed, formal semantics
  - Reimagined “usable work products” - *sustainably usable products*
    - Model-based presentations
      - Can evolve, while relying on a formal information model
    - Model-based tool infrastructure (baseline, coherent integration)

Model responsibly and continuously to better understand your domain

Thank you

Feedback is welcome:
avi.shaked@cs.ox.ac.uk