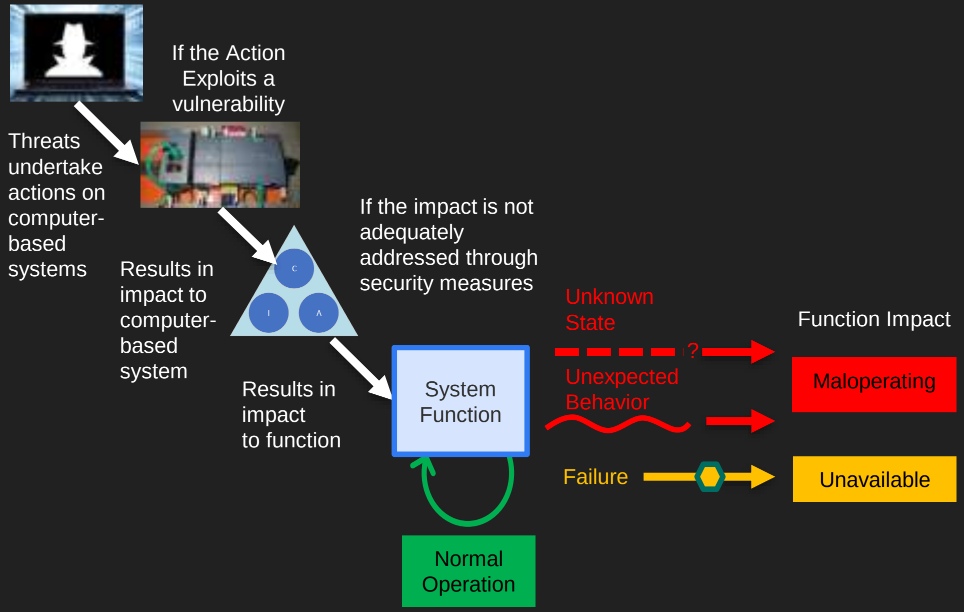
Understanding Digital Trust

Scenario Development Through Mapping Transitive Trust Relationships in Computer-based Systems

Mitchell Hewes

Basis

- We have a lexicon describing the impact of a threat compromising a computer-based I&C system (NSS No. 33-T Para 2.21) that can apply to all threat actions.
- However it has limitations:
  - Only captures the final Effect/Consequence, the “Boom”.
  - Does not support events which exploit Human/Computer as an information interface requiring trust.
  - Described through technical specificities.
  - Does not consider computers as complex systems more susceptible to a recursive multi-stage compromise of trust.
- We can extend the model by taking a broader view.



Threats undertake actions on computer-based systems

If the Action Exploits a vulnerability

Results in impact to computer-based system

If the impact is not adequately addressed through security measures

Results in impact to function

System Function

Normal Operation

Unknown State

Unexpected Behavior

Failure

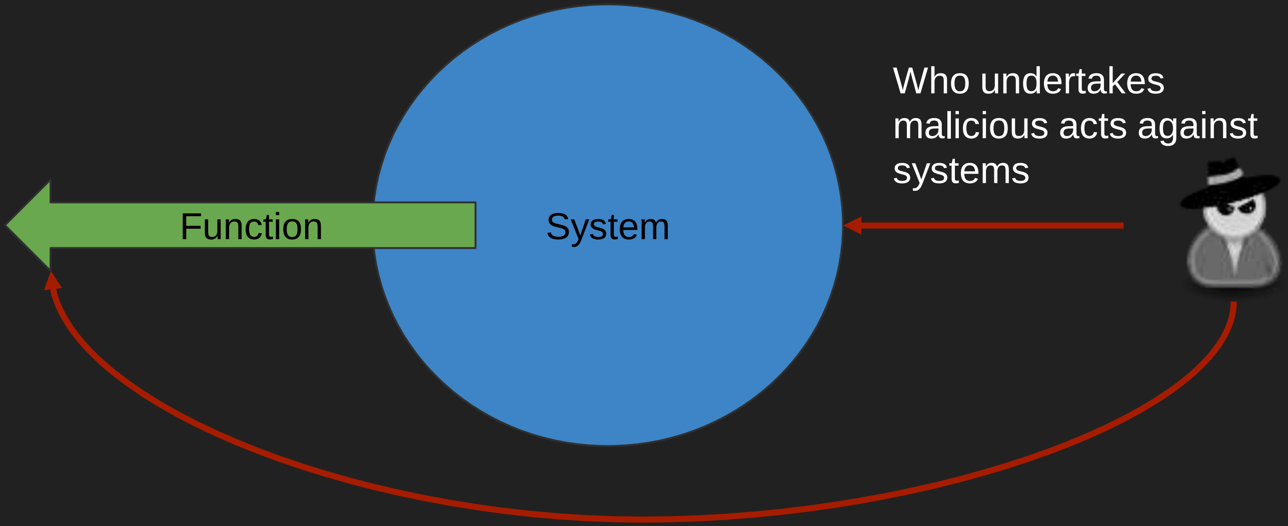
Function Impact

Maloperating

Unavailable

What is Security?

Systems, Functions, and Compromise



Who undertakes malicious acts against systems

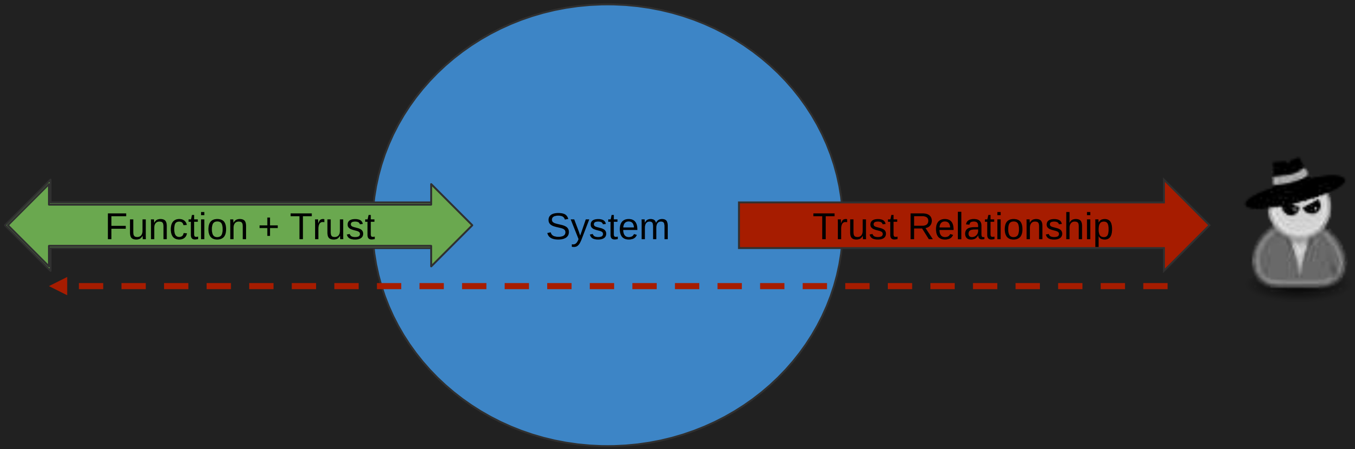
This is an adversary

In order to compromise the systems function

What is Security?

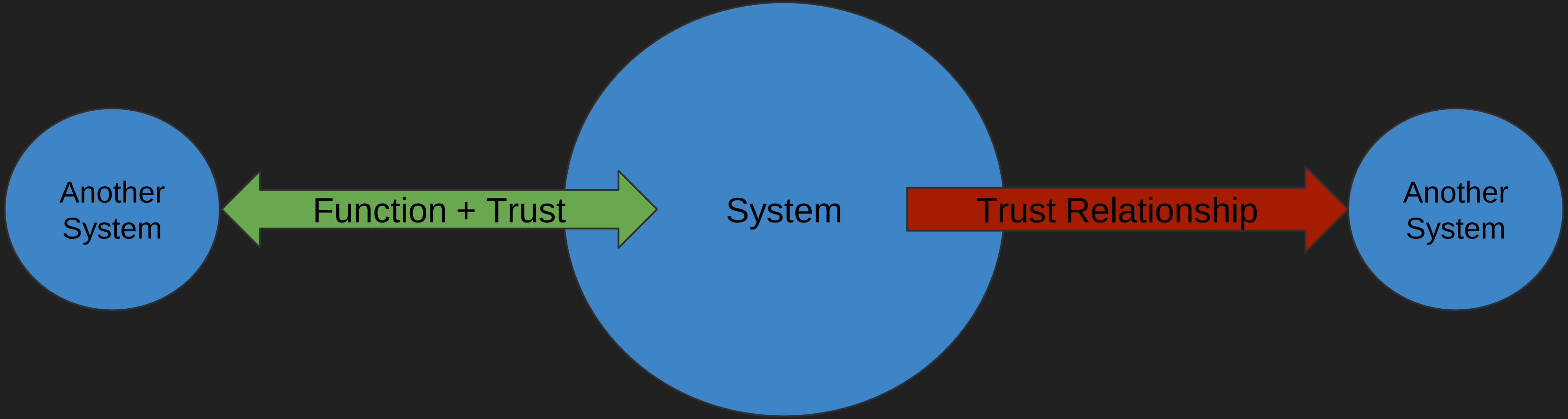
The degree of ***trust*** that a given ***system*** will continue to provide a desired ***function*** despite a ***malicious act***.

Transitive Trust



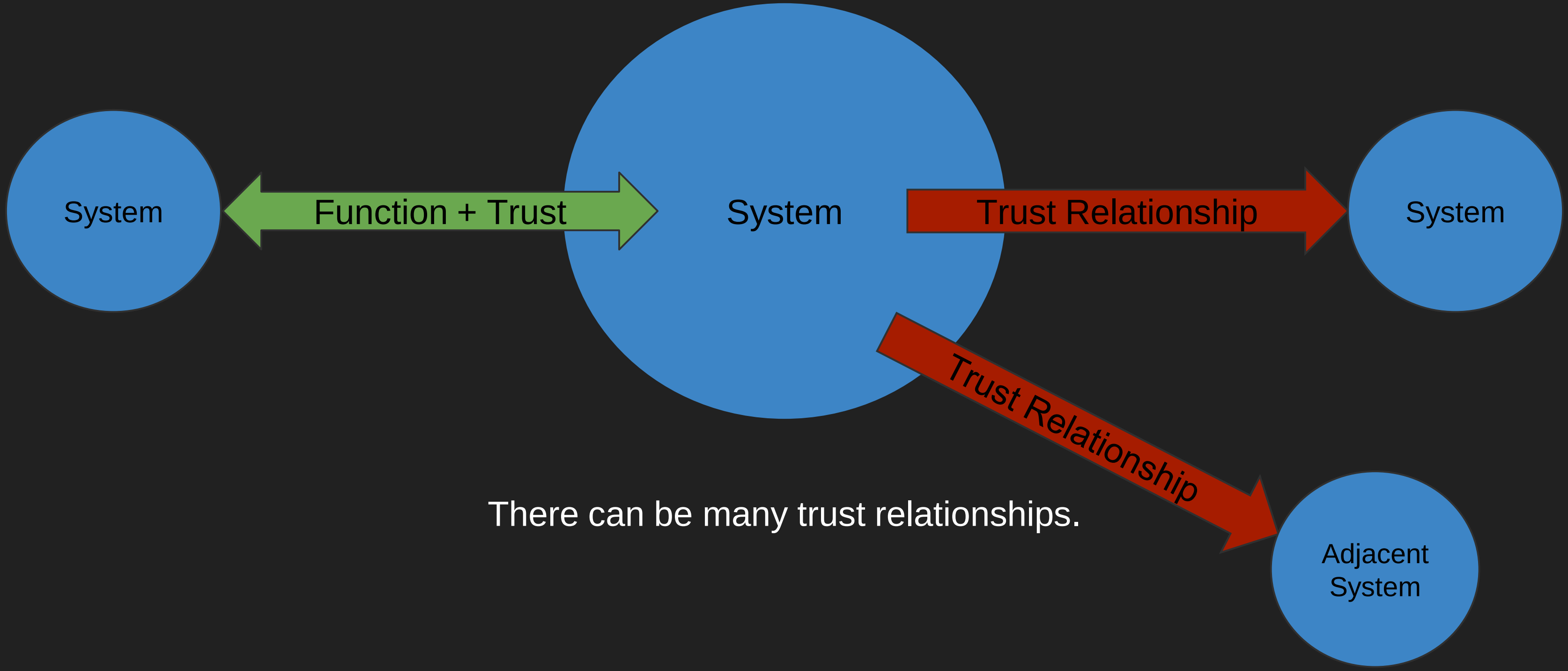
Adversaries impact ***systems*** by exploiting a trust relationship through a ***malicious act***.
Relying on the ***function*** of another ***system*** provides an implicit trust relationship.

Transitive Trust



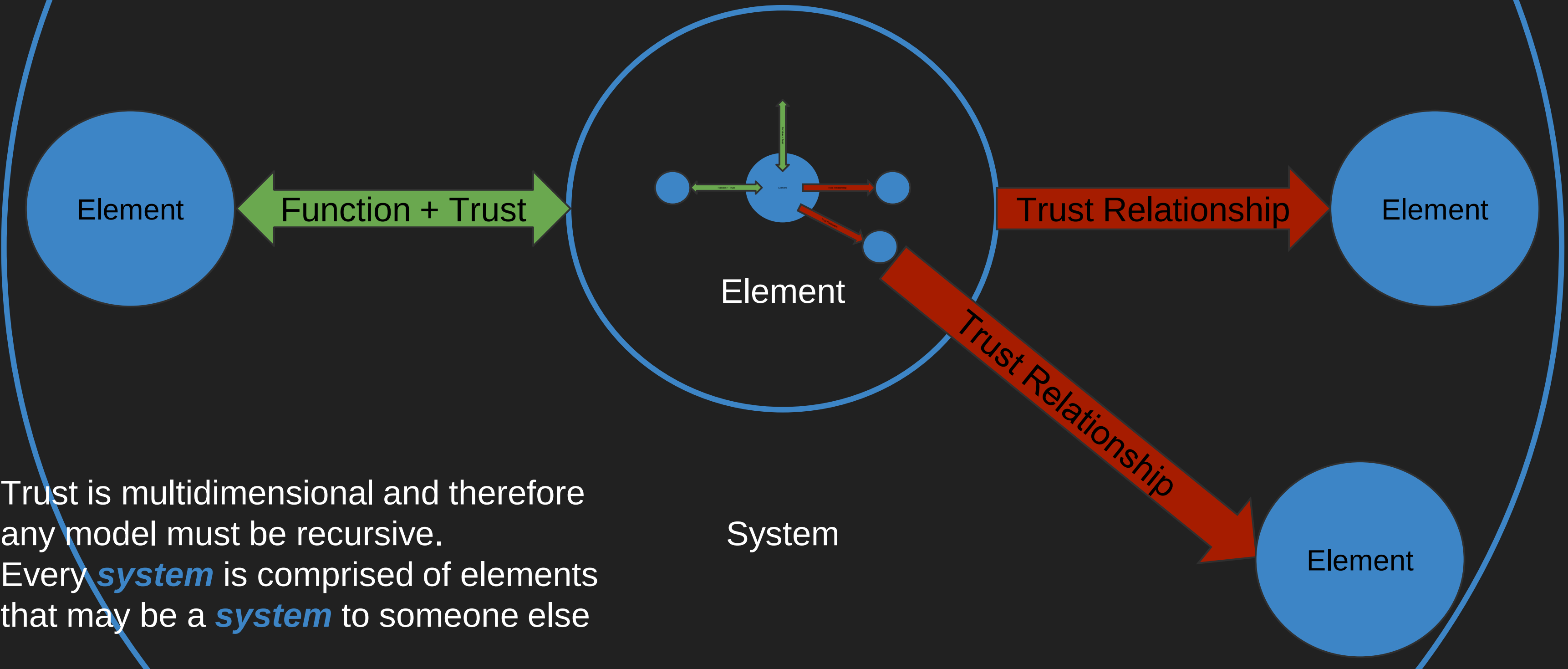
There always exists trust relationships between ***systems***.

Transitive Trust



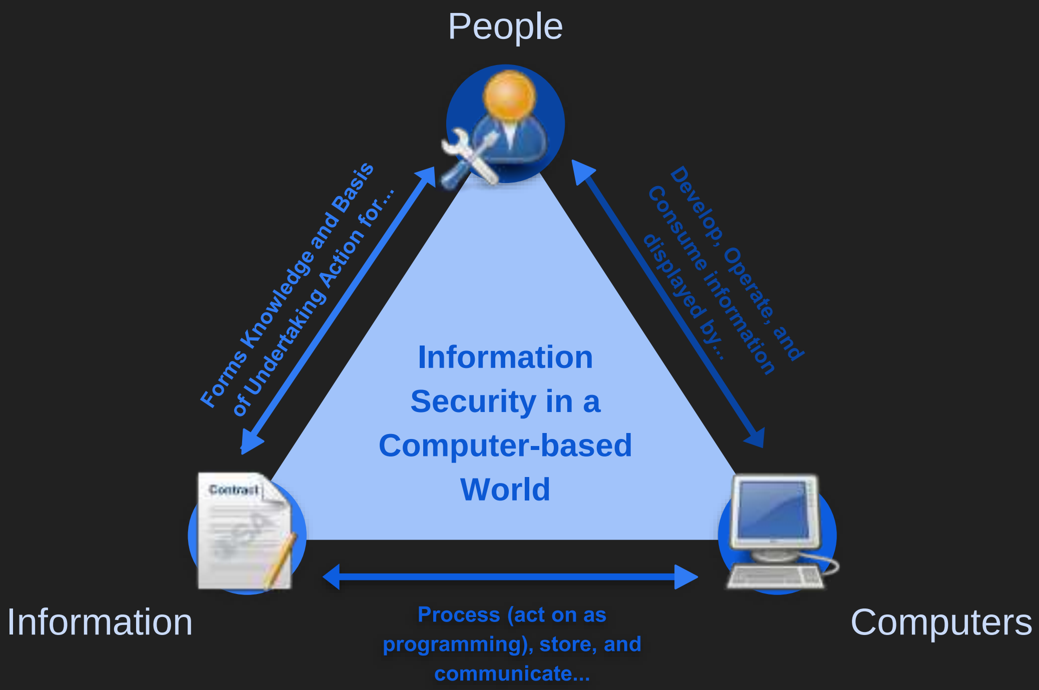
There can be many trust relationships.

Recursive Models



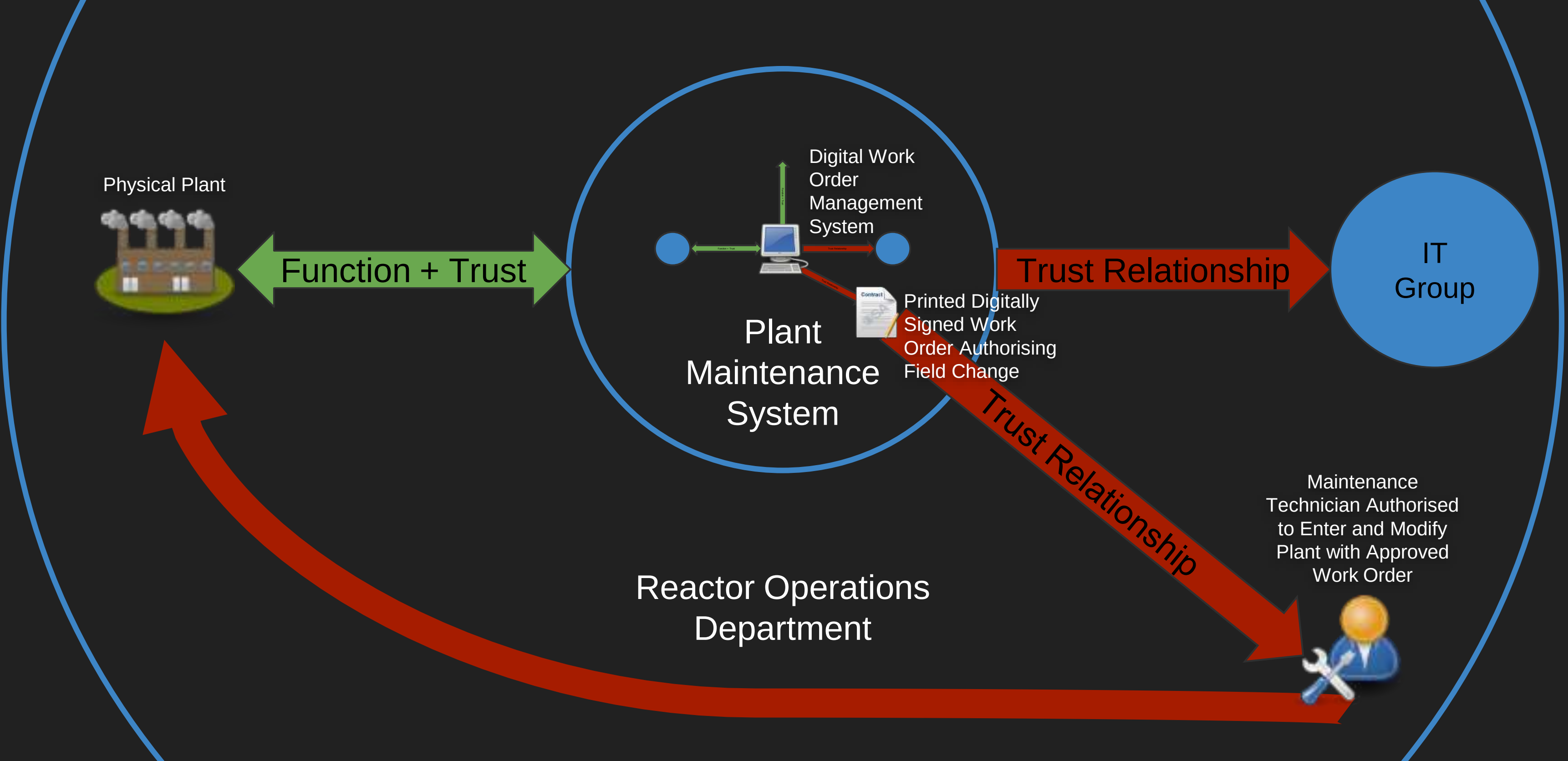
Trust is multidimensional and therefore any model must be recursive.
Every ***system*** is comprised of elements that may be a ***system*** to someone else

Computer-based Systems and Information Security


People
Forms Knowledge and Basis of Undertaking Action for...
Develop, Operate, and Consume information displayed by...
Information Security in a Computer-based World
Contrast
Information
Process (act on as programming), store, and communicate...
Computers

A ***System*** may be broader than computer-based systems.
Trust relationships need to be considered transitive far beyond pure digital connections.

Beyond Computer-based Systems



Physical Plant

Function + Trust

Digital Work Order Management System

Plant Maintenance System

Trust Relationship

IT Group

Printed Digitally Signed Work Order Authorising Field Change

Trust Relationship

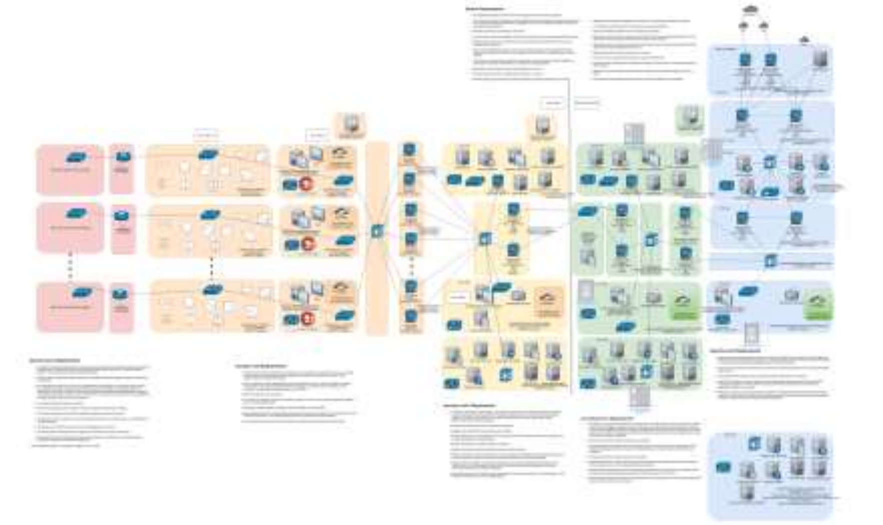
Maintenance Technician Authorised to Enter and Modify Plant with Approved Work Order

Reactor Operations Department

Using this to model Computer Security?

Limitations of Current Approaches

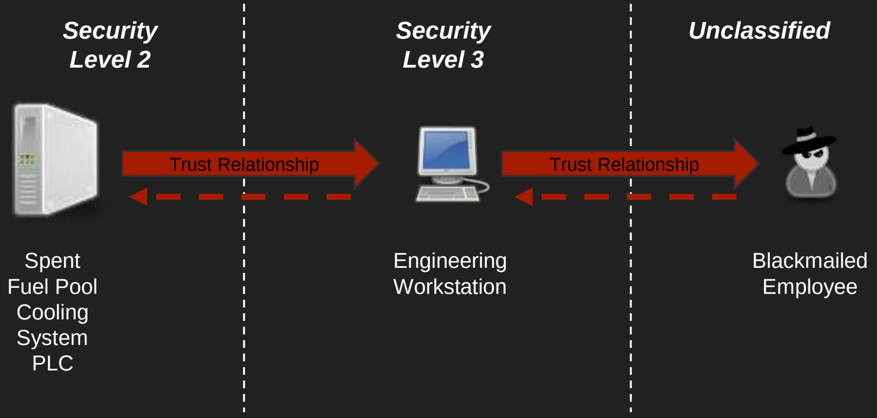
- The strong jargon in computer security comes off as spreading fear, uncertainty, and doom.
- No tool for defining a computer-security scenario escapes the above.
- We as computer security practitioners do not know all of the information held by individuals who are immersed in the problem spaces we're protecting.
- Computer-based systems always support larger ***systems*** providing ***functions***.
    - We protect the ***function***, not the computer.
- We need to be able to capture these relationships and then build on them.



DCSA for the Asherah Hypothetical Facility

Why I Believe This Works?

- You can ask anyone about what they and the ***systems*** they own trust. This allows advanced computer security scenarios to be expressed despite reducing the requirement technical specificities.
  - Without this we are artificially limited.
- In a cyber-attack the goal of an adversary is to use your ***systems*** against you to exploit further trust relationships (TR) until they compromise the desired ***function***
  - All ***threat actions*** can be pre-defined against trust relationships
  - Only adversarial elements undertake ***threat actions***
- *It is possible to compute all possible scenario permutations.*



Lexicon

Elements: people, information, applications, digital components, computers.

Security Measures: Measures preserving a TR.

Threat Actions: Actions compromising a TR.

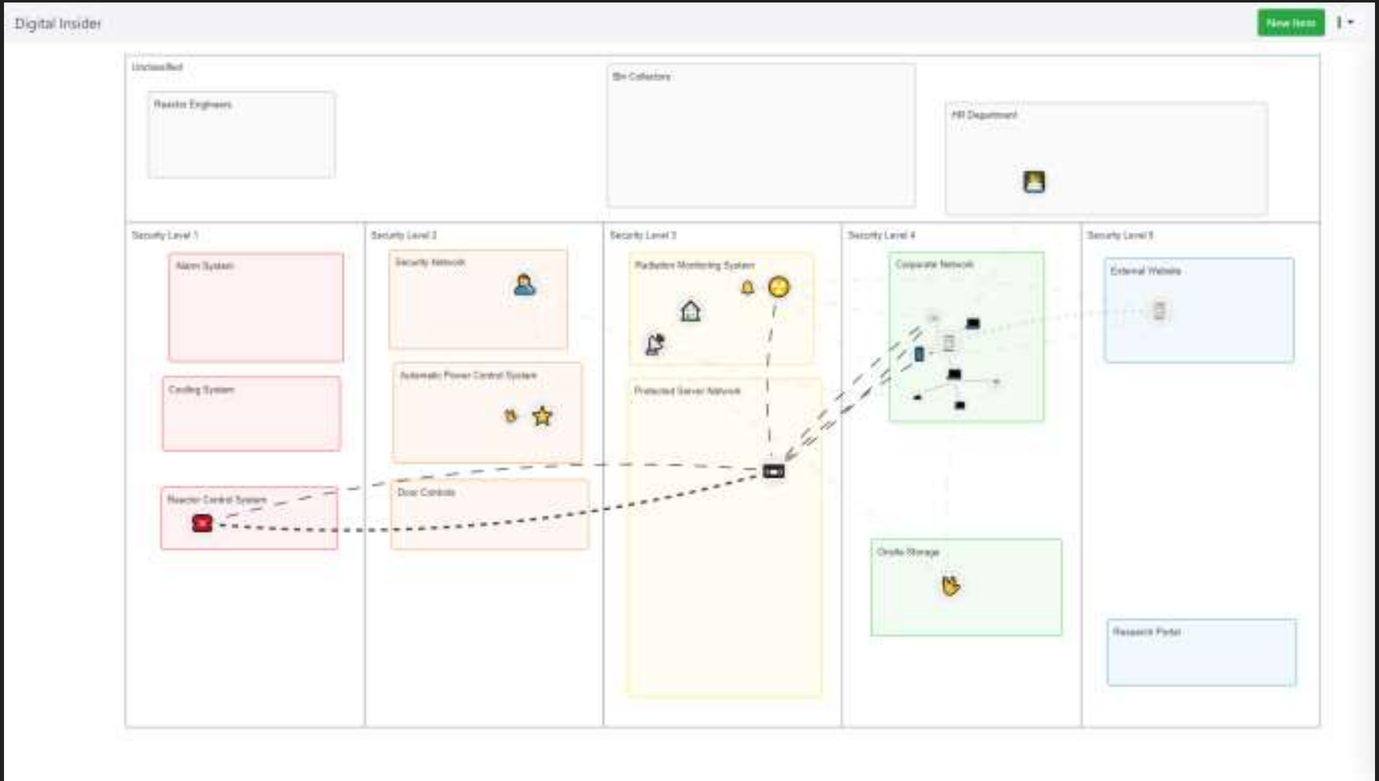
Expressing the Scenario as a Data Structure (YAML)

```
---
name: sfpcs-plc
computer-based: true
adversarial: false
description: “The PLC providing control of
setpoints for the Spent Fuel Pool plant”
platform: Siemens
function: cooling-spent-fuel
parent:
zone: plant-control
trust-relationships:
  - engineering-workstation:
      description: “The engineering
workstation has access through the SL2
firewall to update the PLC”
      security-measures:
        - password-protected:
            Description: “A password is
required to update the application logic”
      threat-actions:
        - change-plc-logic:
            description: “modify PLC logic to
cause a compromise of the function”
            security-measure:
              - sfpcs-programming-password
```

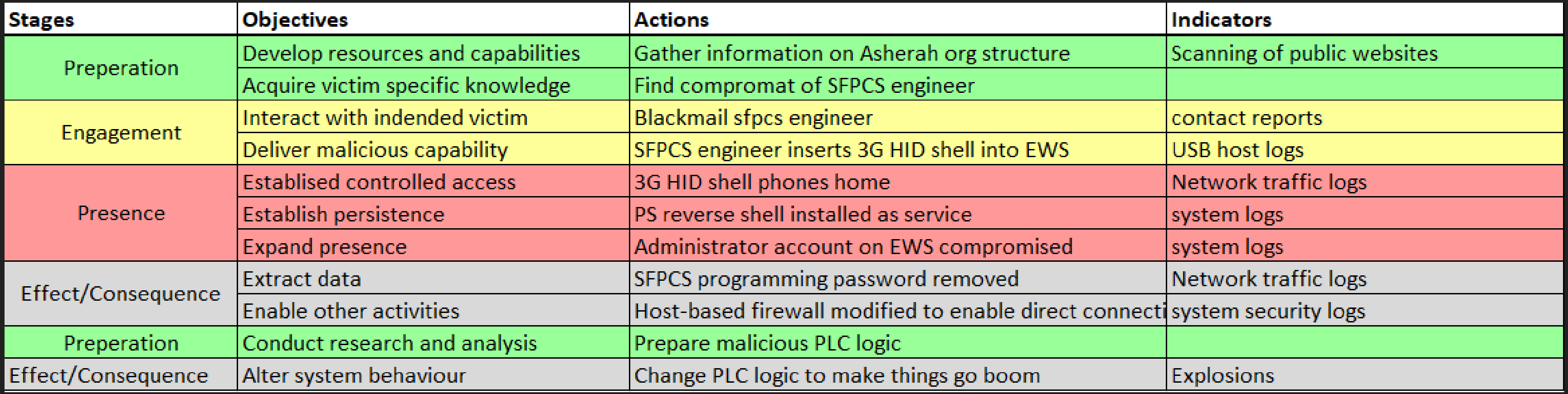
```
---
name: engineering-workstation
computer-based: true
adversarial: false
description: “The primary engineering
workstation for accessing plant systems”
platform: Windows
function:
parent:
zone: engineering-services
trust-relationships:
  - plant-engineer:
      actions:
        - unauthorised-use
---
name: sfpcs-programming-password
description: “The password to update the
SFPCS PLC application logic”
...
parent: engineering-workstation
zone: inherited
trust-relationships:
  - engineering-workstation:
      threat-actions:
        - recover-plaintext-password
```

```
---
name: sfpcs-engineer
computer-based: false
adversarial: true
description: “An engineer trained and
authorised to configure setpoints for the
spent fuel pool cooling system”
trust-relationships:
  - external-bad-guy:
      threat-actions:
        - blackmail
```

Proof of Concept Application

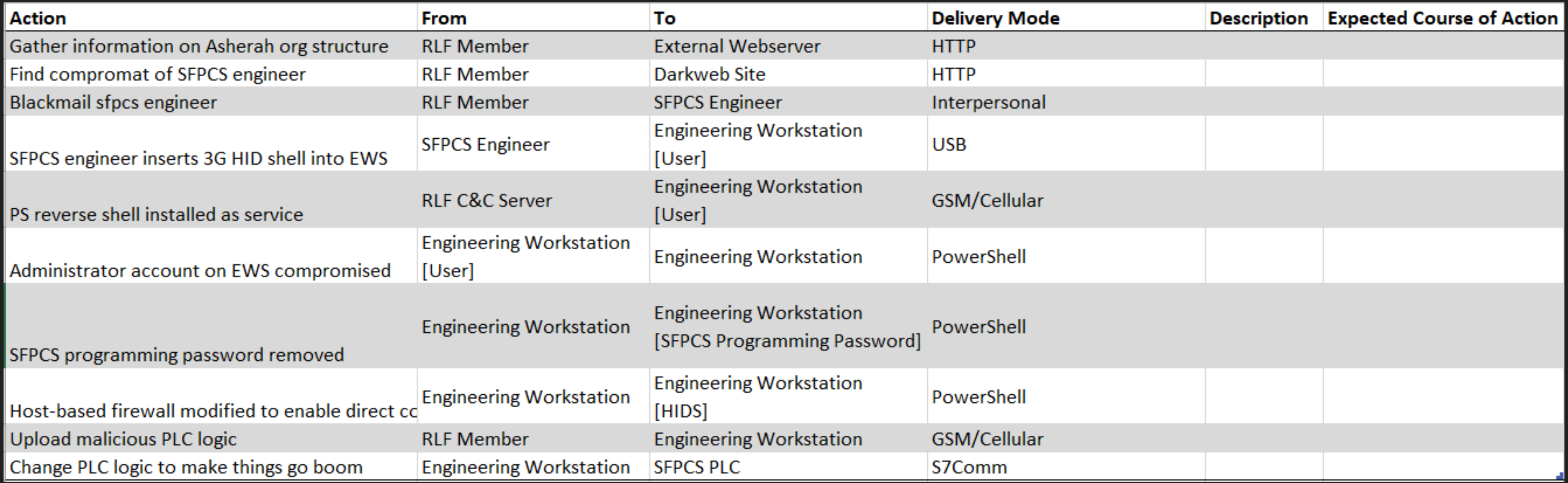


CTF Progression (Intended)



Stages	Objectives	Actions	Indicators
Preperation	Develop resources and capabilities	Gather information on Asherah org structure	Scanning of public websites
	Acquire victim specific knowledge	Find compromat of SFPCS engineer	
Engagement	Interact with indended victim	Blackmail sfpcs engineer	contact reports
	Deliver malicious capability	SFPCS engineer inserts 3G HID shell into EWS	USB host logs
Presence	Establised controlled access	3G HID shell phones home	Network traffic logs
	Establish persistence	PS reverse shell installed as service	system logs
	Expand presence	Administrator account on EWS compromised	system logs
Effect/Consequence	Extract data	SFPCS programming password removed	Network traffic logs
	Enable other activities	Host-based firewall modified to enable direct connecti	system security logs
Preperation	Conduct research and analysis	Prepare malicious PLC logic	
Effect/Consequence	Alter system behaviour	Change PLC logic to make things go boom	Explosions

MSEL (Intended)



Action	From	To	Delivery Mode	Description	Expected Course of Action
Gather information on Asherah org structure	RLF Member	External Webserver	HTTP		
Find compromat of SFPCS engineer	RLF Member	Darkweb Site	HTTP		
Blackmail sfpcs engineer	RLF Member	SFPCS Engineer	Interpersonal		
SFPCS engineer inserts 3G HID shell into EWS	SFPCS Engineer	Engineering Workstation [User]	USB		
PS reverse shell installed as service	RLF C&C Server	Engineering Workstation [User]	GSM/Cellular		
Administrator account on EWS compromised	Engineering Workstation [User]	Engineering Workstation	PowerShell		
SFPCS programming password removed	Engineering Workstation	Engineering Workstation [SFPCS Programming Password]	PowerShell		
Host-based firewall modified to enable direct cc	Engineering Workstation	Engineering Workstation [HIDS]	PowerShell		
Upload malicious PLC logic	RLF Member	Engineering Workstation	GSM/Cellular		
Change PLC logic to make things go boom	Engineering Workstation	SFPCS PLC	S7Comm		

Note

All models are flawed, some are useful.

Hopefully this fits into the latter category.

Thank You ☺

M.Hewes@iaea.org