



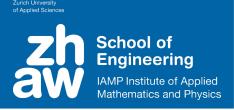
# Integration of Security into the STAMP based Safety Analysis Method CAST

**Carmen Frischknecht-Gruber, Mario Marti** 

**Supervisor Sven Stefan Krauss Christoph Senn, Benjamin Contreras** 

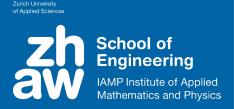
**ZHAW Zurich University of Applied Sciences, Switzerland** 

### **Outline**





### **Outline**





#### Zurich University of Applied Science

#### Introduction





#### **Background**

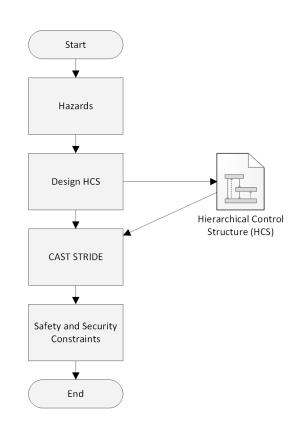
- Zurich University of Applied Sciences
- Institute of Applied Mathematics and Physics

#### **Research Objectives**

- Integrate security aspects into a safety analysis method
- Show feasibility of integrating a security method into CAST

#### **Talk Focus**

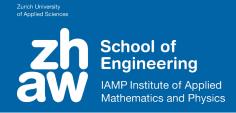
- CAST-STRIDE Approach
- Application of method using a case study



#### Note:

We use the word method, although CAST and STRIDE are actually techniques. Due to the frequent use in the field of safety we will use the terminology method.

# Why Security in Safety Analysis?





#### Jeep Cherokee Hack 2015



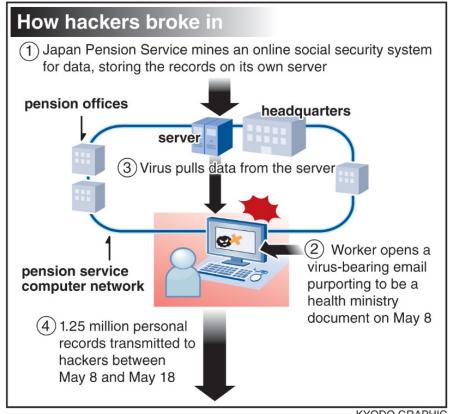
Andy Greenberg/Wired <a href="https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/">https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/</a>

# Why Security in Safety Analysis?



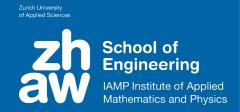


#### Japan Pension Service Hack



https://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.WhVGN0riZaQ

# Why Security in Safety Analysis?





#### WannaCry ransomware attack 2017

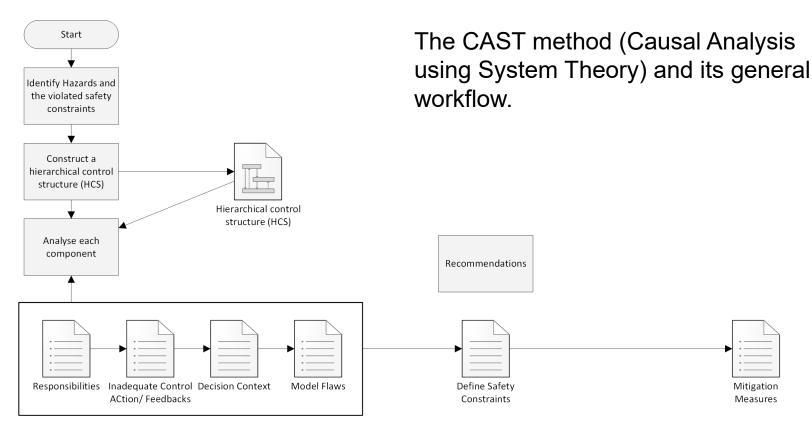


http://www.bbc.com/news/uk-40995121

#### **CAST** in a nutshell







#### Zurich University of Applied Sciences

#### STRIDE in a nutshell



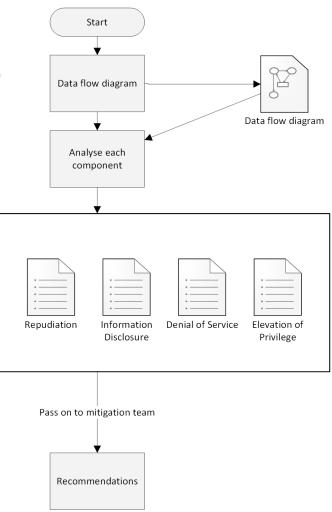


The general workflow of STRIDE, a threat classification model.

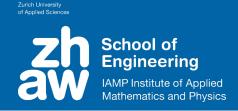
**STRIDE** 

Spoofing

**Tampering** 



### STRIDE in a nutshell



Name of Threat	Violated Security Property	Short Description
Spoofing identity	Authentication	Pretending to be something different than yourself.
Tampering with Data	Integrity	Modification of data either on the system or in transfer over the network.
Repudiation	Non-Repudiation	Denial of responsibility. Related to logging of actions happening in the system.
Information disclosure	Confidentiality	Disclosure of information to an unauthorized party.
Denial of Service	Availability	Absorption of system resources.
Elevation of	Authorization	Performing actions without the
Privilege		appropriate privileges needed to do so.

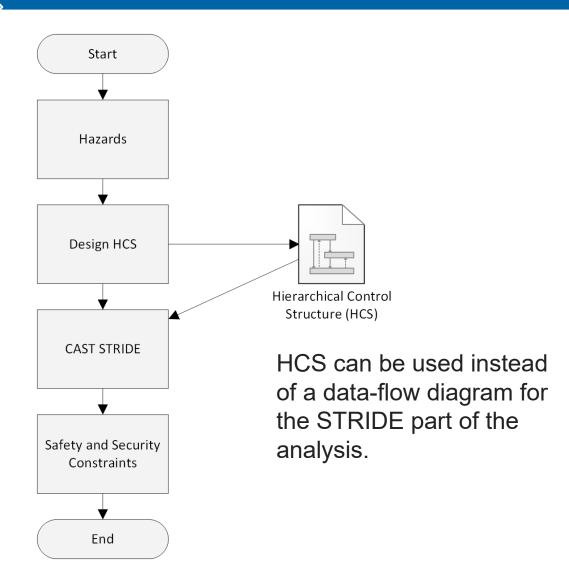
#### Zurich University of Applied Science

# **CAST-STRIDE Approach**



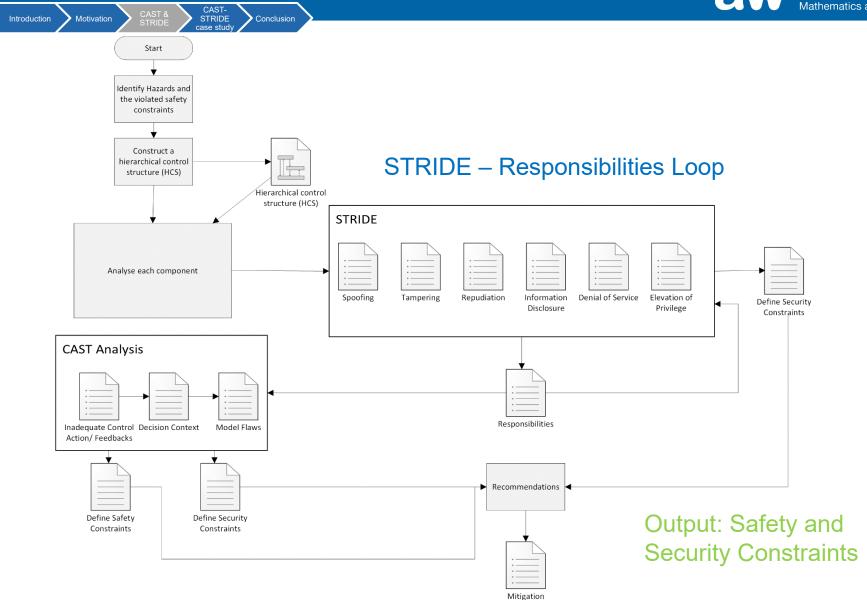


General workflow of the CAST-STRIDE method.



# **CAST-STRIDE Approach**



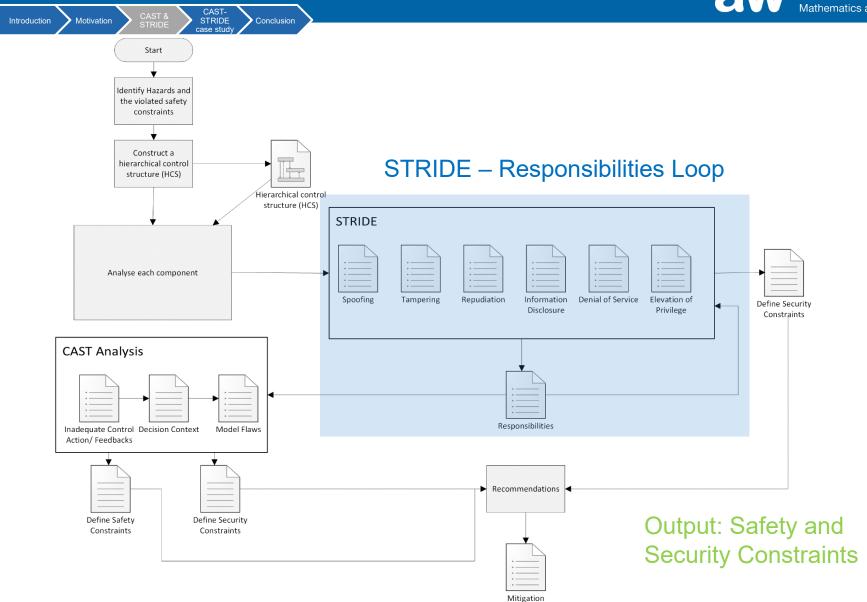


Measures



# **CAST-STRIDE Approach**



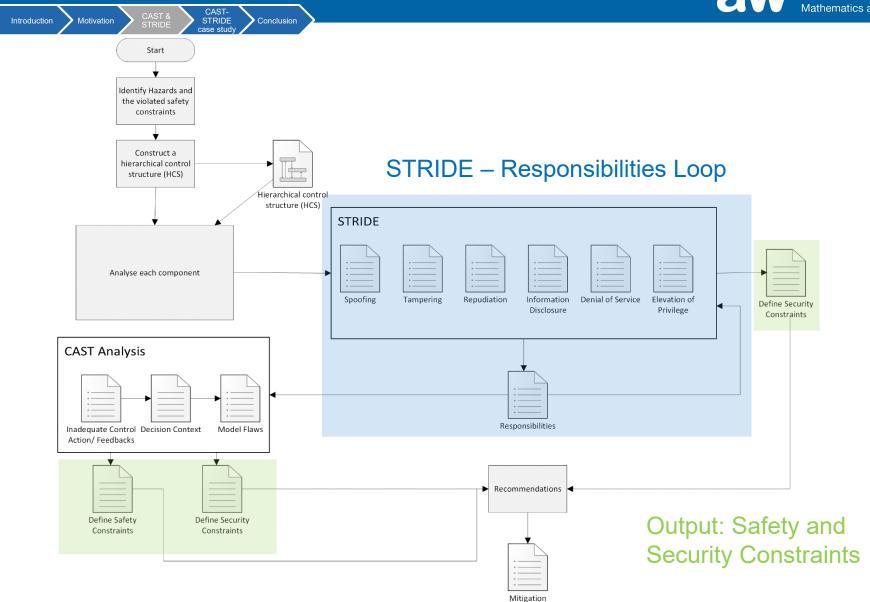


Measures



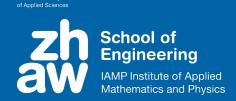
# **CAST-STRIDE Approach**





Measures

### **WannaCry**





#### Incident

- WannaCry ransomware attack affected over 150 countries.
- More than 230'000 devices.
- In May 2017



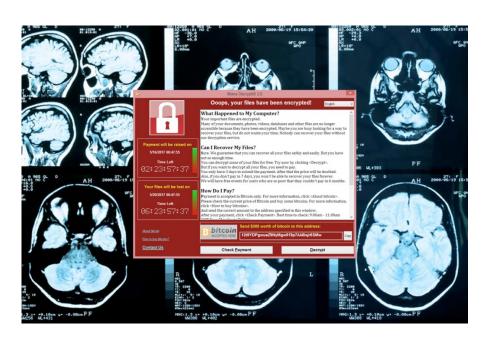
### **WannaCry**





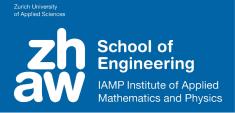
#### Incident

- National Health Service (NHS) in the UK was badly hit
- At least 6900 appointments had to be cancelled.
- Approximately 40 NHS trusts and their hospitals were affected.
- At least 6900 appointments had to be cancelled



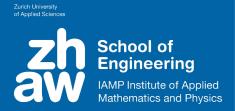
https://www.telemedicineclinic.com/blog/wannacry-ransomware-hits-nhs-fails-interrupt-tmc-service/

### **Hazards**



Hazard	Safety Constraint	Violated Safety Constraint
System fails	System must be recoverable within time	37 trusts were infected
	constraints.	(including 27 acute trusts)
No access to data	Data must be accessible within time	Unknown number of NHS
	constraints.	organisations unable to access
	Data must be recoverable within time	records because they shared
	constraints.	data or systems with an infected
		trust.
		Unknown number of trusts or
		GPs that were delayed in
		receiving information, such as
		test results, from infected trusts
		595 practices infected and
		locked out of devices.

### **Hazards**

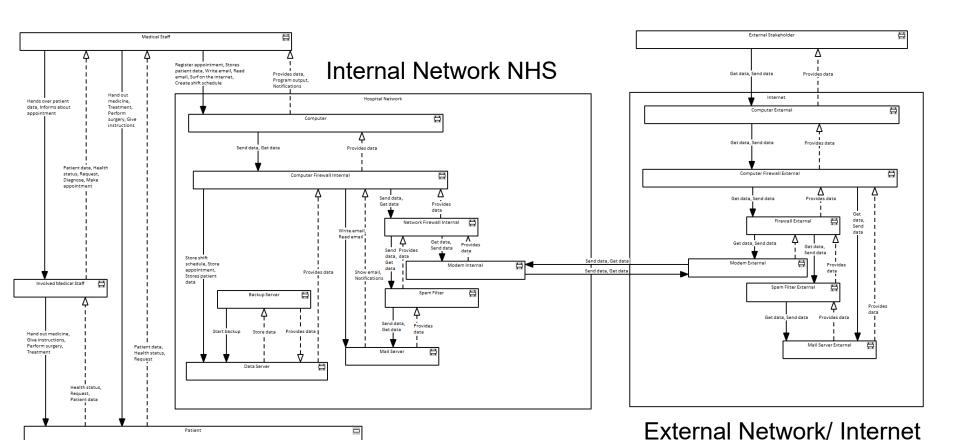


Hazard	Safety Constraint	Violated Safety Constraint
Appointments	Data must be accessible within time constraints.	At least 6912 appointments and
must be cancelled	Data must be recoverable within time	an estimated 19'494
	constraints.	appointments had to be
		cancelled.
Emergency cases	Operating system and software of diagnostic	Five accident and emergency
	equipment must be up to date.	departments were unable to treat
	Data must be accessible within time constraints.	patients.
	Data must be recoverable within time	1220 diagnostic equipment,
	constraints.	which had been infected.
Communication	Alternate communication methods must be	They weren't able to send MRI
paths not	provided.	scans to clinicians treating
accessible	Original communication path must be recovered	patients in other parts of the
	within time constraints.	hospital. 1% of devices in use.

School of Engineering

IAMP Institute of Applied Mathematics and Physics

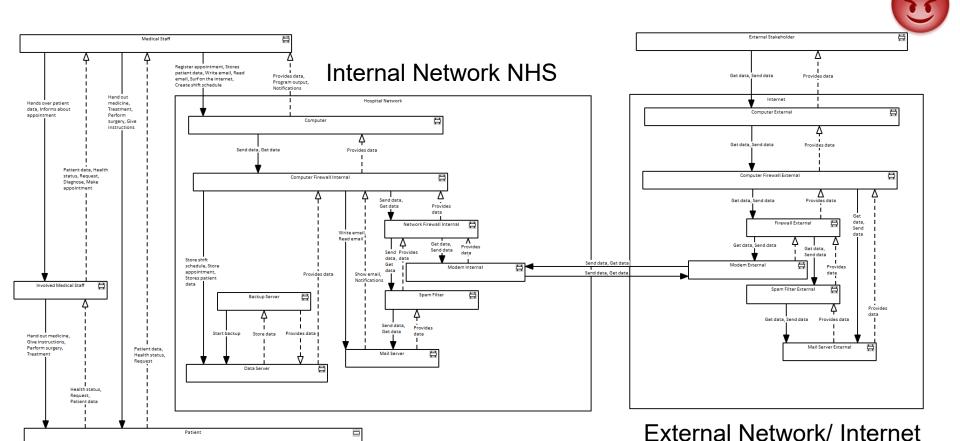




**Controlled Process** 





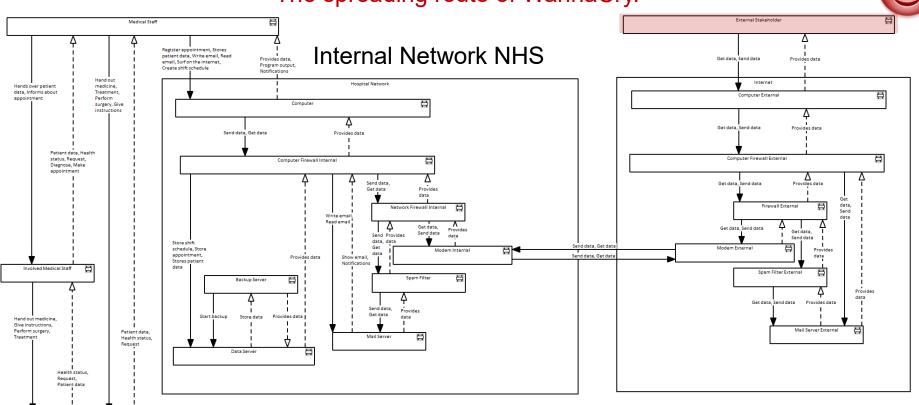


**Controlled Process** 





#### The spreading route of WannaCry.



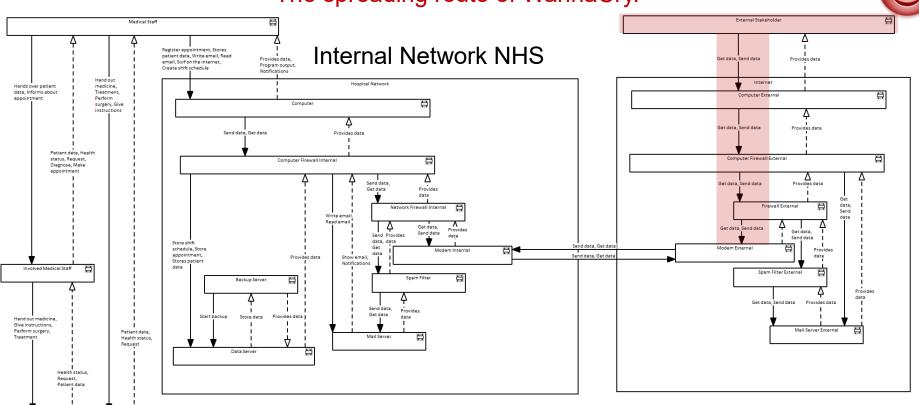
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.



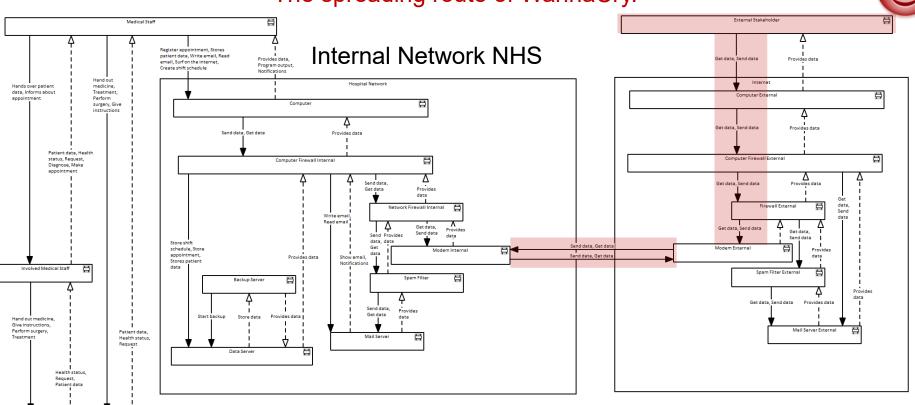
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.



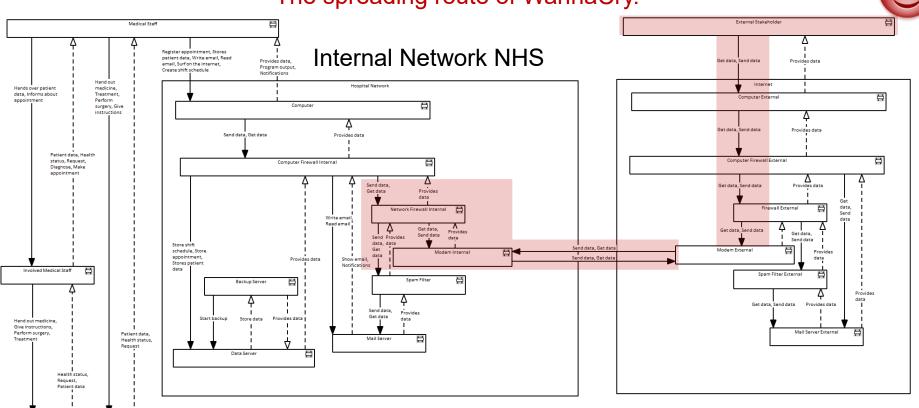
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.



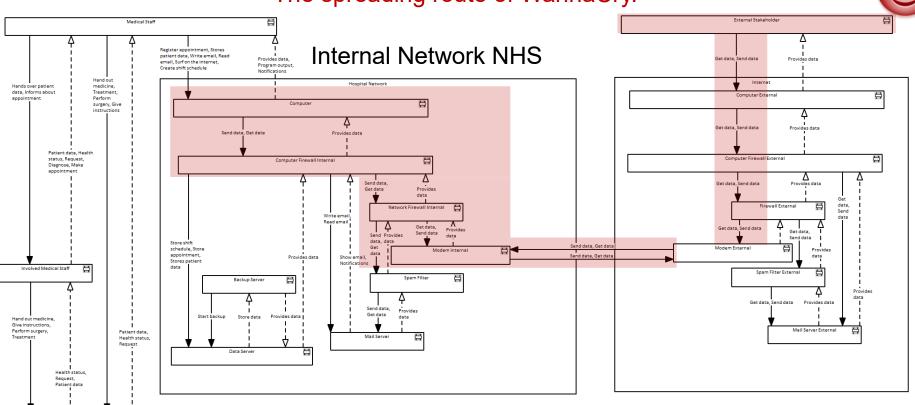
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.



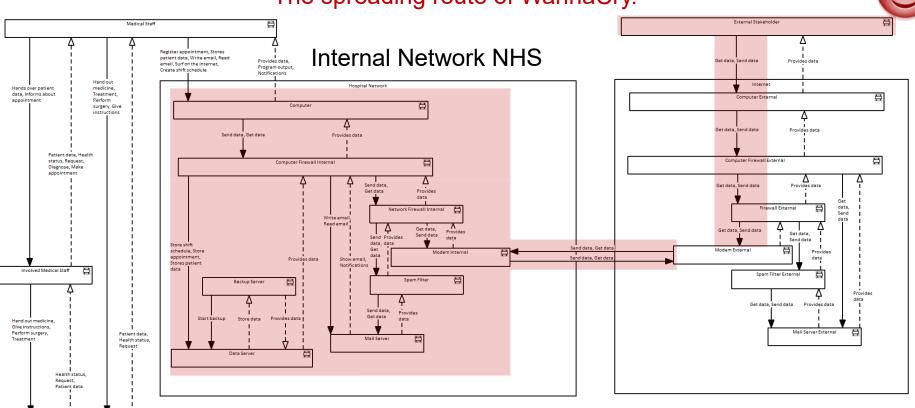
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.



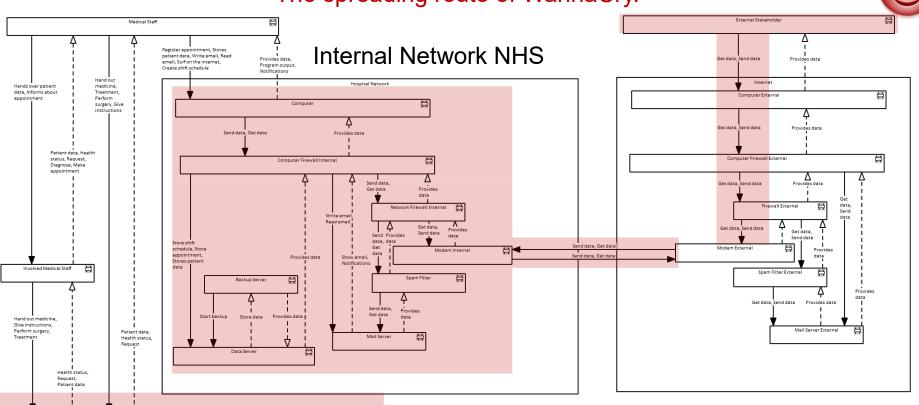
External Network/ Internet

**Controlled Process** 





#### The spreading route of WannaCry.

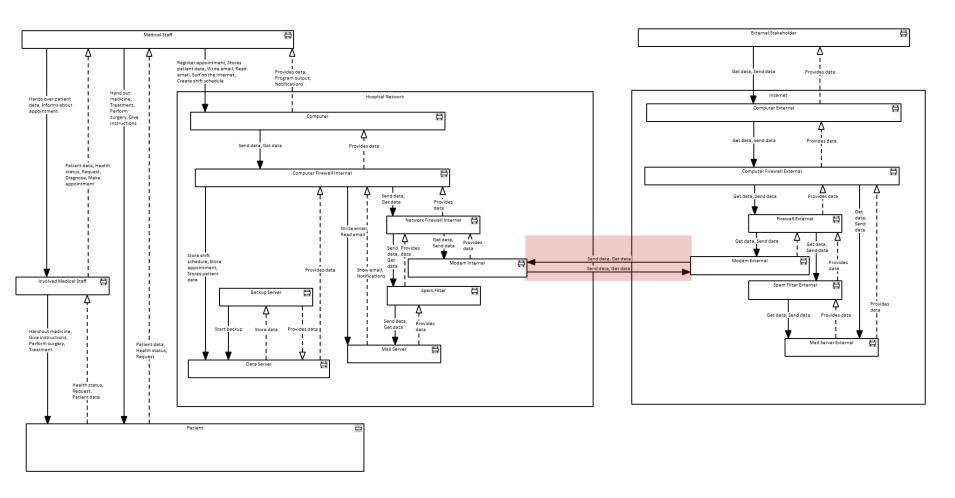


External Network/ Internet

**Controlled Process** 

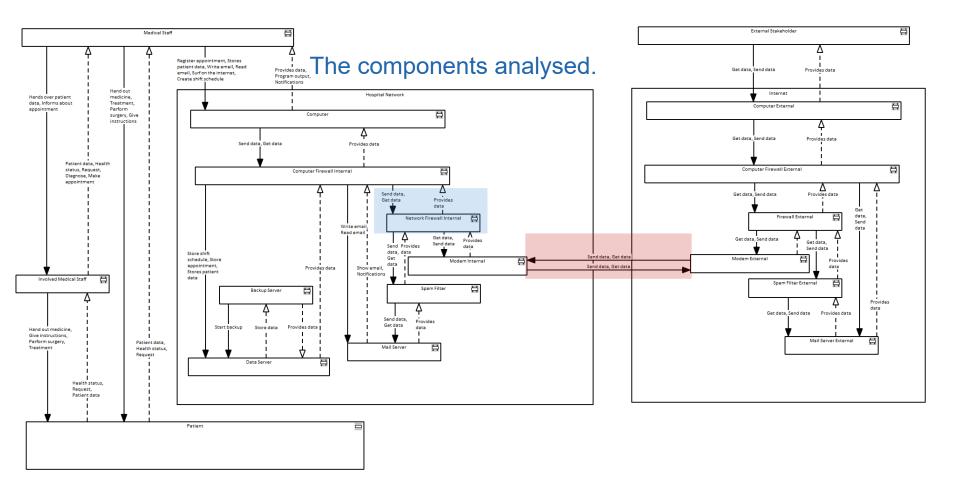






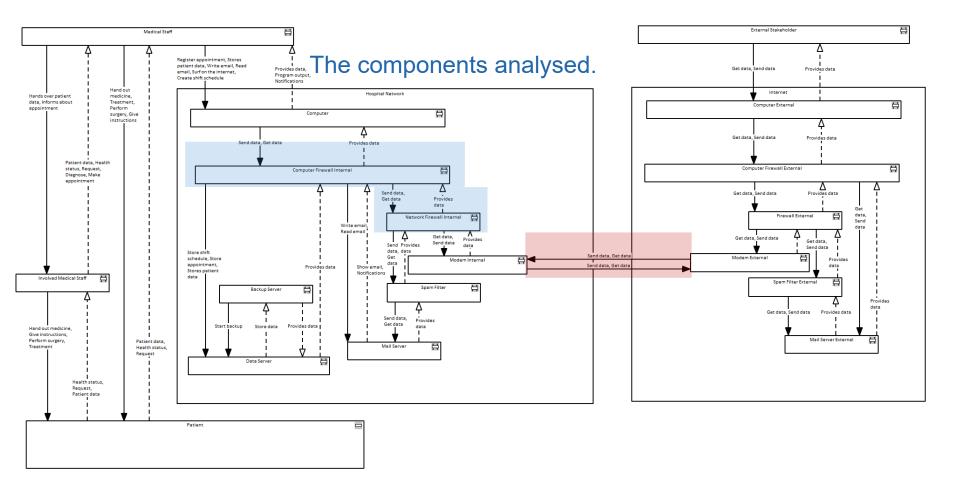






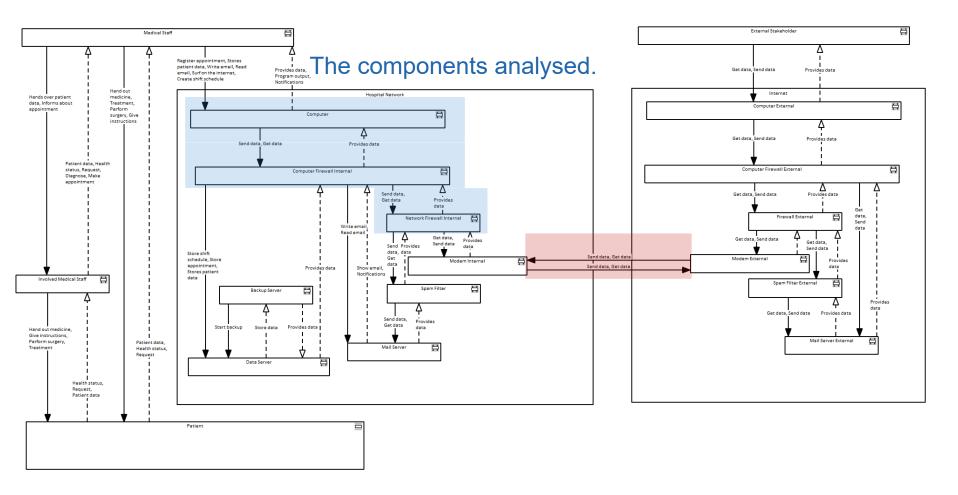




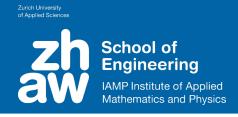






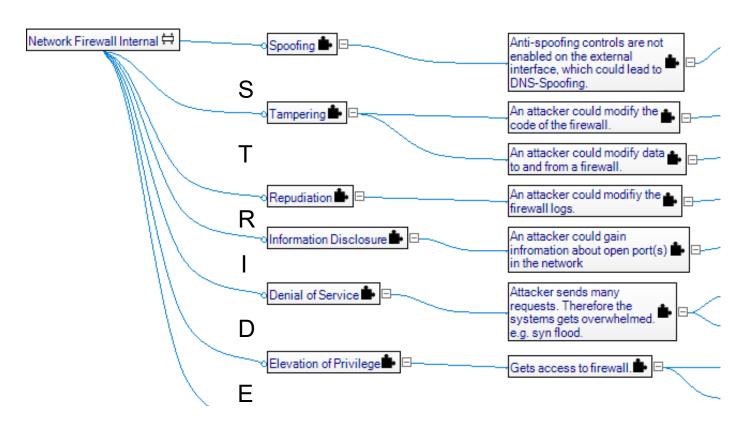


#### 1. STRIDE

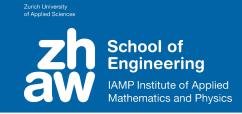




#### After the HCS is made the actual analysis starts with STRIDE.

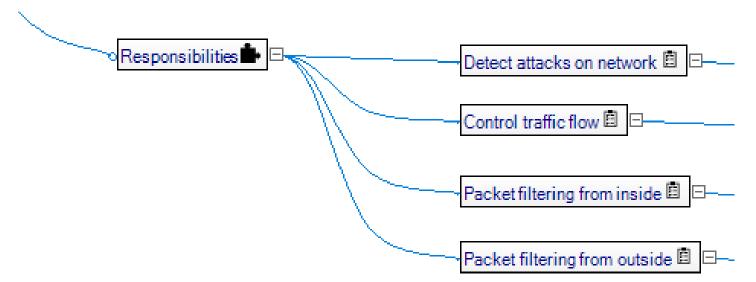


### 2. Responsibilities

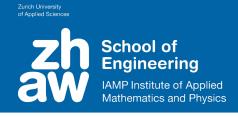




Afterwards the responsibilities are identified.

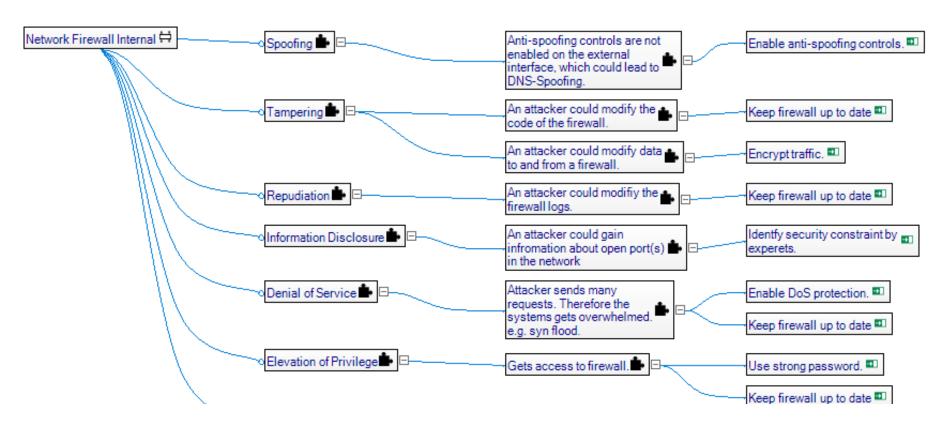


#### 3. Reiterate





#### Reiterate this steps to complete STRIDE and responsibilities.

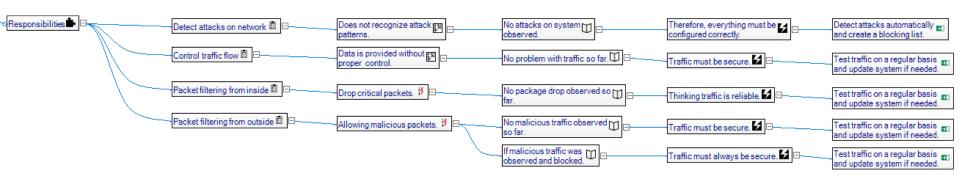


# 4. Finish CAST Analysis

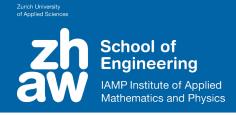




#### Finish Analysis:



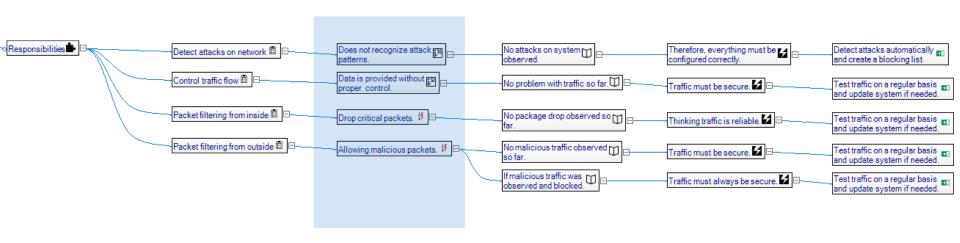
# 4. Finish CAST Analysis



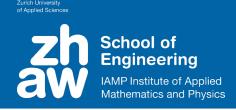


#### Finish Analysis:

Inadequate Control Actions & Inadequate Feedbacks



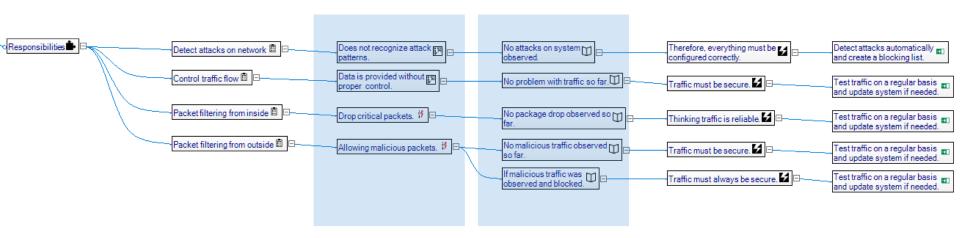
### 4. Finish CAST Analysis



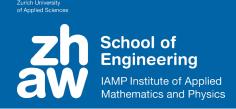


### Finish Analysis:

- Inadequate Control Actions & Inadequate Feedbacks
- Context Decision



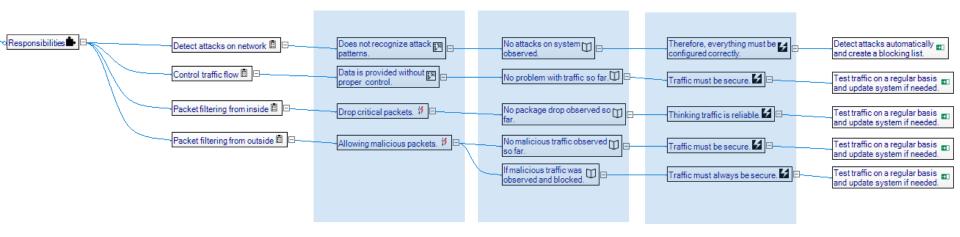
### 4. Finish CAST Analysis



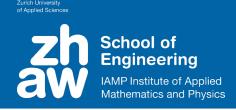


### Finish Analysis:

- Inadequate Control Actions & Inadequate Feedbacks
- Context Decision
- Model Flaw



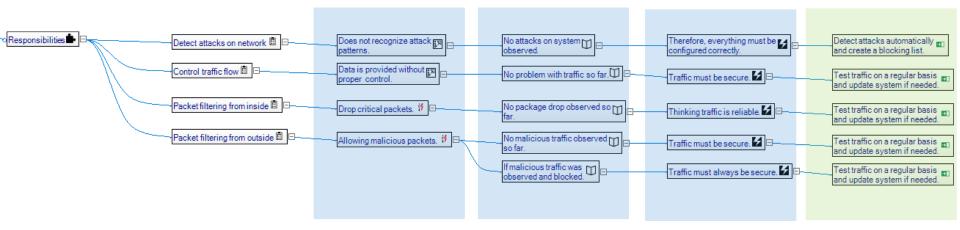
### 4. Finish CAST Analysis





### Finish Analysis:

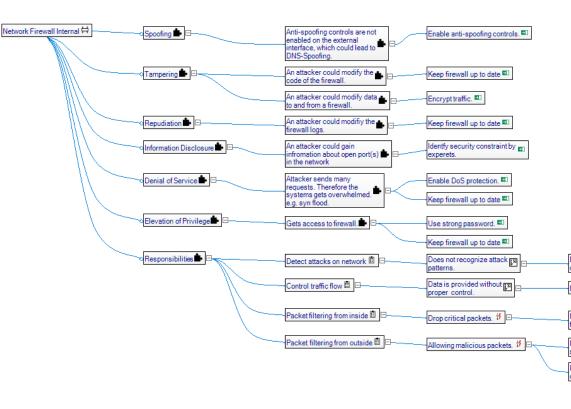
- Inadequate Control Actions & Inadequate Feedbacks
- Context Decision
- Model Flaw
- Safety and Security Constraints

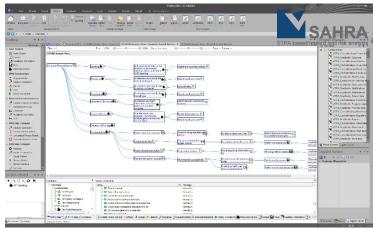






### Full View of Network Firewall Internal Analysis





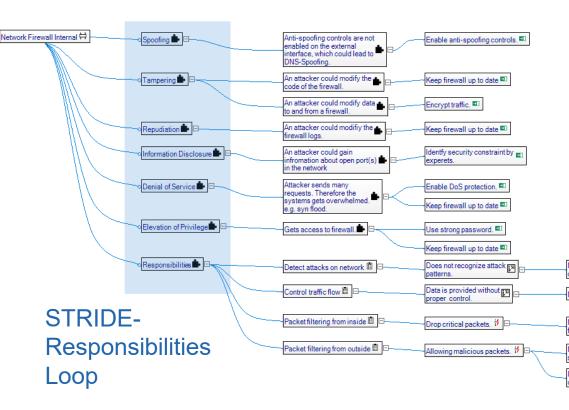
Modelled in Enterprise Architect with SAHRA.

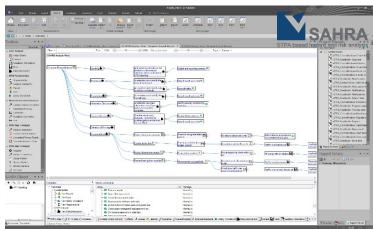






#### Full View of Network Firewall Internal Analysis





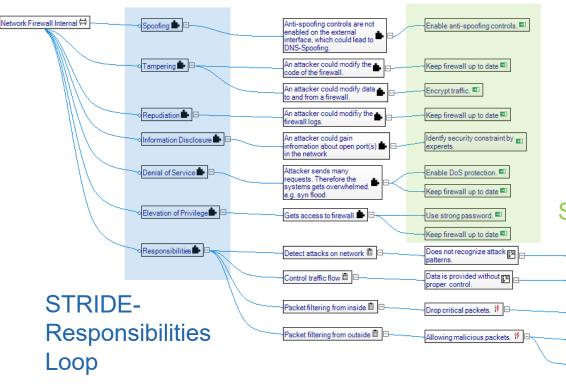
Modelled in Enterprise Architect with SAHRA.

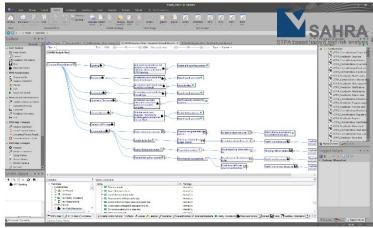






### Full View of Network Firewall Internal Analysis

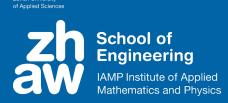


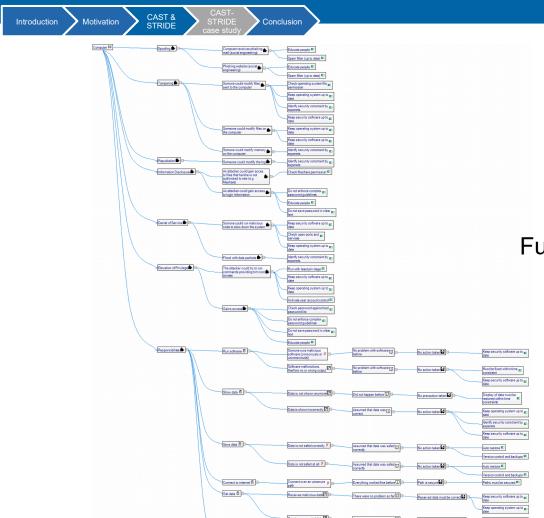


Modelled in Enterprise Architect with SAHRA.

### Safety and Security Constraints







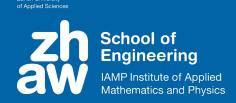
Send data 🖺 E

Sends corrupted data If

There were no problems so far 🛈 🖯

Full Computer Analysis View

## **Conclusion CAST-STRIDE Analysis**



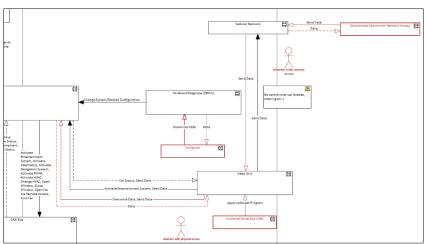


#### Results

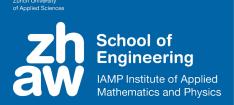
- Iterative process
- Helps to find responsibilities, which leads to more output
- Structured procedure
- Helpful guide through analysis

#### **Outlook**

- Verify CAST-STRIDE framework
- Execute case study from different groups Small section from the Jeep Cherokee analysis.
- Re-analysis of case study after improvement
- Try to use STRIDE in STPA to analyse a whole system
- Prioritization of constraints?



## The Safety Critical Systems (SKS) Research Team

















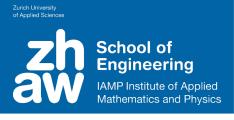
www.sahra.ch



www.anzen-solutions.ch

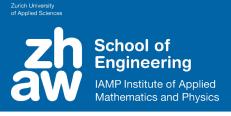


http://www.iamp.zhaw.ch/sks



## Questions?

ご清聴ありがとうございました

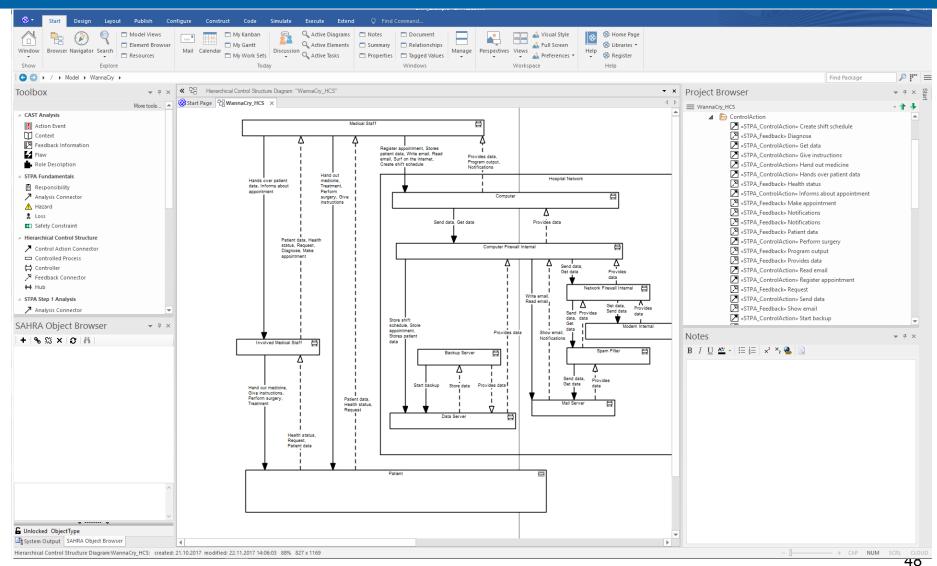


## **Appendix**

#### Zurich University of Applied Scien

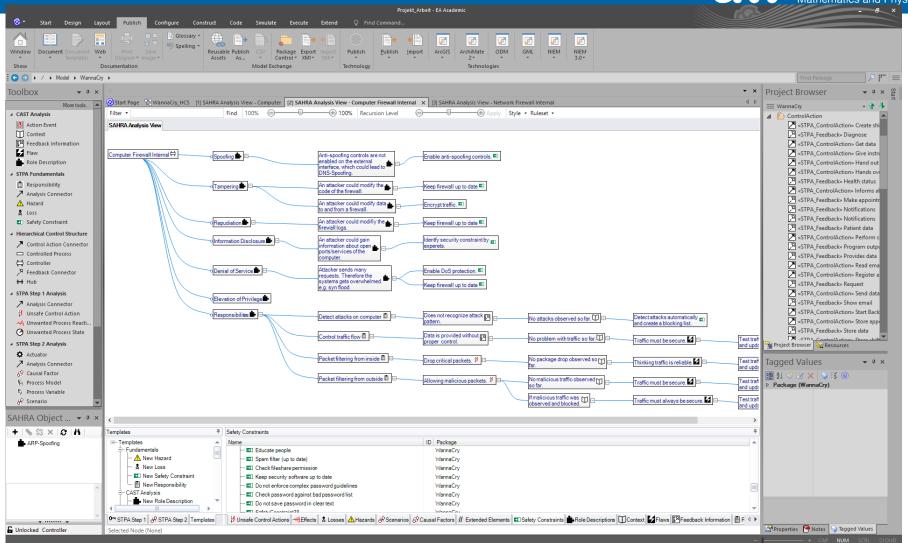
## School of Engineering IAMP Institute of Applied Mathematics and Physics

### **SAHRA** – Enterprise Architect Extension



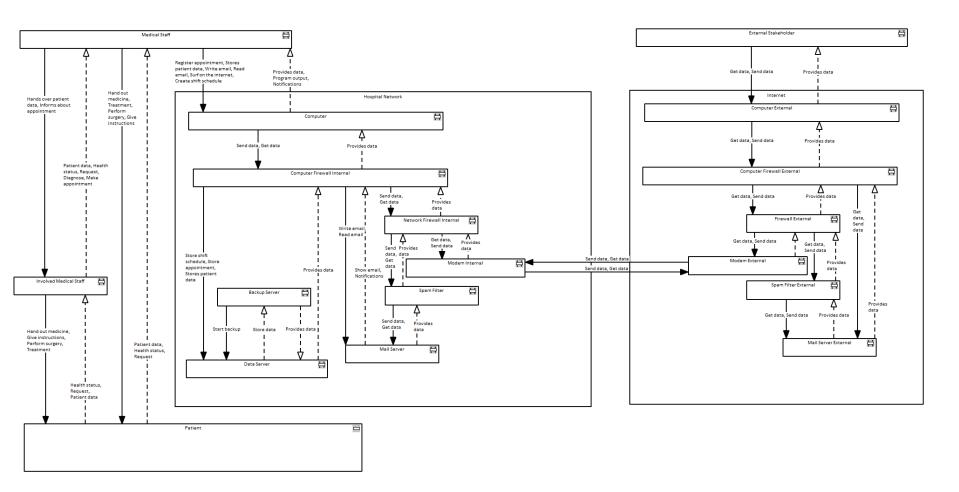
### **SAHRA** – Enterprise Architect Extension





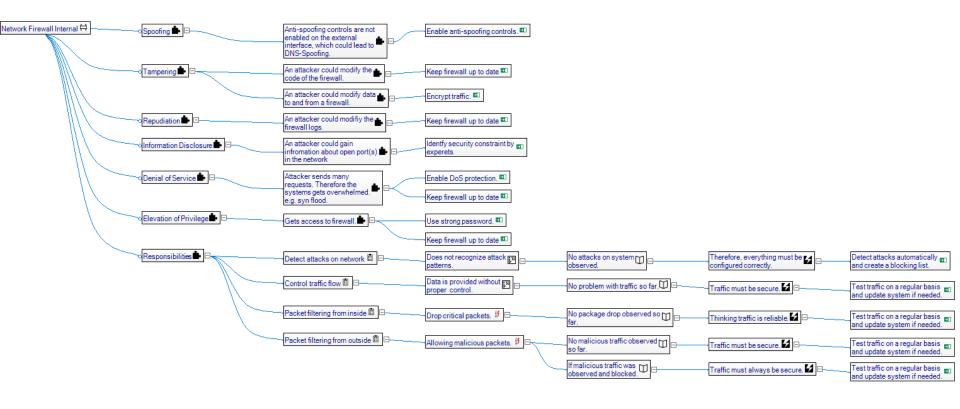
## WannaCry HCS



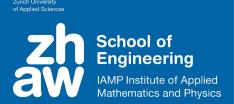


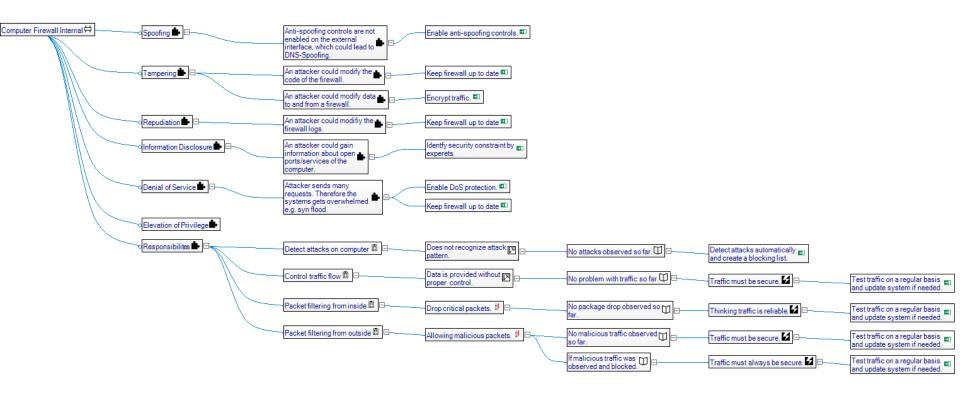
## WannaCry Network Firewall Internal Analysis



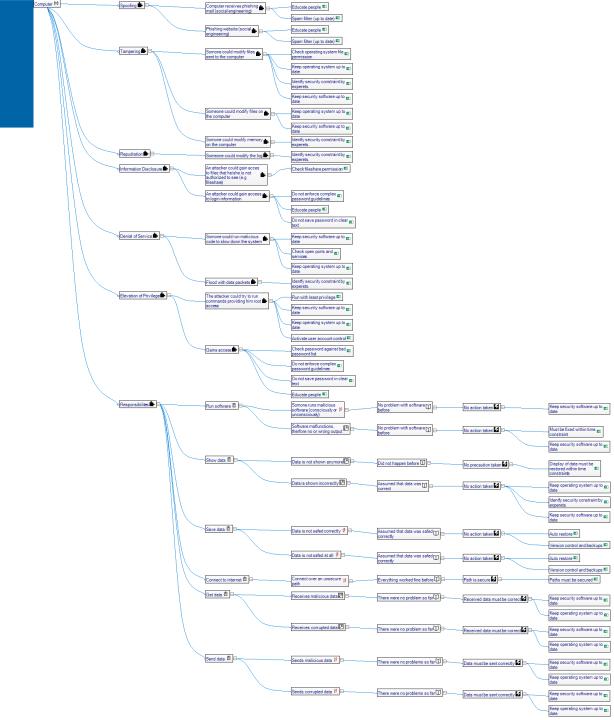


# WannaCry Computer Firewall Internal Analysis

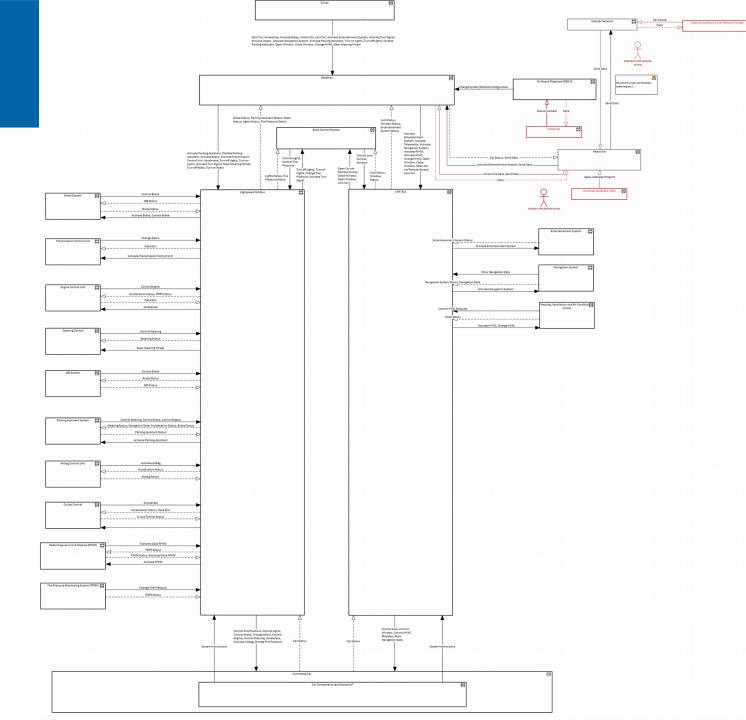




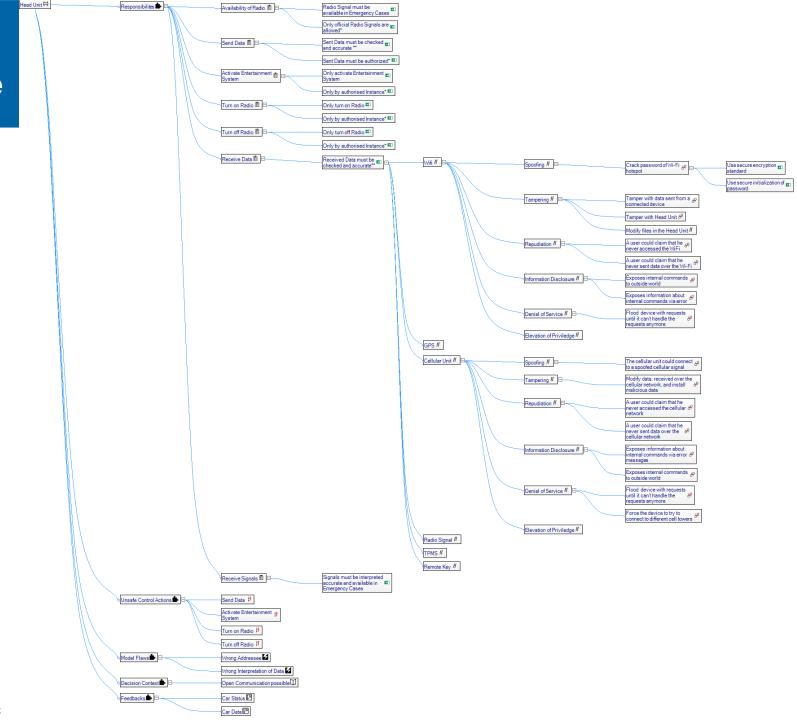
## Computer



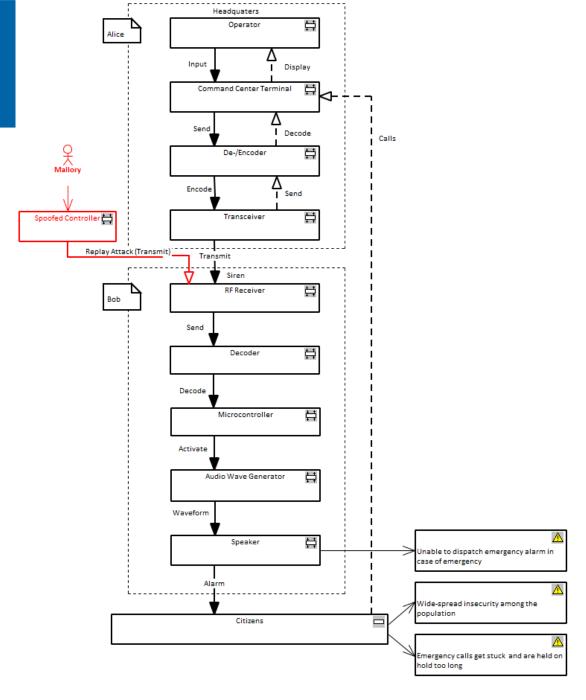
## Jeep Cherokee

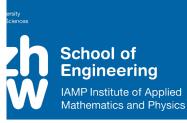


### Jeep Cherokee



### Siren Dallas





56

## Siren Dallas

