CAST-STRIDE
An approach of bringing safety and security together

Zurich University of Applied Sciences ZHAW, Switzerland

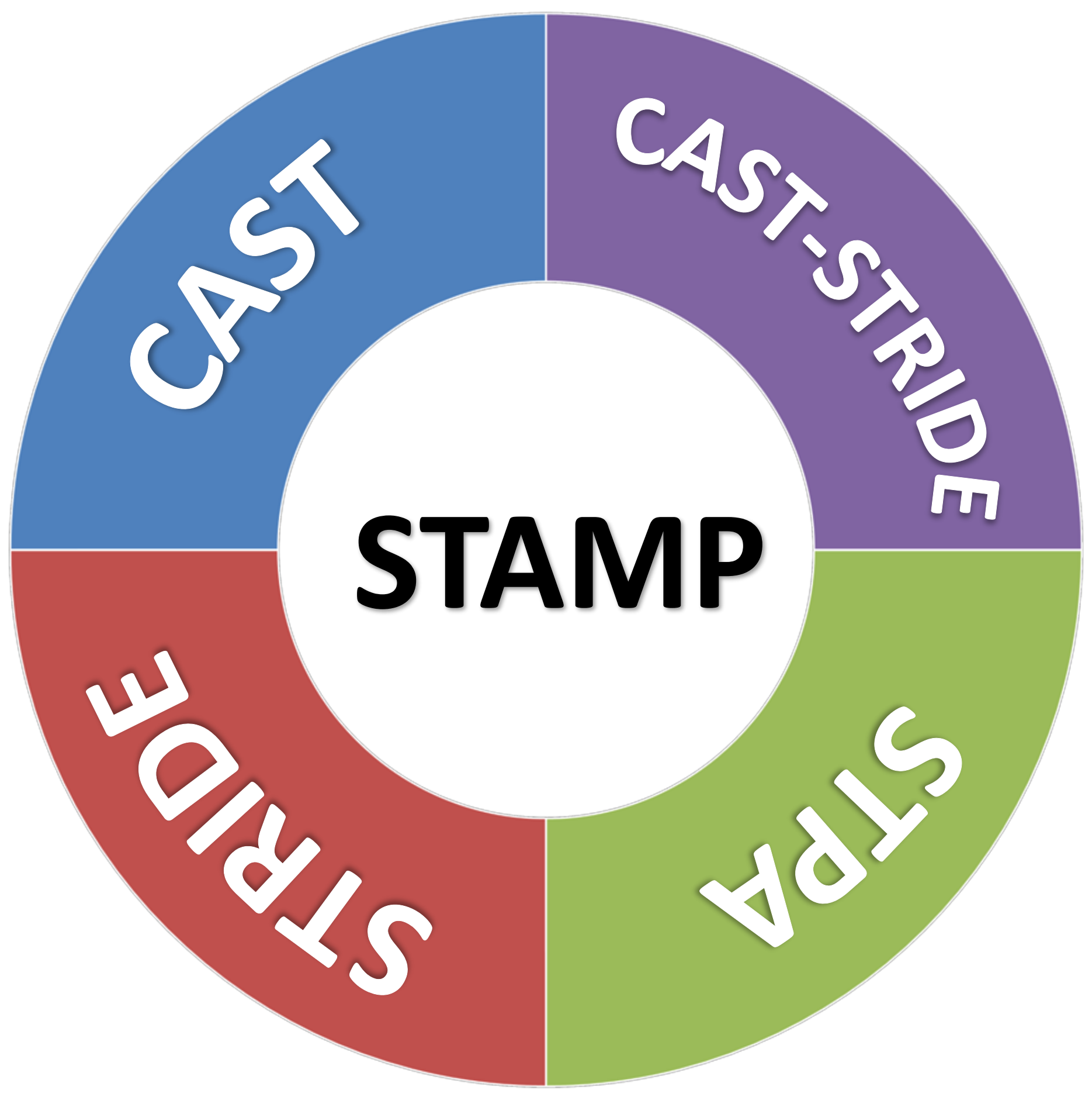
Carmen Frischknecht-Gruber, Mario Marti and Sven Stefan Krauss

Abstract

Due to increasingly complex systems, the demand for safety and security has grown. Even though both fields, safety, and security, aim to create safe, reliable and secure systems, they are treated as different domains. Thus, the positive effect on systems created when methodologies of both domains are applied is probably underestimated. The main objective of this work is to integrate security aspects into the STAMP technique CAST. Therefore, the incident from Dallas in spring 2017, in which a signal spoof attack set off the city's emergency sirens, was used as a case study to evaluate if CAST can be applied for security incident analysis. We were also analysing the issue with security vulnerabilities of modern cars applying a CAST analysis, a security-based analysis and a combination of both on the Jeep Cherokee model. Based on the results we show the feasibility of the developed analysis framework combining methods from safety and security. As a third case study, we analysed the WannaCry ransomware attack, which was used as a feasibility example.

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 Privilege	Authorization	Performing actions without the appropriate privileges needed to do so.

Explanation of the STRIDE keywords [1].

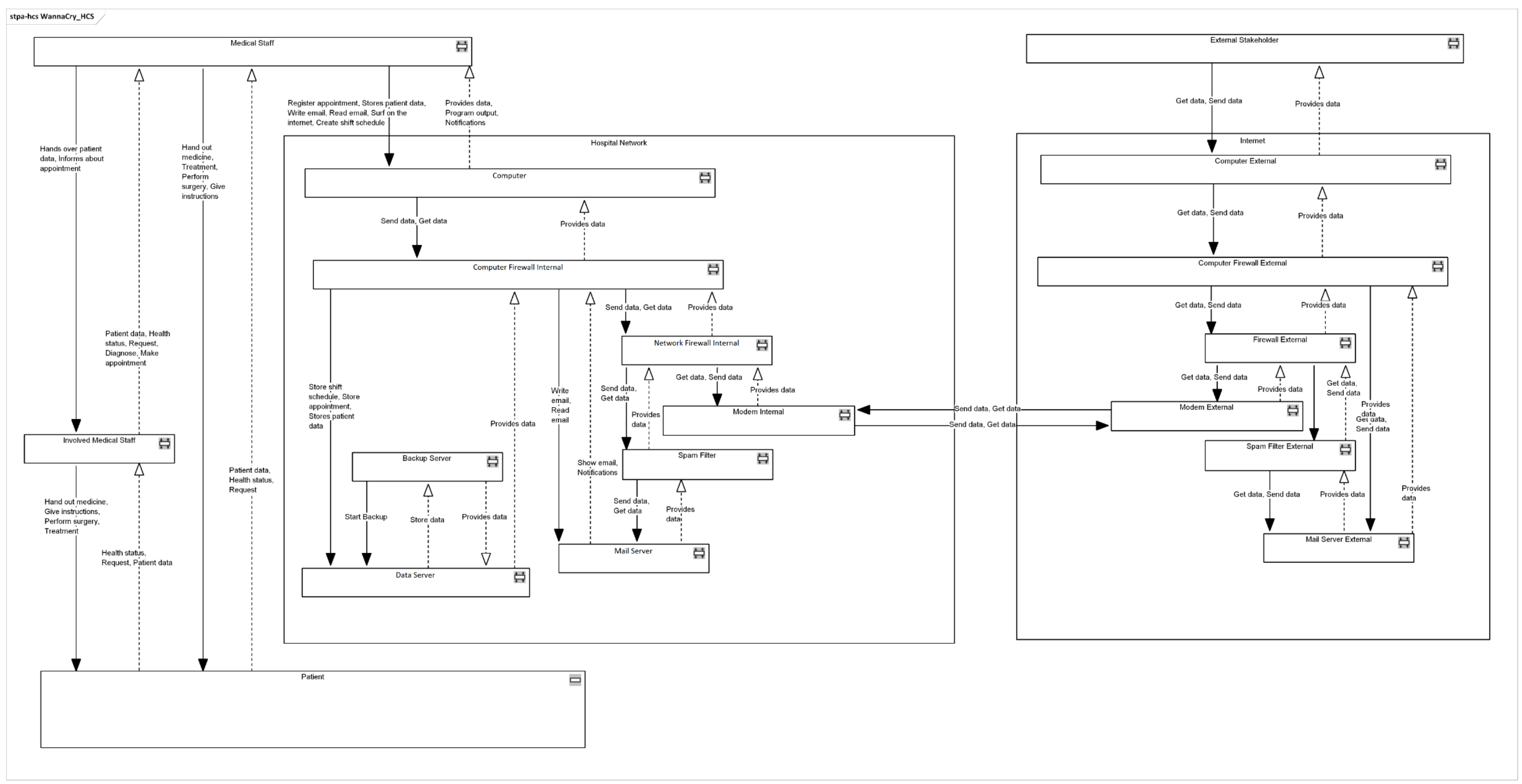


Case Study WannaCry

The WannaCry ransomware attack affected over 150 countries and infected more than 230'000 devices in May 2017, the worst hit was the NHS in the UK. Approximately 40 NHS trusts and their hospitals were affected [2]. At least 6900 appointments had to be cancelled. In some cases, operations could not be performed and five emergency departments were unable to care for all patients. A lot of information, such as patient data and test results were not accessible. The attack was spread worldwide by phishing emails, and the malware could spread from machine to machine within networks. At first, it ran inconspicuously in the background while attacking the operating system. Afterwards, it restarted the computer and encrypted the hard drive and tried to extort money from its victims in the form of bitcoins [3].

Conclusion

The iteration part has helped us to find more STRIDE [1] issues and we were able to add more responsibilities. After approximately three operations it was possible to move on with the analysis. Depending on the observed object we assume that this step requires more or fewer iterations. CAST-STRIDE seems to us a very structured procedure. During the analysis, we asked ourselves more and more questions regarding responsibilities and safety and security issues, which we might not have posed ourselves otherwise. We have also noticed that IT-security experts must definitely be consulted on certain issues. In other respects, too, there is a need for an interdisciplinary team to conduct the analysis to discuss and exchange valuable information. We also found that safety and security constraints are not simply assigned to one or the other domain. Also, we assume that certain security constraints can result in safety constraints, which leads us to suppose that safety and security should not just be considered separately. We did not analyse the whole system during the case study and stayed within the network boundary. The aim was to investigate the feasibility of the technique found and also to verify its practicability. We have seen that our technique shows good practical options for a safety-security analysis.


stpa-hcs WannaCry_HCS
Medical Staff
Hands over patient data, Informs about appointment
Hand out medicine, Treatment, Perform surgery, Give instructions
Register appointment, Stores patient data, Write email, Read email, Surf on the internet, Create shift schedule
Provides data, Program output, Notifications
Hospital Network
Computer
Send data, Get data
Provides data
Computer Firewall Internal
Patient data, Health status, Request, Diagnose, Make appointment
Network Firewall Internal
Get data, Send data
Store shift schedule, Store appointment, Stores patient data
Write email, Read email
Modem Internal
Involved Medical Staff
Backup Server
Spam Filter
Show email, Notifications
Patient data, Health status, Request
Hand out medicine, Give instructions, Perform surgery, Treatment
Start Backup
Store data
Health status, Request, Patient data
Data Server
Mail Server
Patient
External Stakeholder
Internet
Computer External
Computer Firewall External
Firewall External
Modem External
Spam Filter External
Mail Server External

The National Health Service (NHS) - WannaCry Hierarchical Control Structure (HCS). Enterprise Architect extension SAHRA was used to perform the analysis.

Outlook

The CAST-STRIDE framework could be verified by conducting a case study by different teams. We would have to compare the results and with a classical analysis approach. In addition, the case study could be replayed after an improvement of the system and examined to see whether the incident could not happen again. Another objective could be to transform the CAST-STRIDE approach into STPA [4]. In addition, one would have to think about prioritizing the resulting safety and security constraints, DREAD (**D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability) [1] could provide a helpful input.

References

1. A. Shostack, Threat modeling: designing for security. John Wiley & Sons, 2015.
2. M. Burgess, "www.wired.co.uk", 13. July 2017. [Online]. Available: http://www.wired.co.uk/article/nhs-wannacry-response-ransomwar [Accessed 23. October 2017].
3. C. Graham, , "The Telegraph", http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ [Accessed 23. October 2017].
4. N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2011.

Acknowledgement

Thanks goes to Christoph Walter Senn and Benjamin Contreras for their review and valuable input during the study.

www.zhaw.ch/iamp/sks
www.anzen-solutions.ch
www.sahra.ch

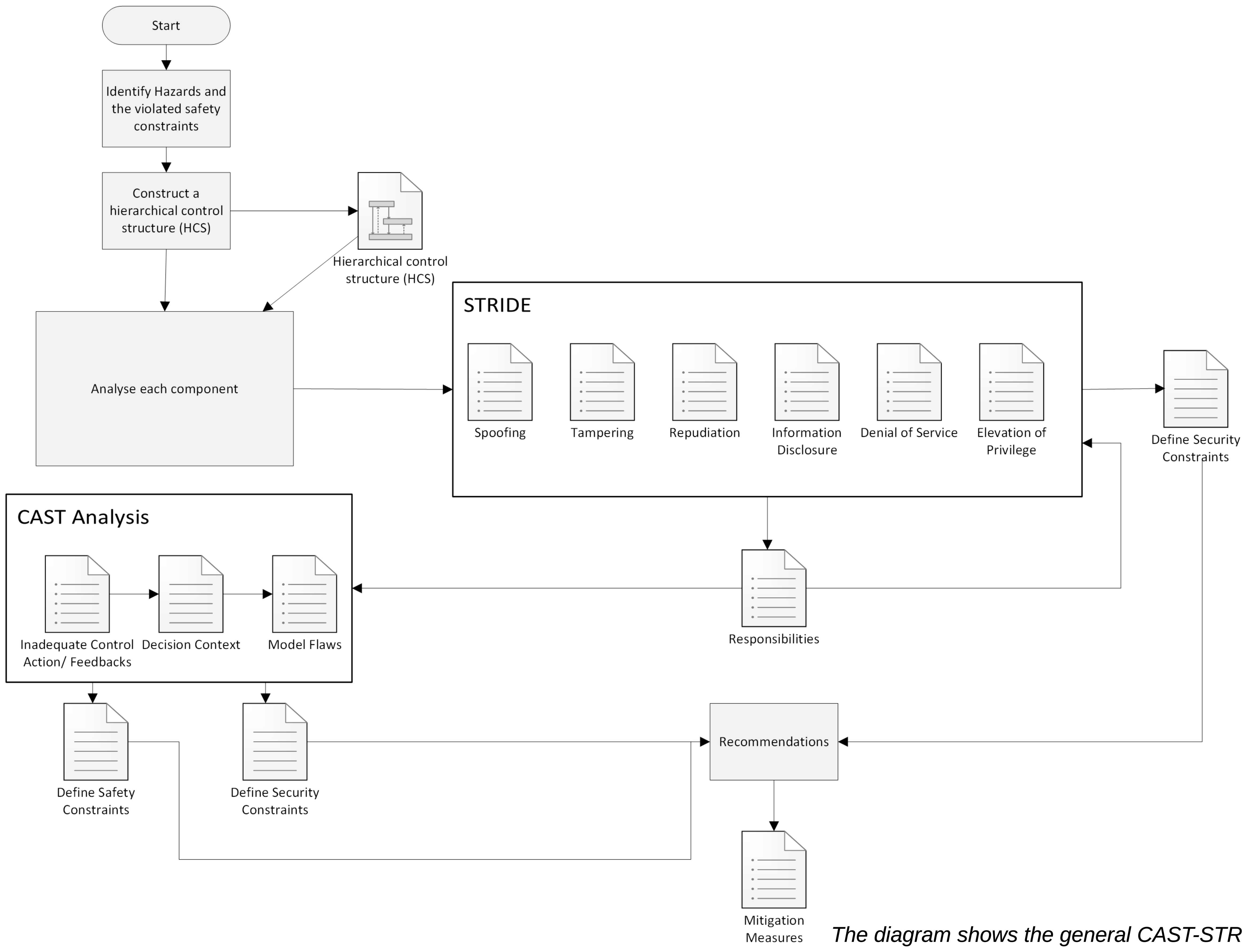
Zurich University
of Applied Sciences

CAST-STRIDE
An approach of bringing safety and security together

Zurich University of Applied Sciences ZHAW, Switzerland
Carmen Frischknecht-Gruber, Mario Marti and Sven Stefan Krauss

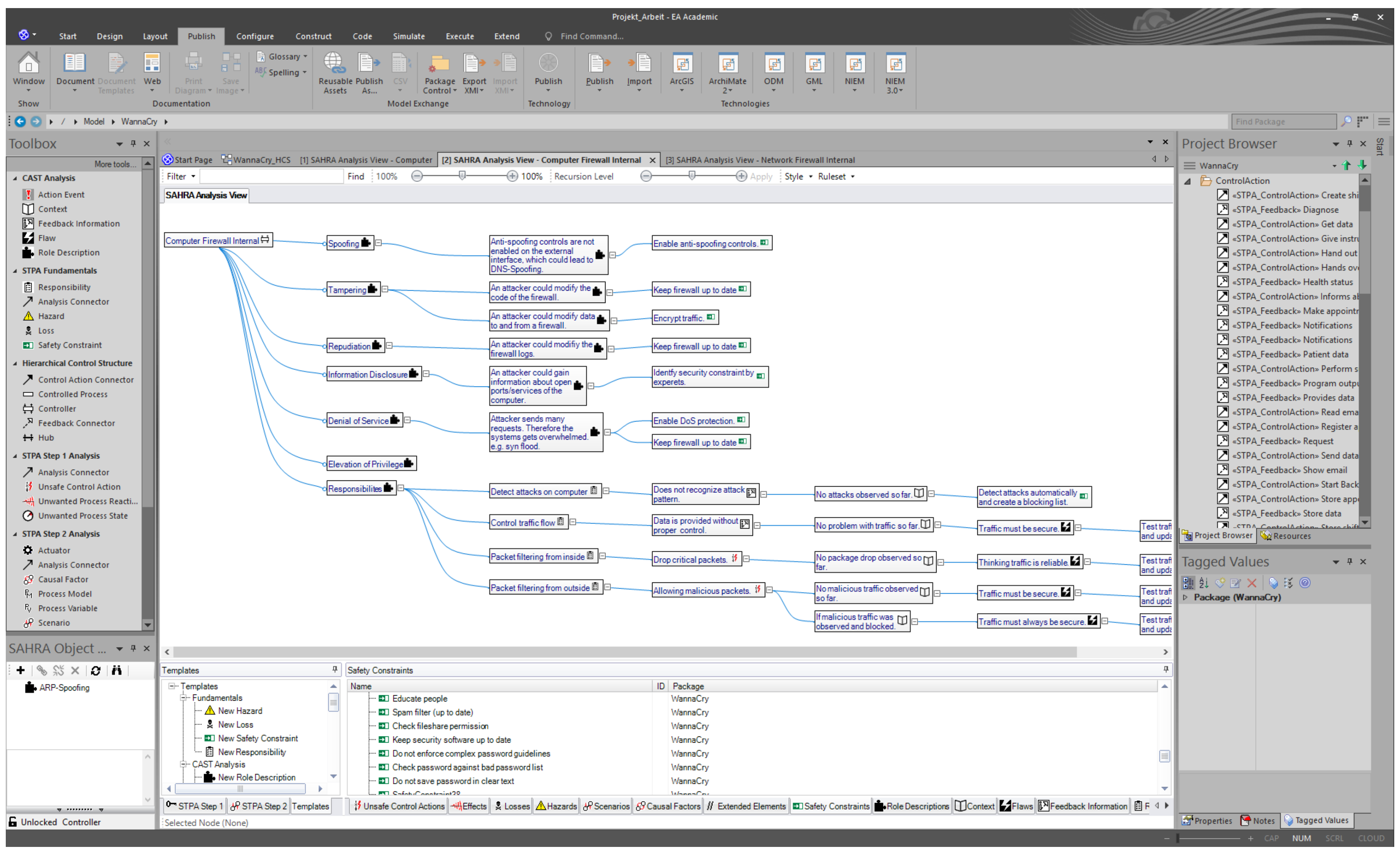
CAST-STRIDE

In this study, the main aim is to show if it is feasible to combine the safety analysis technique CAST with a security analysis approach. We also could see whether this combination would bring possible advantages. We have seen that it makes sense to examine a system not only in terms of safety aspects but also in terms of security factors. Different approaches of security analysis were considered, such as attack trees, STRIDE, DREAD and security design principles. The choice fell on STRIDE, because it seemed promising, using keywords and basing its analysis on data flow diagrams. When carrying out the case studies, we discovered that both analysis techniques could be examined with the HCS, which eliminated the need for a data flow diagram. The first approach of CAST-STRIDE was used in the Jeep Cherokee analysis, but it brought some practical problems with it. This is why the CAST-STRIDE technique was reworked for the WannaCry case study.



Start
Identify Hazards and the violated safety constraints
Construct a hierarchical control structure (HCS)
Hierarchical control structure (HCS)
Analyse each component
STRIDE
Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege
Define Security Constraints
CAST Analysis
Inadequate Control Action/ Feedbacks
Decision Context
Model Flaws
Responsibilities
Define Safety Constraints
Define Security Constraints
Recommendations
Mitigation Measures

The diagram shows the general CAST-STRIDE analysis workflow.



[2] SAHRA Analysis View - Computer Firewall Internal

SAHRA Analysis View

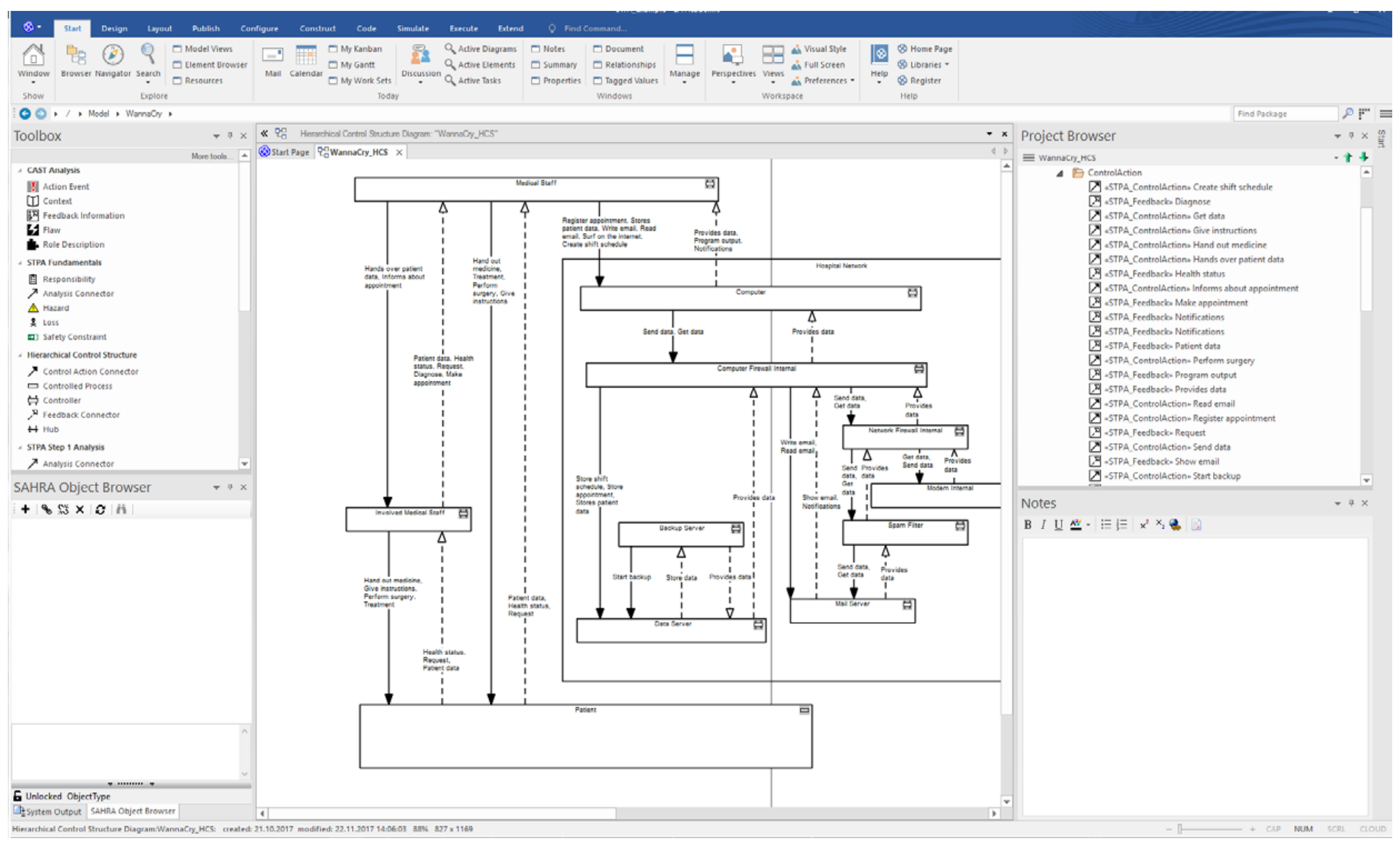
Computer Firewall Internal
- Spoofing
  - Anti-spoofing controls are not enabled on the external interface, which could lead to DNS-Spoofing.
    - Enable anti-spoofing controls.
- Tampering
  - An attacker could modify the code of the firewall.
    - Keep firewall up to date
  - An attacker could modify data to and from a firewall.
    - Encrypt traffic.
- Repudiation
  - An attacker could modifiy the firewall logs.
    - Keep firewall up to date
- Information Disclosure
  - An attacker could gain information about open ports/services of the computer.
    - Identfy security constraint by experets.
- Denial of Service
  - Attacker sends many requests. Therefore the systems gets overwhelmed. e.g. syn flood.
    - Enable DoS protection.
    - Keep firewall up to date
- Elevation of Privilege
- Responsibilites
  - Detect attacks on computer
    - Does not recognize attack pattern.
      - No attacks observed so far.
        - Detect attacks automatically and create a blocking list.
  - Control traffic flow
    - Data is provided without proper control.
      - No problem with traffic so far.
        - Traffic must be secure.
  - Packet filtering from inside
    - Drop critical packets.
      - No package drop observed so far.
        - Thinking traffic is reliable.
  - Packet filtering from outside
    - Allowing malicious packets.
      - No malicious traffic observed so far.
        - Traffic must be secure.
      - If malicious traffic was observed and blocked.
        - Traffic must always be secure.

Safety Constraints

Name	ID	Package
Educate people		WannaCry
Spam filter (up to date)		WannaCry
Check fileshare permission		WannaCry
Keep security software up to date		WannaCry
Do not enforce complex password guidelines		WannaCry
Check password against bad password list		WannaCry
Do not save password in clear text		WannaCry

STRIDE is now carried out in relation to the responsibilities; the aim is to find all sorts of responsibilities that serve possible safety and security aspects. A loop was introduced for this purpose. STRIDE is no longer executed according to all responsibilities, as in the first approach, but only on the considered component. This promotes practicability in the implementation and retains the advantage of bringing in security responsibilities and ultimately possible additional safety and security constraints.

Part of the NHS-WannaCry HCS and the analysis view of the internal firewall in the NHS WannaCry case study
Enterprise Architect extension SAHRA was used to perform the analysis.
CAST-STRIDE Approach.



Acknowledgement
Thanks goes to Christoph Walter Senn and Benjamin Contreras for their review and valuable input during the study.

www.zhaw.ch/iamp/sks
www.anzen-solutions.ch
www.sahra.ch