Interconnected safe and secure systems

Peter Popov,

City, University of London,

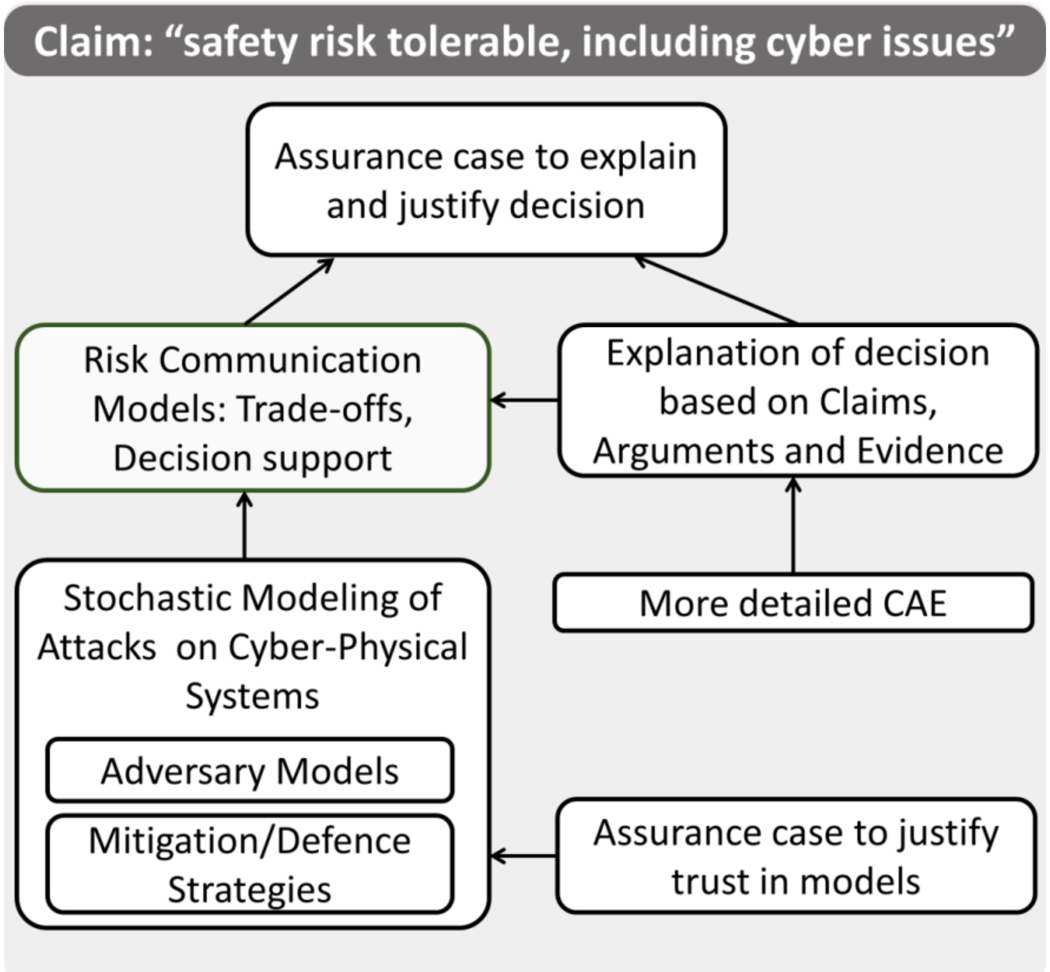
RiTICS Spring Showcase 2019

15th April 2019

CITY UNIVERSITY LONDON
EST 1894

Overview of CERDICS (RITICS - 1)

Stochastic models of systems and adversaries



Decision analysis and communication based on Claims, Arguments, Evidence

Outline

- What we promised in IS3
  - WP 1 “Consultation and outreach”
    - Safety and Security – Workshop with CINEF
    - Interdependency modelling – Workshop with ResilShift and a report on the state-of-the art and ways forward.
  - WP2: Model based analysis
    - Review of SoA in modelling “Resilient Operator of a CNI operator” and identify research issues
    - Examples of models useful in “co-engineering” for safety and security
  - WP3: Safety and Security Decision Making
    - Change of tempo in safety-case lifecycle to account for security (e.g. how to make safety cases robust to software patching)
    - Trade-offs and synergies.

CITY UNIVERSITY LONDON

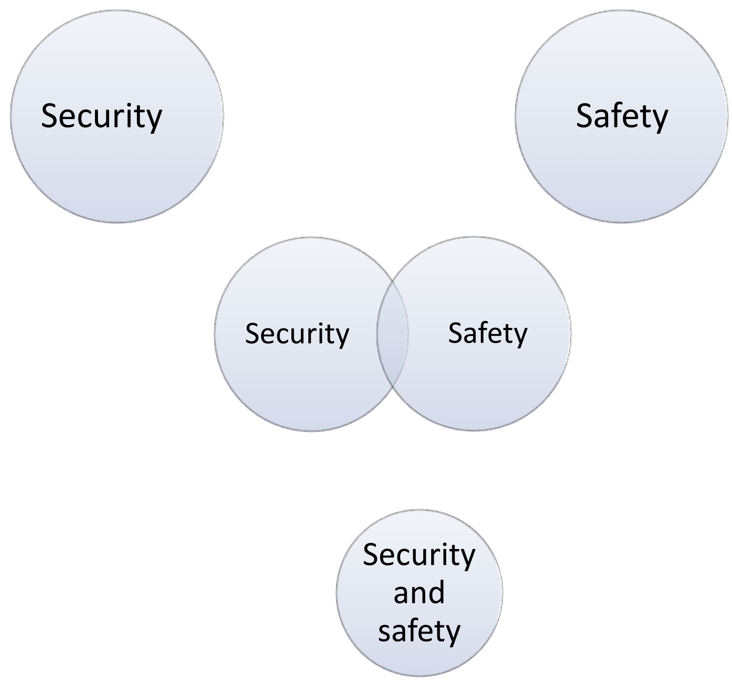
EST 1894

Progress made to date

- Engagement with stakeholders – ongoing. Workshops planned for mid-May/early-June
- Models of safety and security (examples)
  - Examples of models of embedded systems (details will be presented today)
  - Examples of models of critical infrastructures (e.g. to help with “optimal allocation of defence in depth”)
    - Ongoing work with Nordic-32 simulator (used by City in RITICS - 1).
- Models of analysis from SysML models
  - not in the proposal, but approved by sponsors (will give a presentation on the progress)

CITY UNIVERSITY LONDON
EST 1894

Models for combined analysis of safety and security



✗

✓

Maybe???

CITY UNIVERSITY LONDON

EST 1894

Combined safety and security analysis ≠ S + S

- Combined analysis is not just ***safety-only*** + ***security-only*** analyses.
- A truly ***combined SSP analysis*** *requires* an explicit and credible ***model of dependencies*** between the properties of interest, e.g.:
  - Conflicting Safety and Security requirements lead to the need for trade-off analysis:
  - successful attacks may ***impair safety*** against accidental faults, e.g. by eliminating the ***safe state*** (real attacks on safety are well documented)
    - “If it is not secure it is not safe”
  - strengthening security controls typically affects performance (e.g. response time)
    - and increases the likelihood of missing a hard real-time deadline

Credible trade-off analysis is impossible without a credible combined analysis

Quantitative Combined SS analysis (2)

- Hazard analysis to identify security threats that may impact safety (or performance) is complemented by:
  - Judgement about the *likelihood* of various events
    - Attack occurrence
    - Attack success probability
  - An explicit ***model of how successful attacks*** affect reliability/performance of components. Some examples include:
    - the functionality of a *safe state* is blocked (eliminated), or
    - the *rate of failure* of compromised software components increases, thus increasing the likelihood of *unsafe system failures*.

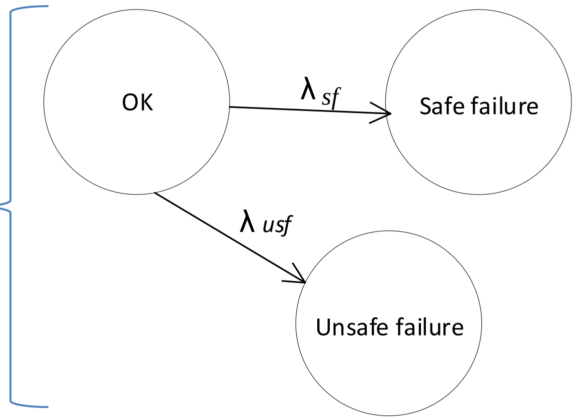
Quantitative Combined SS analysis (3)

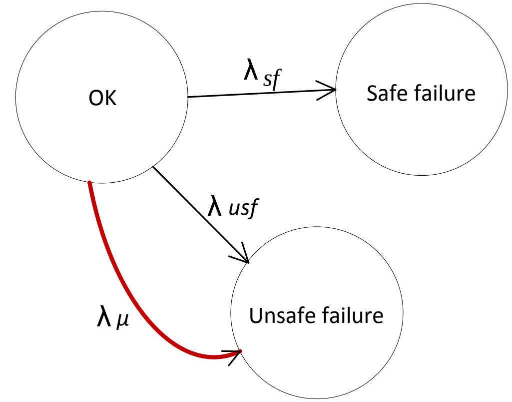
- Common mistakes in constructing models for combined SS analysis:
  - Safety is demonstrated in "trusted" environment
  - Security controls are added (e.g. to meet security requirements), but their impact is limited to checking if the additional overhead due to these security controls is tolerable.
- The questions that we should address in constructing models suitable for SS analysis are:
  - Security controls *are not perfect*. They may have flaws, they may be also compromised.
  - Anticipate compromises everywhere and study the implication of each compromise.
  - The answers related to likelihood of attacks and their effect are subject to *uncertainty*. Can we quantify credibly this uncertainty, or at least establish *bounds* on it?

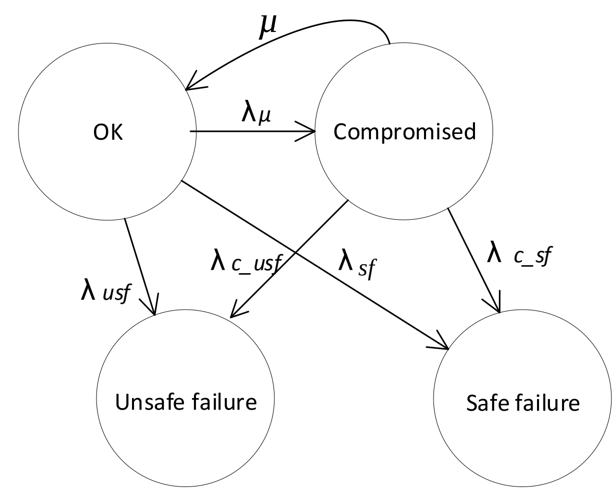
CITY UNIVERSITY LONDON
EST 1894

Model of Dependence: Example 1

- Model of system safety in *"trusted environment"*







- How much worse is system safety in adverse environment?
  - It depends on how we model the adverse environment?
    - *Model 1:* All successful attacks lead to ***unsafe state***.
    - *Model 2*: Attacks lead to a ***compromised state***, from which transitions are possible to safe/unsafe state or to OK (e.g. if we deploy "proactive recovery").
  - The outcomes of trade-off analysis will be affected significantly by the choice of dependency model (1 or 2 above).

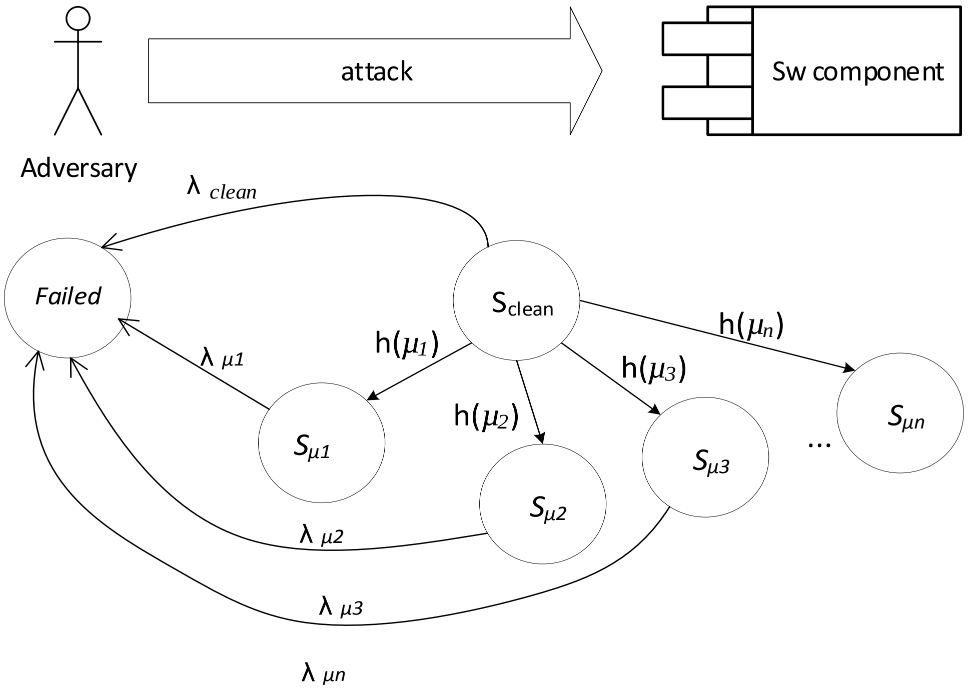
- Models of system safety in "*adverse environment*"

Model of Dependence: Example 2

- Consider the case when ***reliability*** of a software component ***is reduced*** by a successful attack which compromises software integrity.
  - An example: alteration of a threshold value of a software-based ***protection device*** (e.g. of a power line)

Model the effect of a successful attack on software reliability:

  - $\lambda_{clean} \leq \lambda_{\mu1}, \lambda_{\mu2}, \ldots, \lambda_{\mu n}$,
    - Successful attacks increase the rate of software failure.
  - Validating a ***safety goal*** would be dependent on:
    - ***security goal*** set for attacks.
    - ***attack effect*** on software reliability.
  - Parameterisation becomes harder.



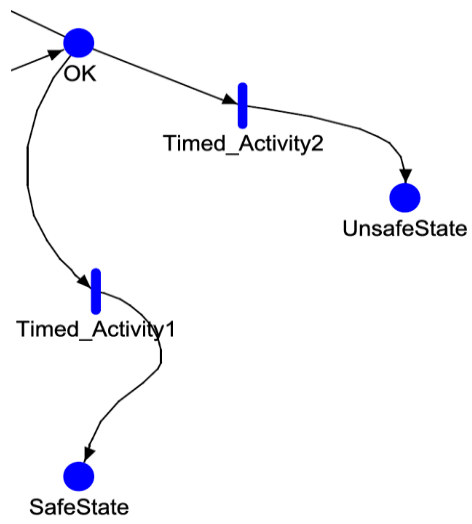
- A similar model of dependence on security, applies to performance, too
  - Successful attacks may increase the response time of a s/w component

Popov, P.T., Models of reliability of fault-tolerant software under cyber-attacks, (ISSRE 2017).
Model of attacks validated recently on NORDIC-32.

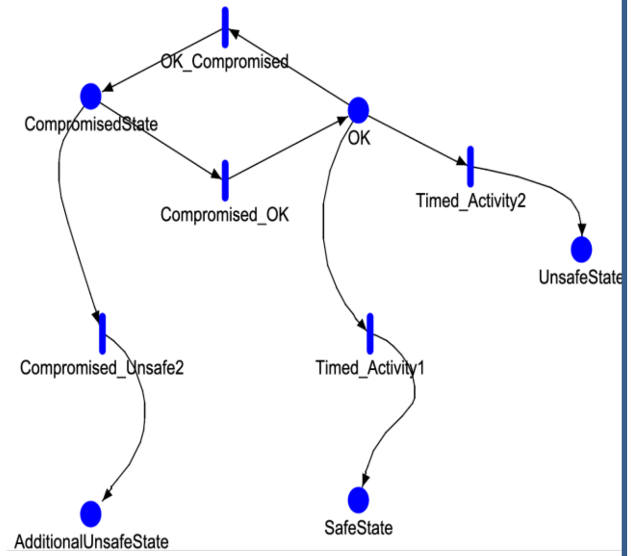
Model of Dependence: Example 3

- The ***safe state may be eliminated*** as a result of a cyber attack.
- λ_{UF} | NonC SS ≤ λ_{UF} | Com SS
- UF – unsafe failure.
- NonC SS - non-compromised safe state
- Com SS – compromised safe state.
- Clearly, the effect of removing the safe state is an *increased rate of unsafe failure*.
- Setting a ***safety goal*** for unsafe failure is simple, but its validation is dependent on the ***security goal*** set for the security event *"compromising the safe state"*.
- This particular problem is *recognised in IAEA guidelines*.

A safety model in ***trusted*** environment



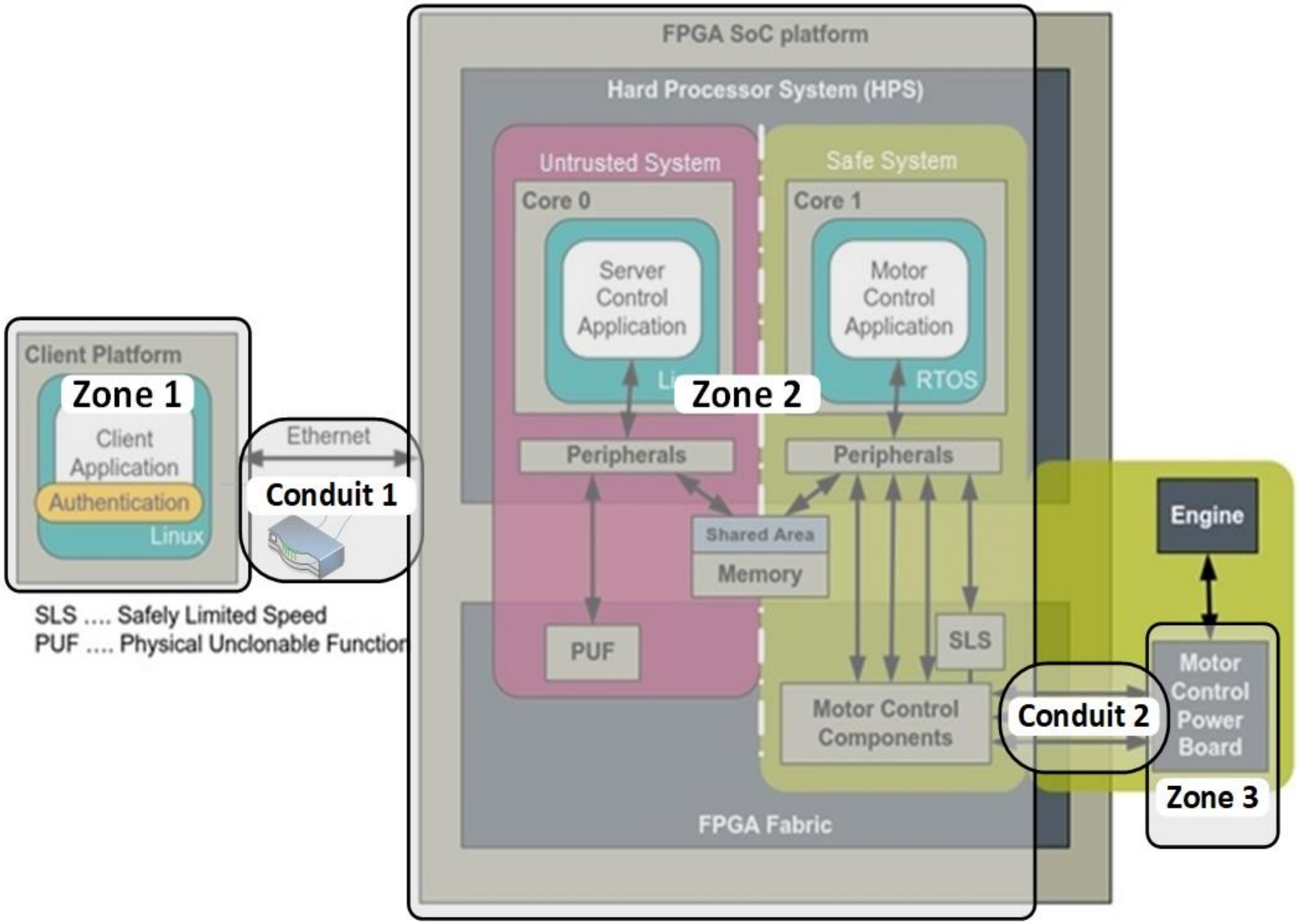
A safety model in ***adverse*** environment



Popov, P.T., Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device., (SAFECOMP 2015).

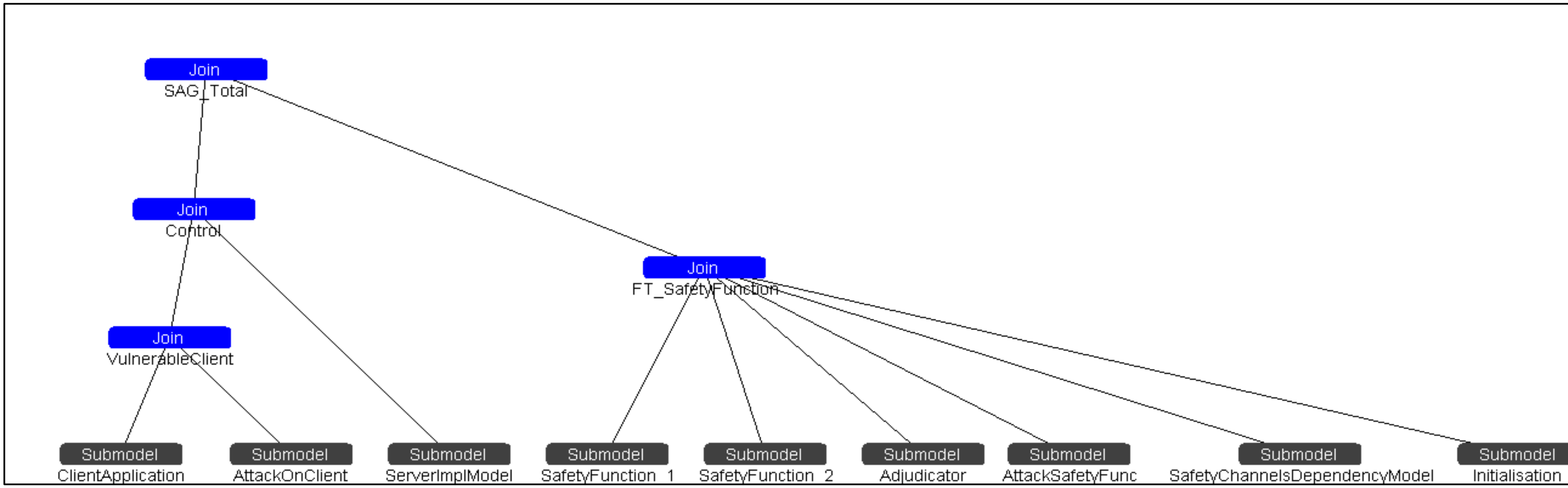
Models for SS analysis in practice

- An AQUAS (an EU ECSEL JU project) case study: A virtual prototype of an Industrial Drive.



CITY UNIVERSITY LONDON
EST 1894

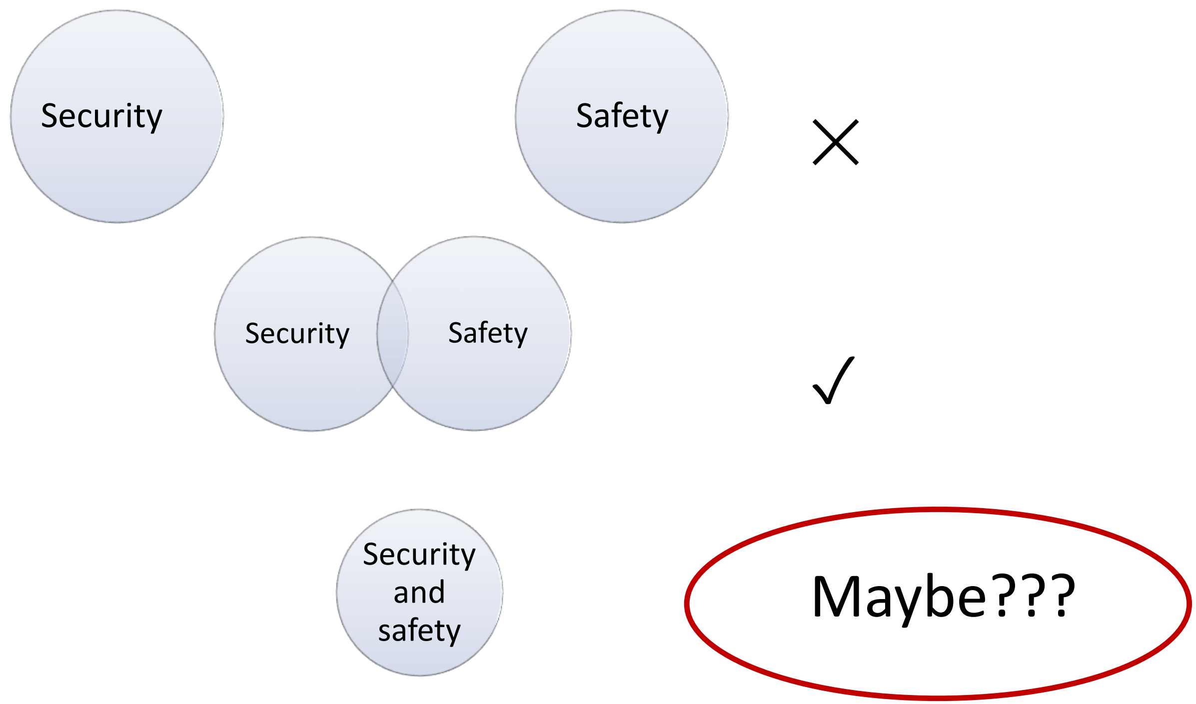
A SAN (stochastic activity networks) model



- Modelled all zones (with some simplifications)
- Modelled 2 attacks:
  - Attack on the client application: when client compromised, the failure rate increases.
  - Attack on the safety function (bringing the device to a safe state, i.e. stop the motor). Safety function is implemented as a 2-channel sub-system:
    - A successful attack on a channel of the safety function may affect either the ***coverage*** (i.e. the probability of detecting a failure provided there is a failure) or the probability of ***false alarm***.
    - Attacks may be on a ***single channel*** or ***simultaneously on both channels*** (with small interval between attacks of the channels).
- ***Sensitivity analysis*** (rate of attacks, probability of success of attacks) completed. Looked at the effect of “cleansing” to mitigate the consequences of successful attacks.
  - Numbers suggests that cleansing is quite effective! The “owner” of the prototype convinced that the client application should be designed with cleansing.

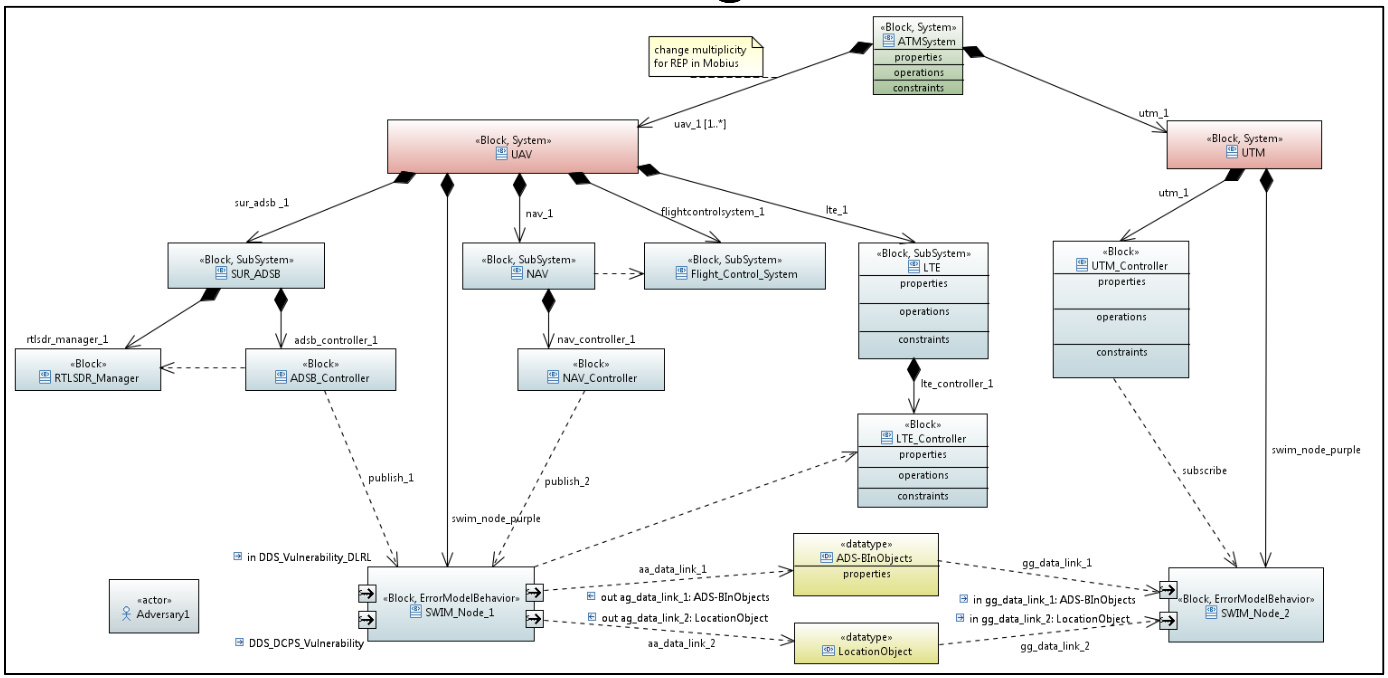
CITY UNIVERSITY LONDON
EST 1894

Models of Combined analysis (Safety and Security)

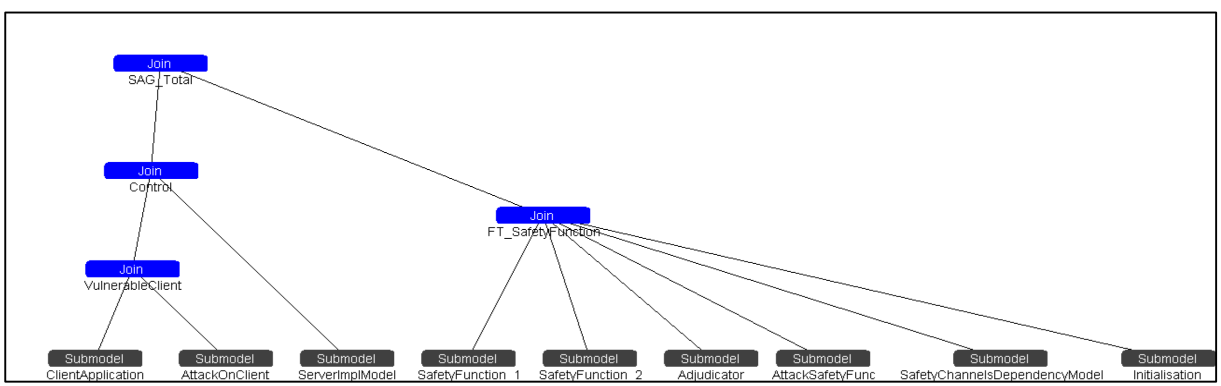


CITY UNIVERSITY LONDON
EST 1894

System development and SS analysis: Deriving SAN models from SysML model



- Model transformation: from CHESS (SysML) -> SAN



CITY UNIVERSITY LONDON
EST 1894

Questions