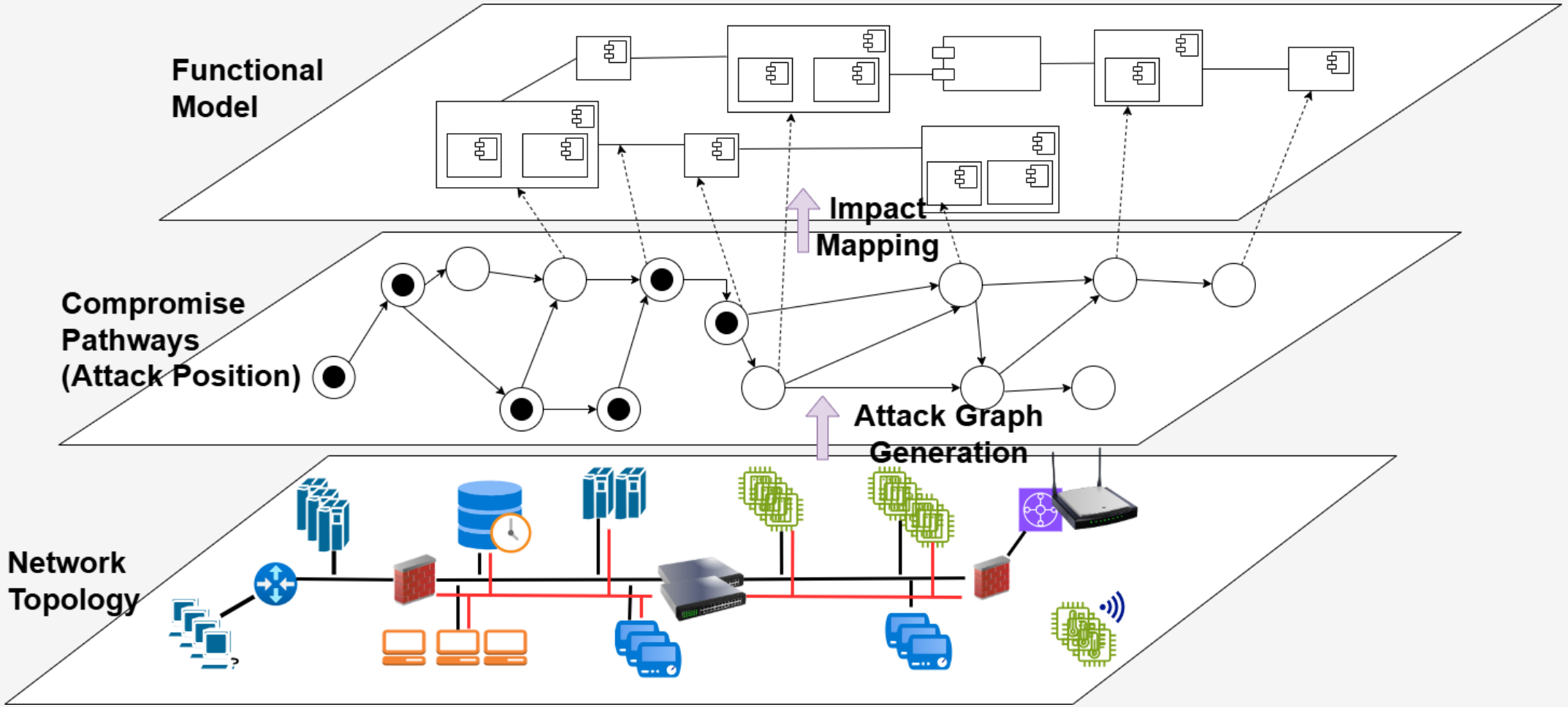
IMPERIAL

The Consilience of Security, Safety and Resilience

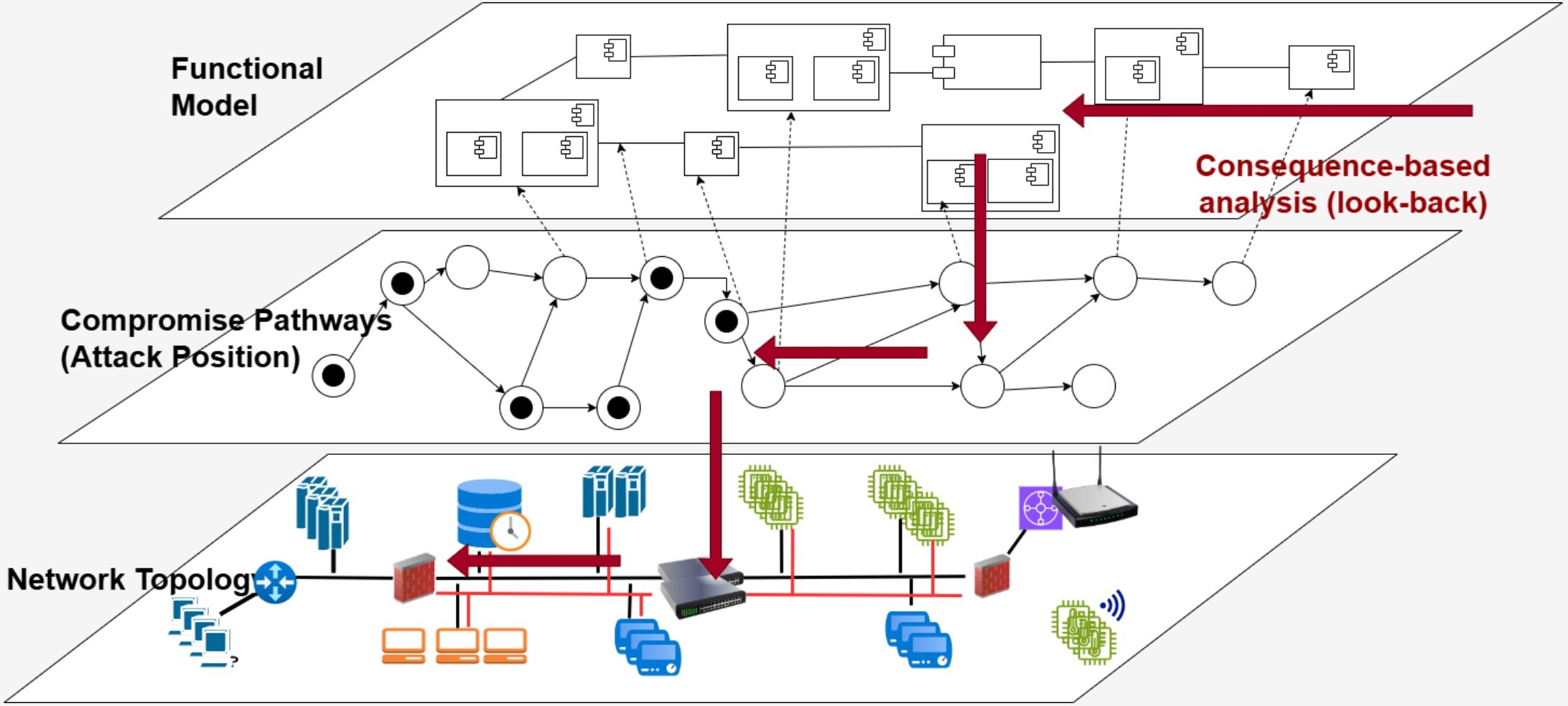
Resilient Information Systems Security Group
www.rissgroup.org

Emil Lupu
Imperial College London

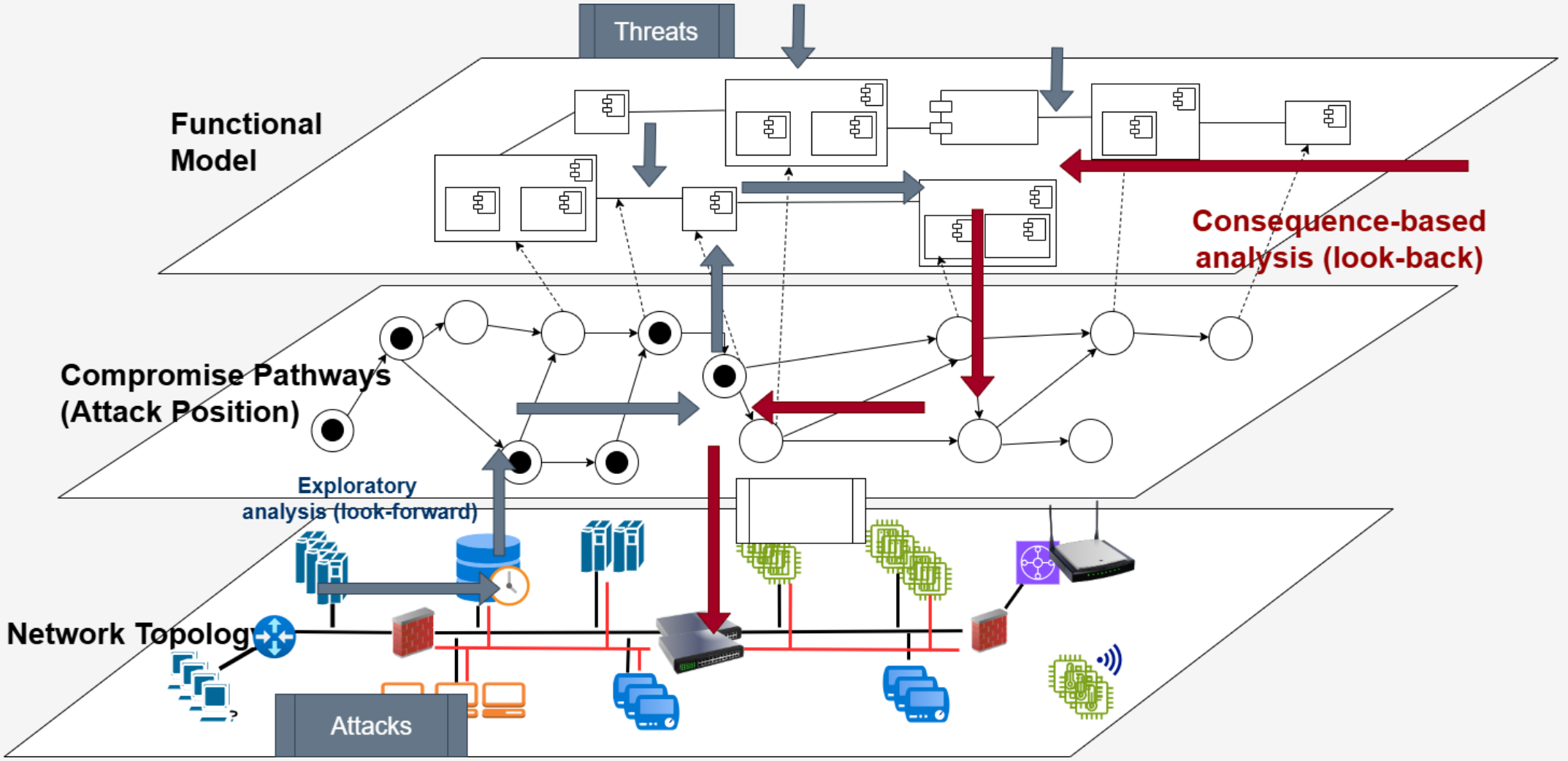
A broader framework for safety, security and resilience analysis



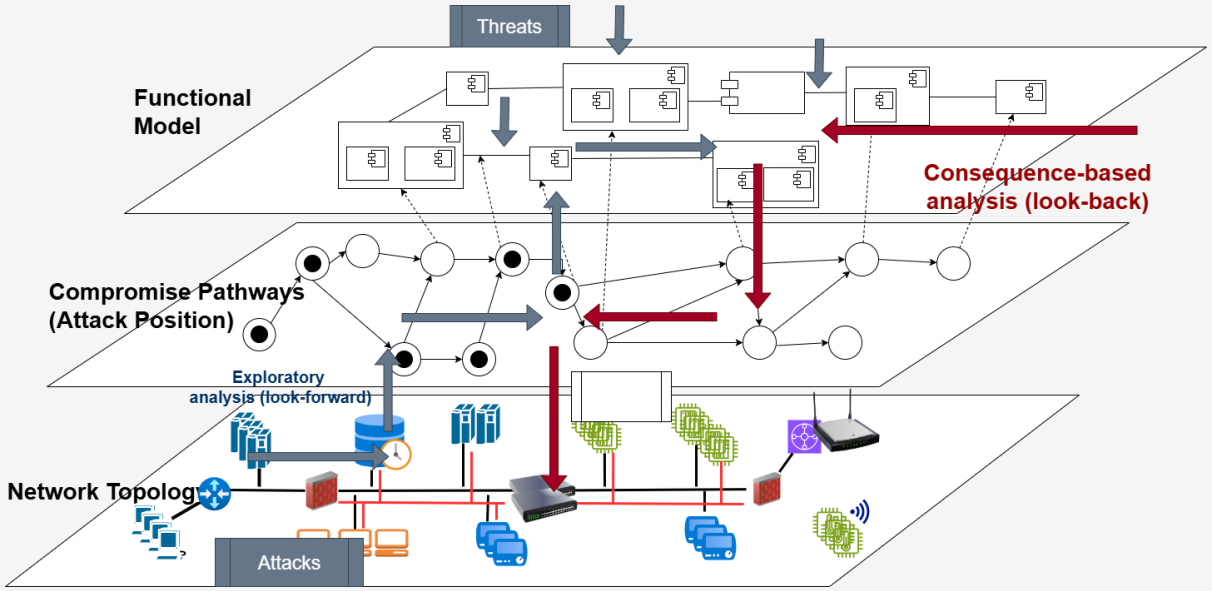
Consequence and Safety



Security Analysis



Resilience Analysis

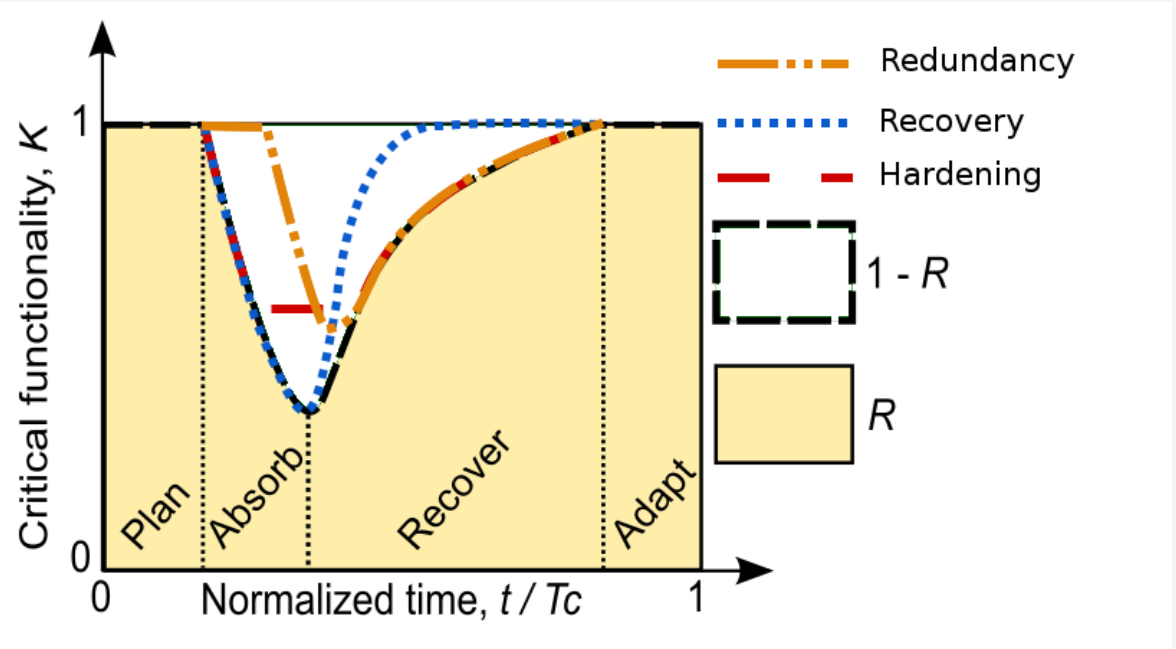


Resilience is identifying the (optimal) combination of strategies (robustness, redundancy, recovery) that minimises loss of function over time for a range of perturbations (including attacks).

At each step the attacker may choose to:

- Continue to compromise the system.
- Perform an action that impacts function.

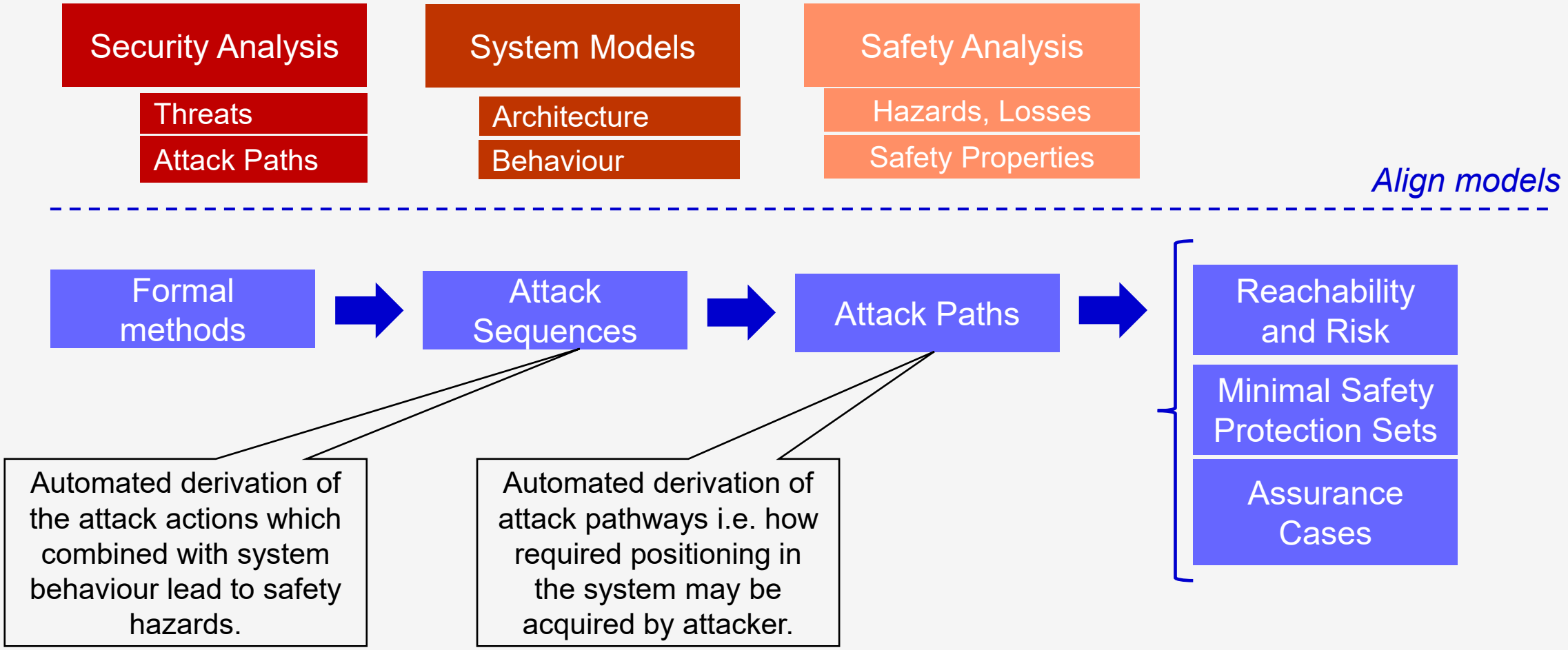
This leads to combinatorial explosion of attack scenarios. Resilience to attacks is difficult.



Modified from: Ganin et al. *Operational resilience: concepts, design and analysis*. Nature Scientific Reports

Combining safety and security analysis

CASSANDRA

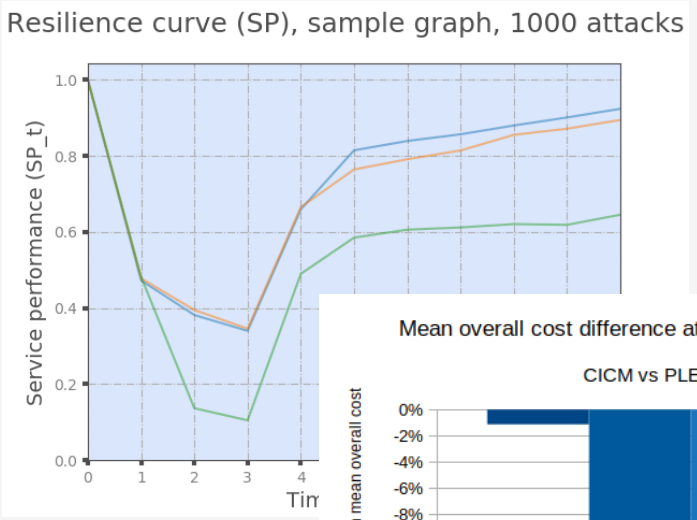


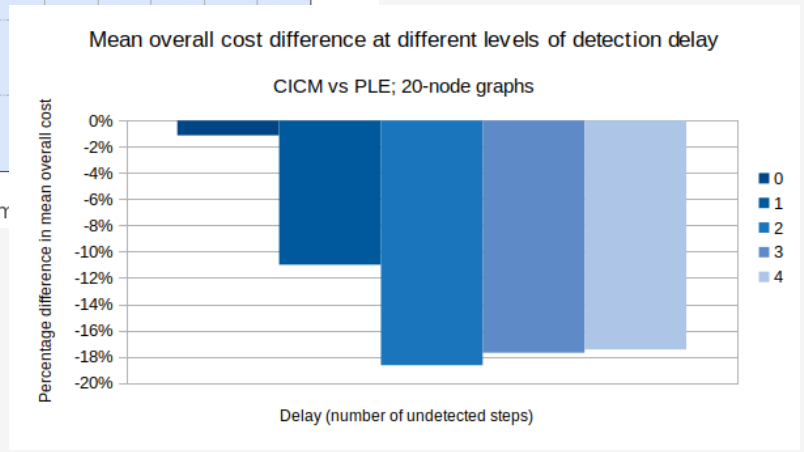
L. M. Castiglione and E. C. Lupu. Which attacks lead to hazards? combining safety and security analysis for cyber-physical systems. IEEE Trans. Depend. Sec. Comput., 21(4):2526–2540, 2023.

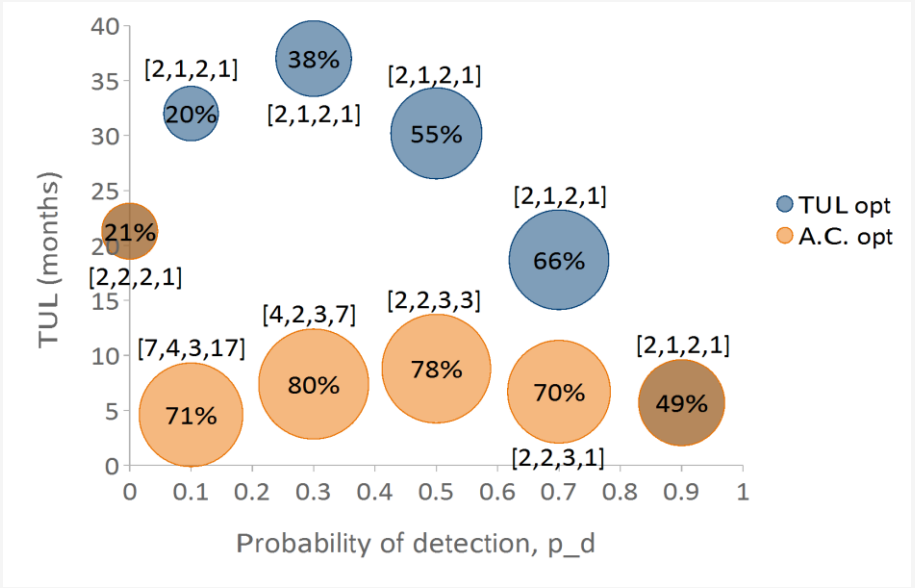
Resilience Analysis

Is it better to focus efforts on attack containment or on recovery?

… well, it depends on the dwell time of the attack (and the limitations of intrusion detection)







How does the structure of SLAs impact investments in resilience?

What are the resilience gains from redundancy (with diversity)?

J. Soikkeli, G. Casale, L. Munoz-Gonzalez and E. C. Lupu, "Redundancy Planning for Cost Efficient Resilience to Cyber Attacks," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2022.3151462.

Closing Thoughts

There are many research questions at the intersection of security, safety and resilience that can be answered, e.g. identifying attacks that will lead to safety violations, characterise degraded modes of operation that preserve safety and isolate threats, respond to perturbations etc. Tool support to help analysis is within reach and currently much of the effort is manual, error prone and painful. This will require combining perspectives.

The **framework** presented proved useful to integrate thinking, identify difficult challenges and construct solutions. Further work is the pipeline including on: continuous risk assessment, reconfiguration when parts of the system have been compromised, dynamic network segmentation, attack simulation/emulation, integration with MBSE.

IMPERIAL

Thank you

Consilience of Security, Safety and Resilience
Emil Lupu (e.c.lupu@imperial.ac.uk)

IMPERIAL RISS
www.rissgroup.org

The Consilience of Safety, Security and Resilience

Emil Lupu {e.c.lupu@ic.ac.uk}
Luca M Castiglione {l.castiglione@ic.ac.uk}

Modern safety-critical systems must be safe, secure, and resilient. Yet, the intersections of these properties are challenging

- Publications and standards discuss the conflicts between safety and security.
- Security is needed for safety, but security is not fully achievable.
- Resilience requires adaptation, which makes assurance more challenging.

Modern systems exhibit common trends as they are increasingly:

- Cyber-physical, thereby enabling physical attacks and consequences.
- Complex, thereby leading to emerging behaviours and cascading effects.
- Larger, thereby having a broader attack surface.
- Inter-connected and inter-dependent.

Interconnections enable the attacks to propagate. Interdependencies can create cascading effects, including in case of attacks.

So, "security" cannot be guaranteed and compromised components must be assumed to behave in any way the attacker chooses.

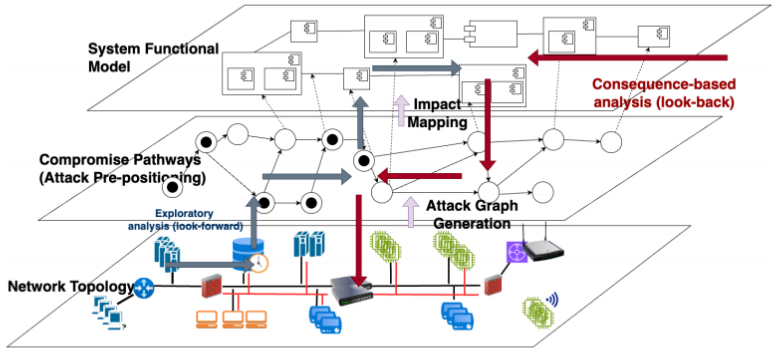


Figure 1: Framework for safety, security, and resilience analysis. The position of an attacker is the set of nodes visited along the attack graph (middle layer).

Framework

Figure 1 shows our framework for simultaneously reasoning about safety, security and resilience. We adopt a layered approach and distinguish:

- the network topology layer, which allows reasoning about attack progression.
- the functional layer, representing functional interdependencies between the components
- the attack graph layer, which makes it convenient to reason about attack pathways and the attacker's acquired position.

Safety (and Consequence-based Analysis) is conducted in the functional layer, starting with the consequences (e.g. losses) of interest and recursively considers what might cause them through the interdependencies in a "look-back" fashion. This reduces the security analysis to only those attack positions that can lead to specific consequences.

However, identifying all combinations of inputs that lead to an output, across all dependencies, is hard. When the causes are failures, experience and historic data guide us. When the inputs are malicious, the entire domain of values must be considered.

Security

Security analysis generally explores, i.e. looks forward, from a point of access considering the chain of attack steps. This is easier, but results in numerous attack paths. Where exploratory security analysis meets consequence-based analysis is rarely considered.

Often, a threat actor may acquire and persist a position, without immediately impacting system operation. Any risk assessment needs to consider the two aspects separately. Linking attack effects directly to vulnerabilities is misguided.

Resilience

aims to minimise the loss of function over time when perturbations occur (including malicious attacks). This can be ensured by a combination of: a) improving security b) increasing redundancy and/or capacity, and c) enabling faster recovery. Choosing the optimal combination, is the fundamental challenge. Figure 1 shows why resilience to attacks is difficult. At each step, an attacker can choose whether to continue compromising the system or trigger an impact-generating attack action. This leads to a combinatorial explosion of possible attack scenarios. Resilience to failures considers perturbations from past history. For adversarial attacks, fewer assumptions can be made and comprehensive evaluations of attack scenarios are needed.

Conclusions

We have shown how our framework (Figure 1) helps identify some of the critical issues in the co-analysis of safety, security, and resilience. We have built on it to show how security and safety analysis can be combined to systematically identify attacks leading to safety violations [1]. We have also shown how the attacker's choices can significantly influence resilience strategies [2, 3].

References

[1] L. M. Castiglione and E. C. Lupu. Which attacks lead to hazards? combining safety and security analysis for cyber-physical systems. IEEE Trans. Depend. Sec. Comput., 21(4):2526–2540, 2023.

[2] J. Soikkeli, G. Casale, L. Muñoz-González, and E. Lupu. Redundancy planning for cost efficient resilience to cyber attacks. IEEE Trans. Depend. Sec. Comput., 20(2):1154–1168, 2022.

[3] J. Soikkeli, C. Perner, and E. C. Lupu. Analyzing the viability of uav missions facing cyber attacks. In 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pages 103–112. IEEE, 2021.

UK Research and Innovation
[dstl]