CITY UNIVERSITY LONDON

Interconnected safe and secure systems

Security and safety: tempo and trade-offs

Robin E Bloomfield, Adelard LP and City, University of London,

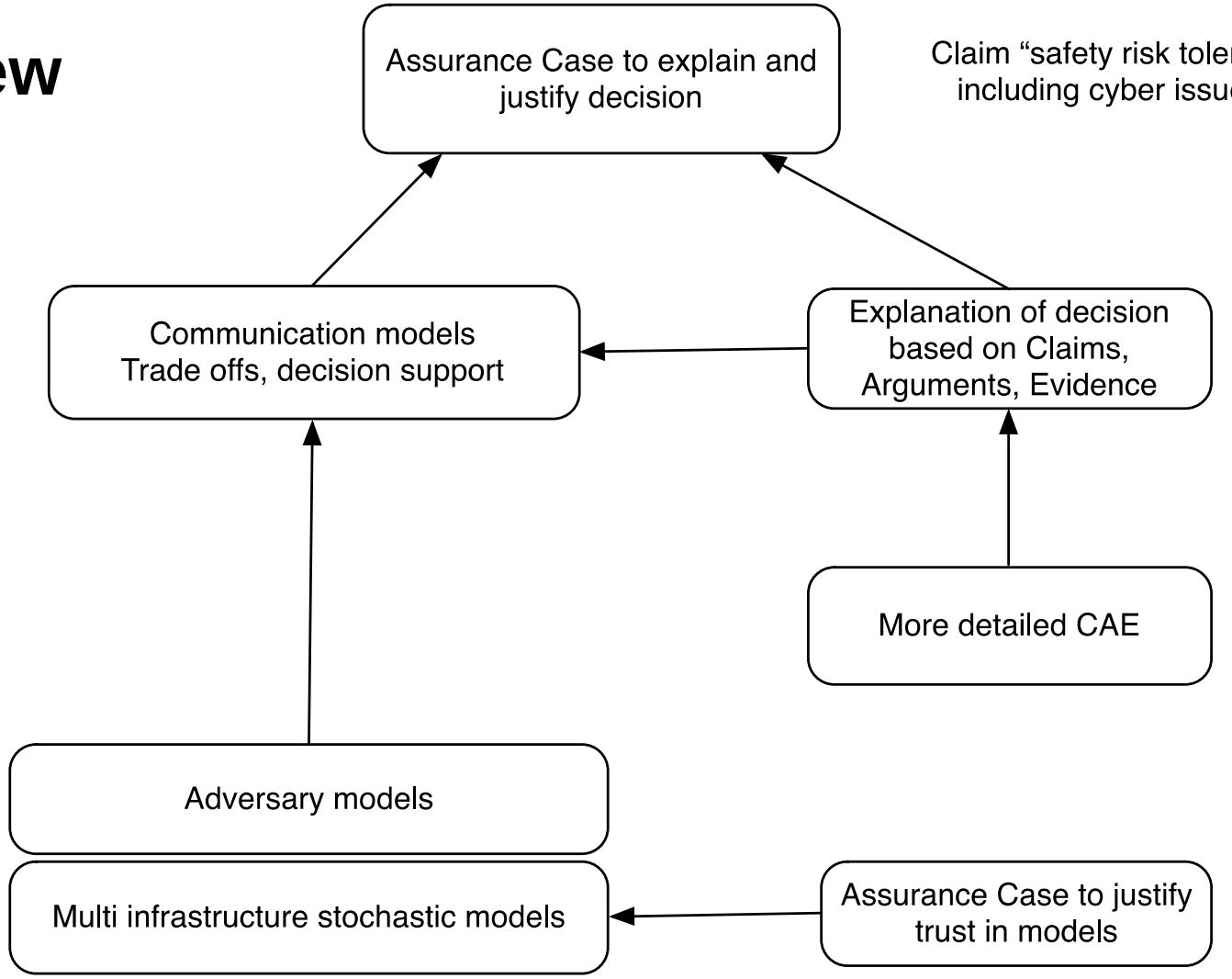
Peter Popov, City, University of London,

RiTICS Showcase

18th October 2018

CITY UNIVERSITY LONDON

Overview

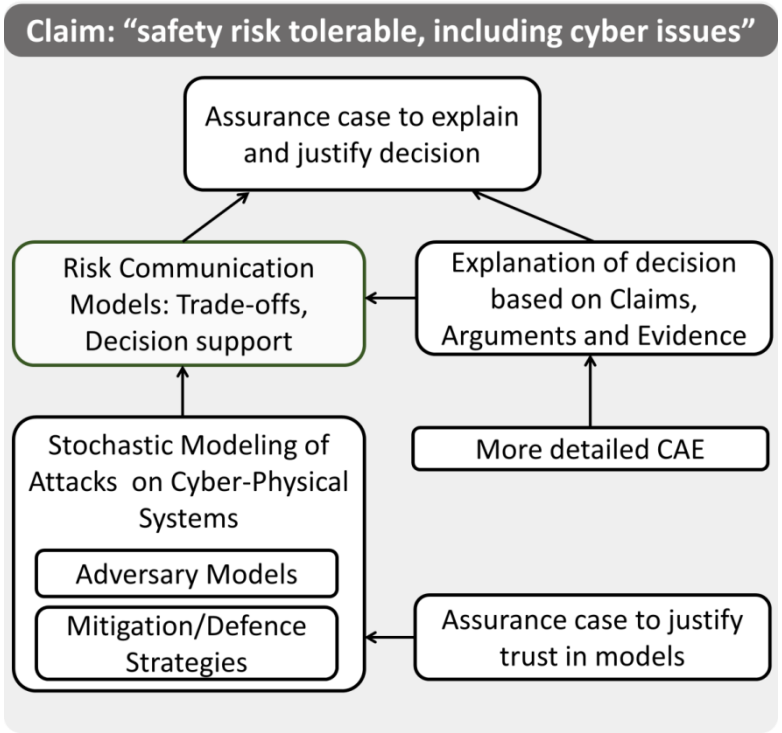


PIA FARA

CITY UNIVERSITY LONDON

CEDRICS Communicating and evaluating risk and dependencies

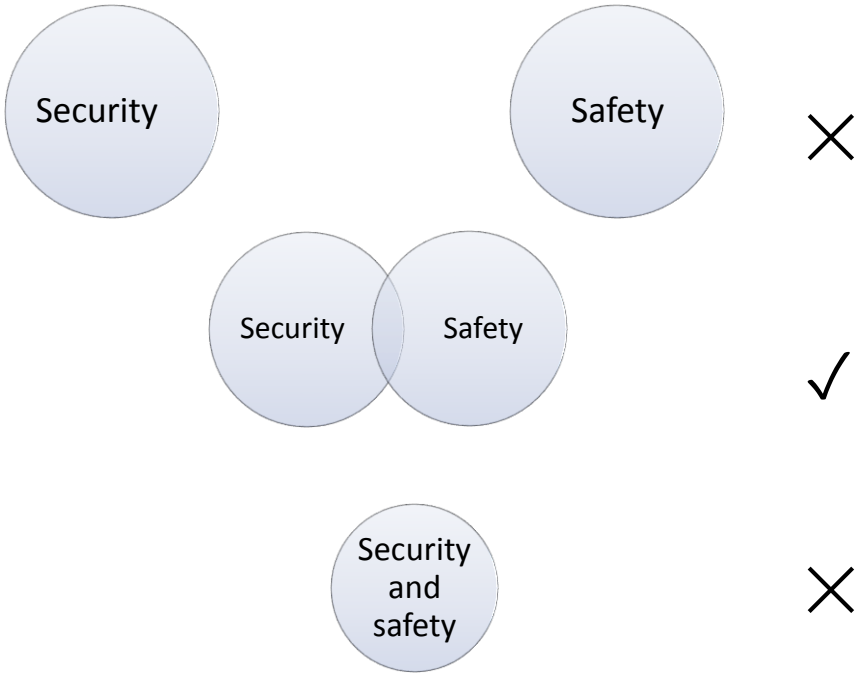
Stochastic models of systems and adversaries



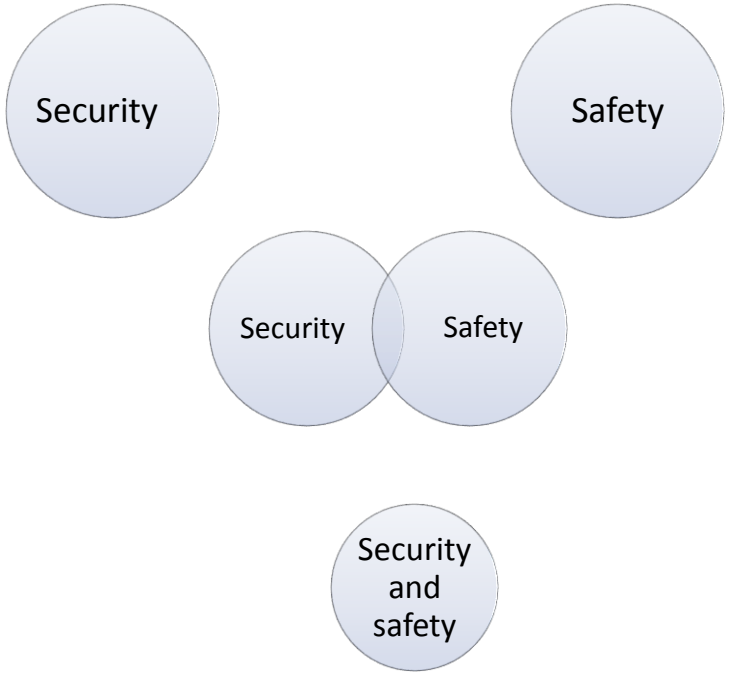
Decision analysis and communication based on Claims, Arguments, Evidence

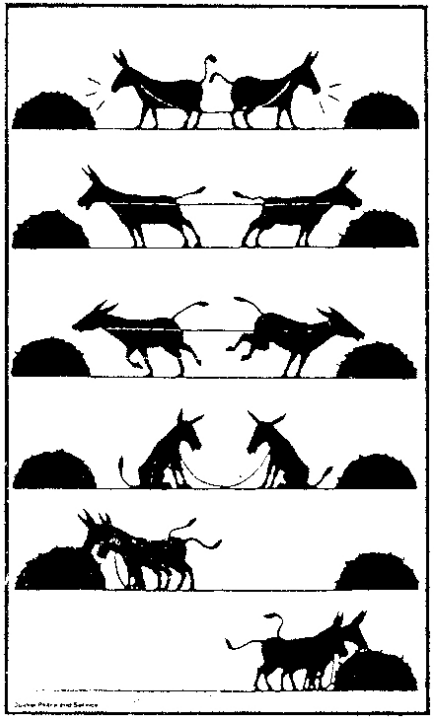
CITY UNIVERSITY LONDON

How much should safety and security be integrated?



Slogan “If it’s not secure, it’s not safe”

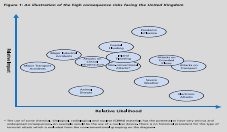
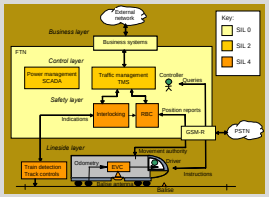
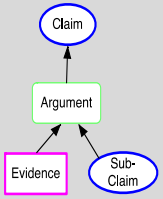
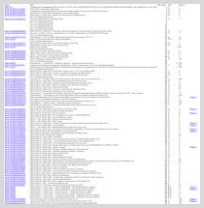




CITY UNIVERSITY LONDON

EST 1894

Security-informed safety and resilience - overview

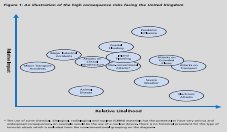
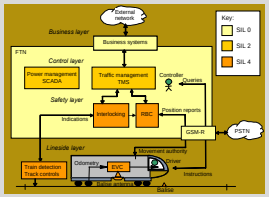
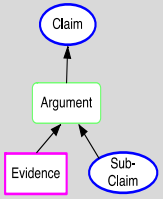
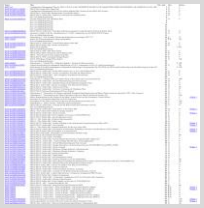
Systems of systems	Risk assessment	Training	Assurance and policy Framework	Standards and policy
				

MINDSET

CITY UNIVERSITY LONDON

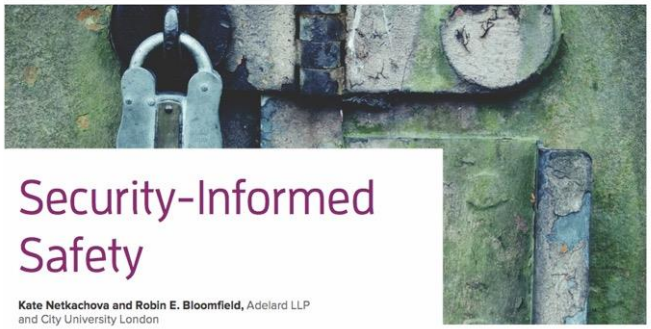
EST 1894

Security-informed safety and resilience

Systems of systems	Risk assessment	Training	Assurance and policy Framework	Standards and policy
				

Many projects: Sesamo, Aquas, IEC, BSI, IET …

CYBERTRUST



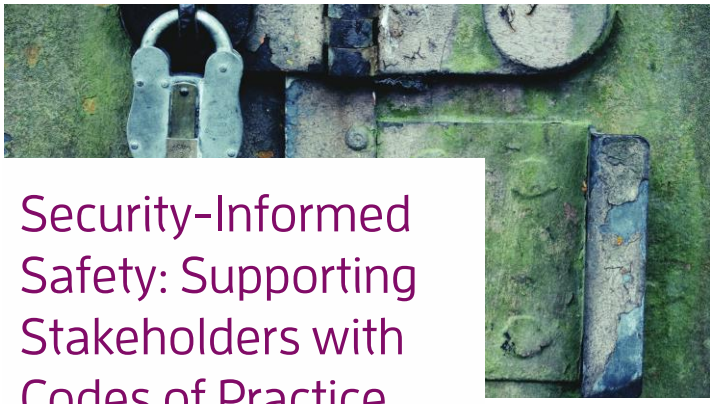
Security-Informed Safety

Kate Netkachova and Robin E. Bloomfield, Adelard LLP and City University London

For safety-critical systems, if it isn't secure, it isn't safe.

which a system malfunction could lead to accidents with marginal or negligible severity, to high criticality, in which a system failure or malfunction could result in death and

CYBERTRUST



Security-Informed Safety: Supporting Stakeholders with Codes of Practice

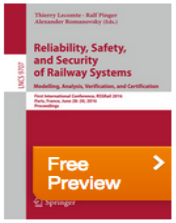
Robin Bloomfield and Peter Bishop, Adelard LLP and City, University of Londo
Eoin Bu
Robert S

Codes
guidar
securi
engine
minde

engineers think, in order to make

» Computer Science » Software Engineering

Programming and Software Engineering



© 2016

Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification

First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings

Editors: **Lecomte**, Thierry, **Pinger**, Ralf, **Romanovsky**, Alexander (Eds.)

ROYAL ACADEMY OF ENGINEERING

Cyber safety and resilience

strengthening the digital systems that support the modern economy

Kate Netkachova and Robin Bloomfield, City, University of London; and Adelard LLP

Bloomfield, R. E., Bendele, M., Bishop, P. G., Stroud, R. & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspective Methodology and lessons learned. Paper presented at the First International Conference, RSSRail 2016, 28-30 Jun 2016, Paris, France.

CYBERTRUST

PAS 11281

Connected automotive ecosystems – Impact of security on safety – Code of practice

September 2018

CPNI
Centre for the Protection of National Infrastructure

RAIL CODE OF PRACTICE FOR SECURITY-INFORMED SAFETY

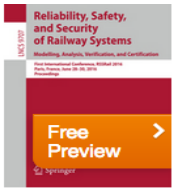
A GOOD PRACTICE GUIDE

OCTOBER 2018 (DRAFT)

-Informed
Supporting
lders with
f Practice

shop, Adelard LLP and City, University

engineers think, in order to make "security mindedness" a common practice—to consider the impact their work might have on security as well as the impact security may have



Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certificatior

First International Conference, RSSRail 2016, Paris, Fran June 28-30, 2016, Proceedings

Editors: **Lecomte**, Thierry, **Pinger**, Ralf, **Romanovsky**, Alexander (Ed

Bloomfield, R. E., Bendele, M., Bishop, P. G., Stroud, & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspecti Methodology and lessons learned. Paper presented at the First International Conference, RSSRail 2016, 28-3 Jun 2016, Paris, France.

ROYAL ACADEMY OF ENGINEERING

Cyber safety and resilience

strengthening the digital systems that support the modern economy

CITY UNIVERSITY LONDON

Assuring autonomy

Enclosure 2

Lloyd's Register Foundation

UNIVERSITY of York

Assuring Autonomy International Programme
Expression of Interest Form – Call 01

Towards Identifying and closing Gaps in Assurance of autonomous Road vehicleS
(TIGARS)

ADELARD

WITZ

INFORMATION SCIENCE NAGOYA UNIVERSITY

CITY UNIVERSITY LONDON

KANAGAWA UNIVERSITY

90th ANNIVERSARY SINCE 1928

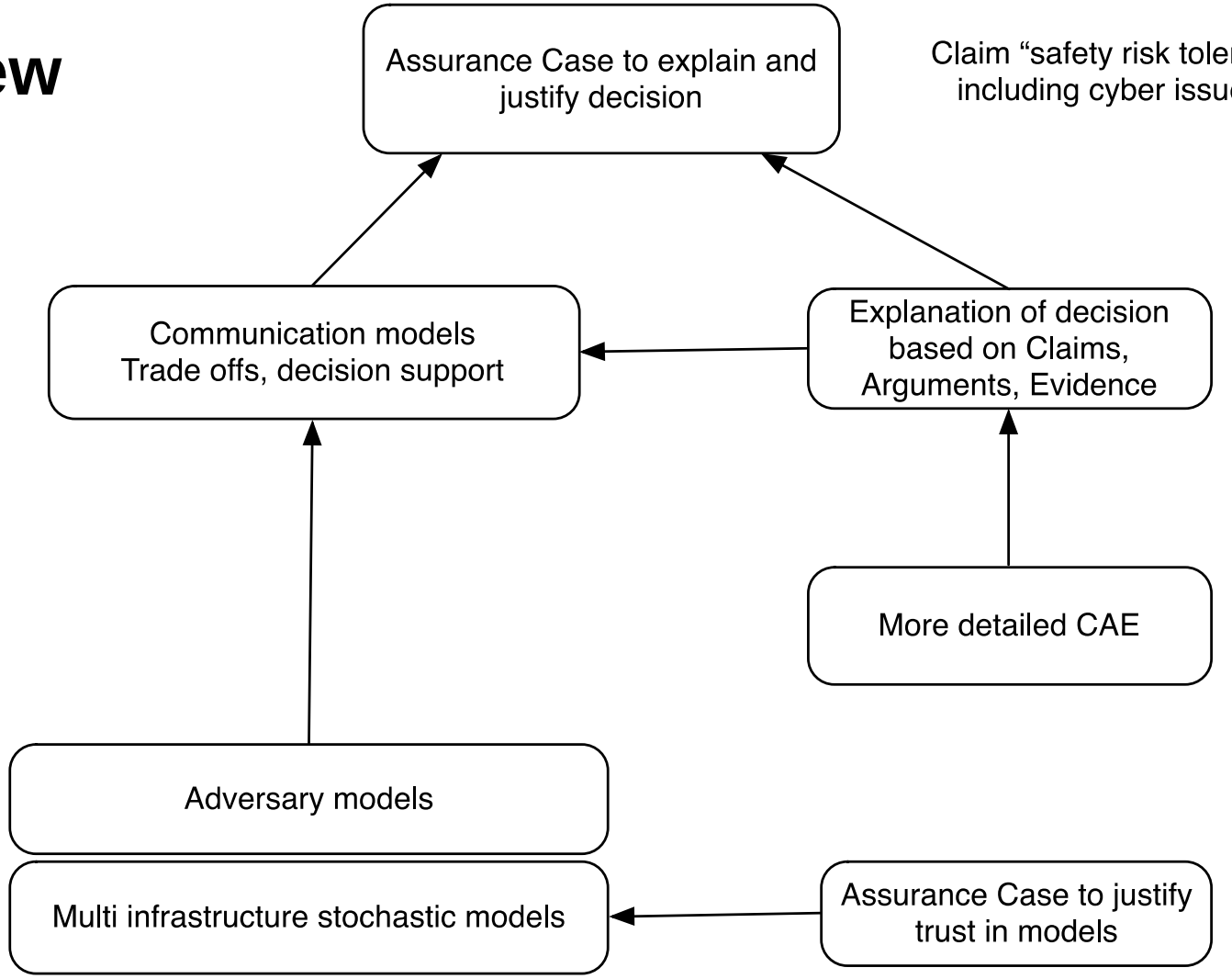
CITY UNIVERSITY LONDON

Short term

- Landscape and road mapping
  - Identify issues with practitioners
    - Transport, Nuclear,
    - Resilience community
  - Develop issues
    - Breadth and selective depth
  - Combine
    - Technology and threat awareness
  - Develop R&D roadmap
- Progress research
  - Tempo and agile assurance cases
  - Model based trade-off analysis

CITY UNIVERSITY LONDON

Overview



PIA FARA

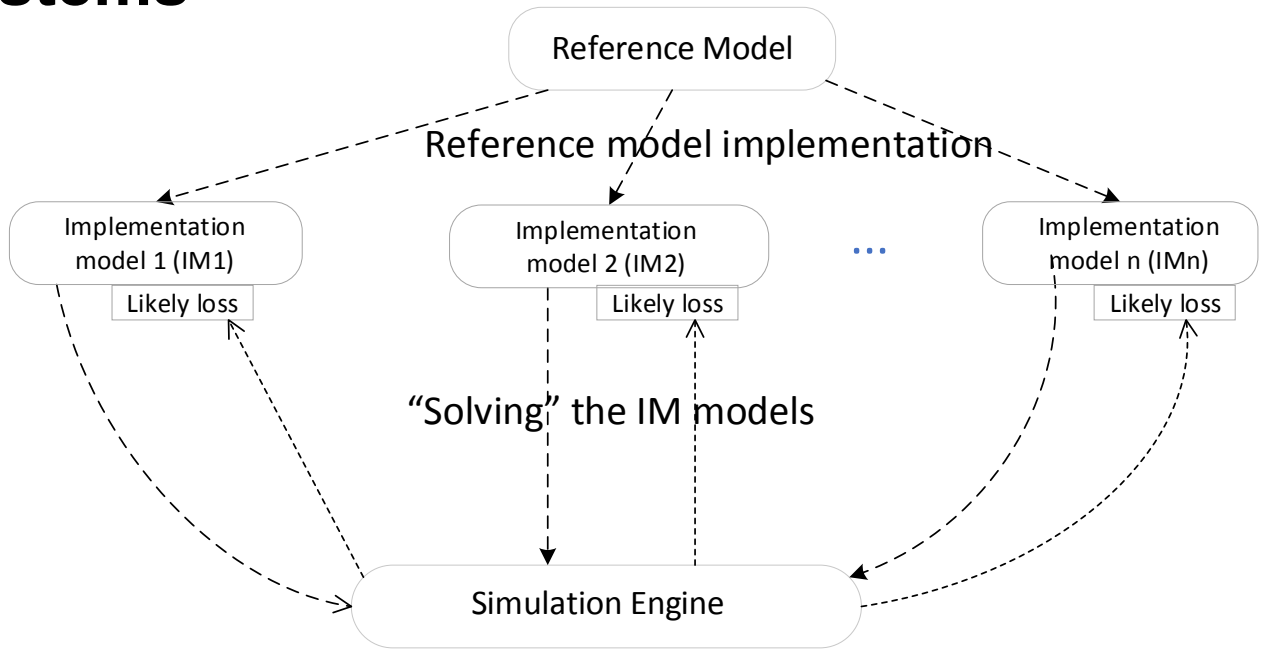
CITY UNIVERSITY LONDON

Safety and Security: trade-off analysis

- Trade-offs analysis between safety and security is often done qualitatively. The modelling approach to resilience improvement offers a quantitative alternative.
- Trade-offs between safety and security may be subject to review and change throughout the development process and after deployment
  - e.g. targets decided early may become infeasible or new threats may emerge
- We will scope tool support for quantitative trade-off analysis which covers the entire product life-cycle of safety-critical development: from feasibility to maintenance.

CITY UNIVERSITY LONDON

Model-driven approach to improving cyber- resilience of complex systems



- Explore role of ***reference model*** will assist decision makers to identify the space of credible alternatives.
- Compare using high-fidelity models, which will be derived for the specific "base-line" system and solved using PIA:FARA tools, designed to do that.

CITY UNIVERSITY LONDON

Short term

- Landscape and road mapping
  - Identify issues with practitioners
    - Cross sector …Transport, Nuclear, Electricity ..
    - Resilience community
  - Develop issues
    - Breadth and selective depth
  - Combine
    - Research, technology and threat awareness
  - Develop R&D roadmap
- Progress research
  - Tempo and agile assurance cases
  - Model based trade-off analysis