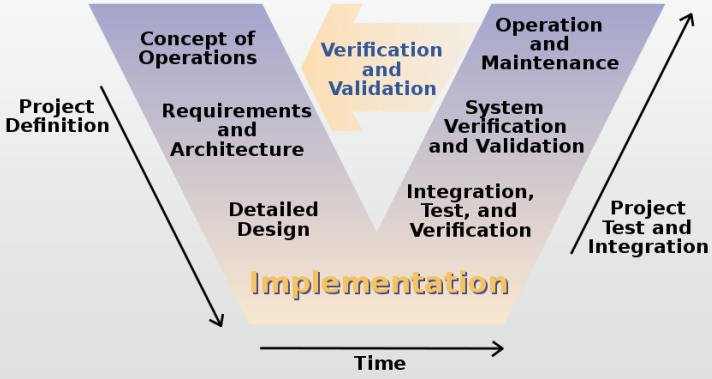
UNIVERSITY OF Southampton

Research in software design, safety and test

Michael Butler

Electronics and Computer Science

www.ecs.soton.ac.uk/people/mjb



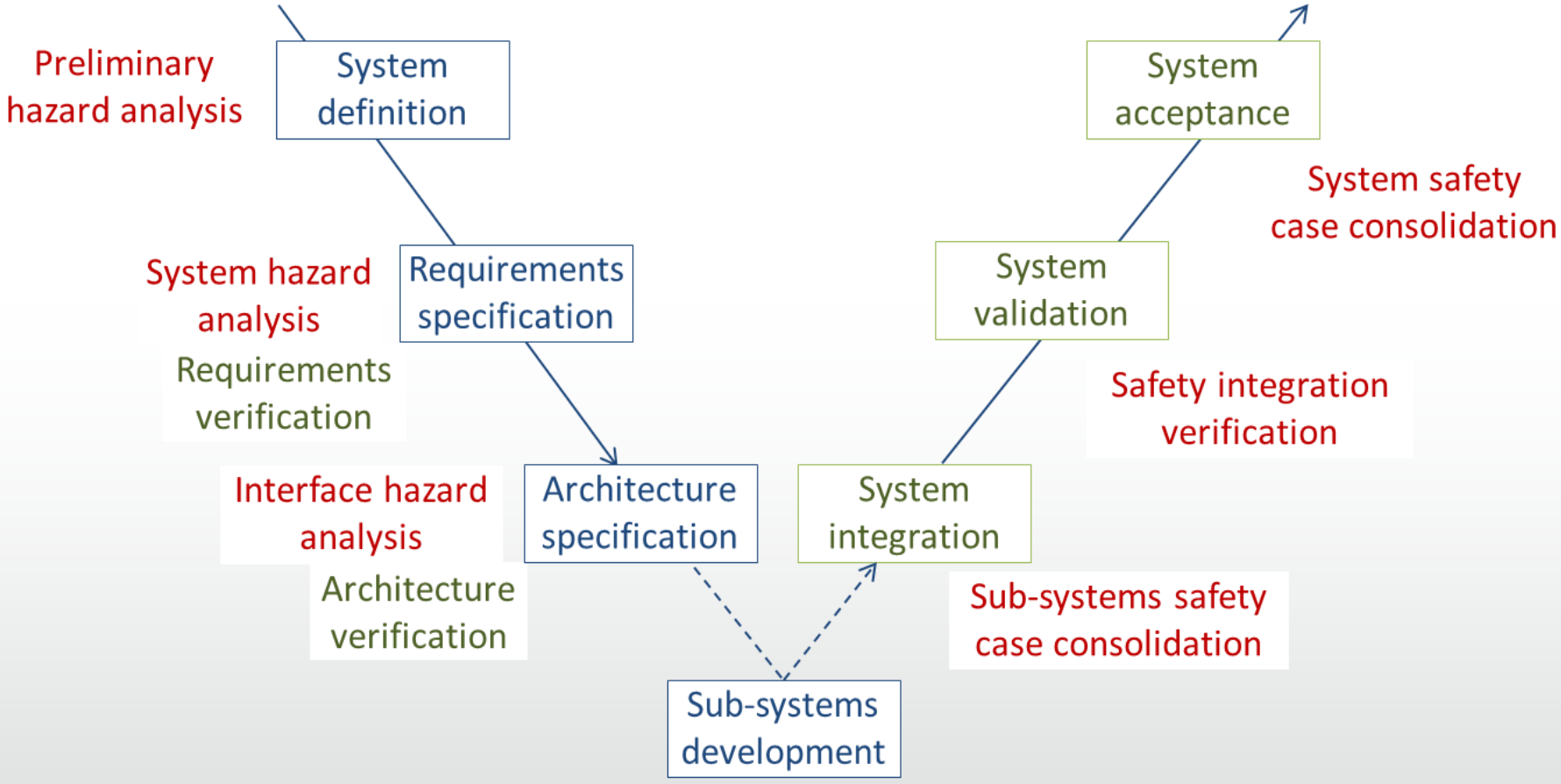
UNIVERSITY OF Southampton

Engineering Cyber-Physical Systems (CPS)

- CPS: Integrations of software, electronics, sensing, information, intelligence/autonomy, networking, mechanics,
- Domains: Aerospace, Automotive, Defence, Rail, Utilities, Medical, Manufacturing, Exploration, …
- Engineering challenges:
  - *Safety* increasingly depends on *complex software*
  - Networking increases *cyber threats* to operation and safety
  - Software and electronic *design* and *assurance* dominating *engineering costs*

UNIVERSITY OF Southampton

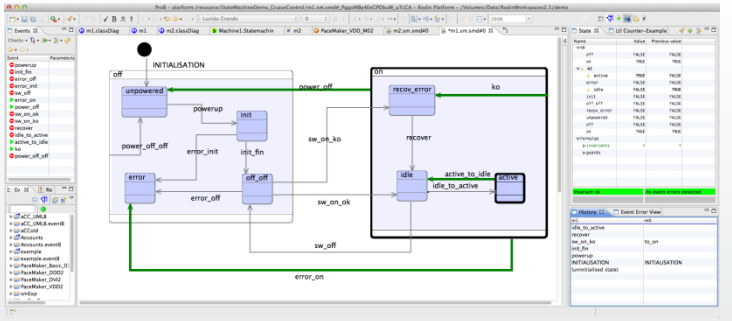
Safety Lifecycle with Formal Modelling

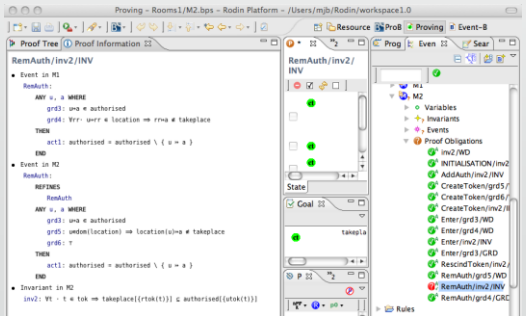


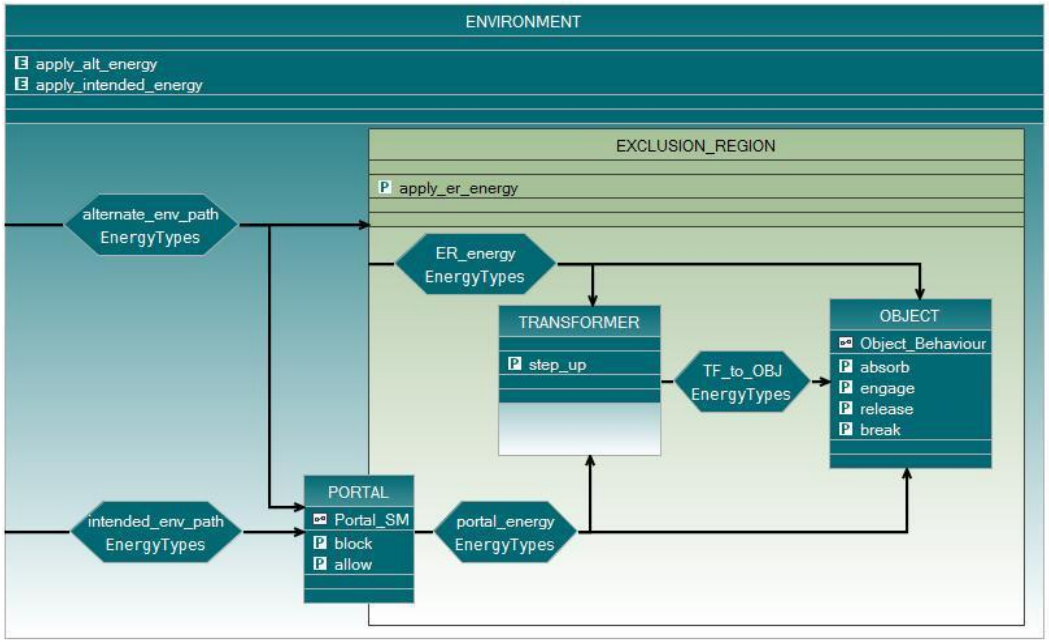
UNIVERSITY OF Southampton

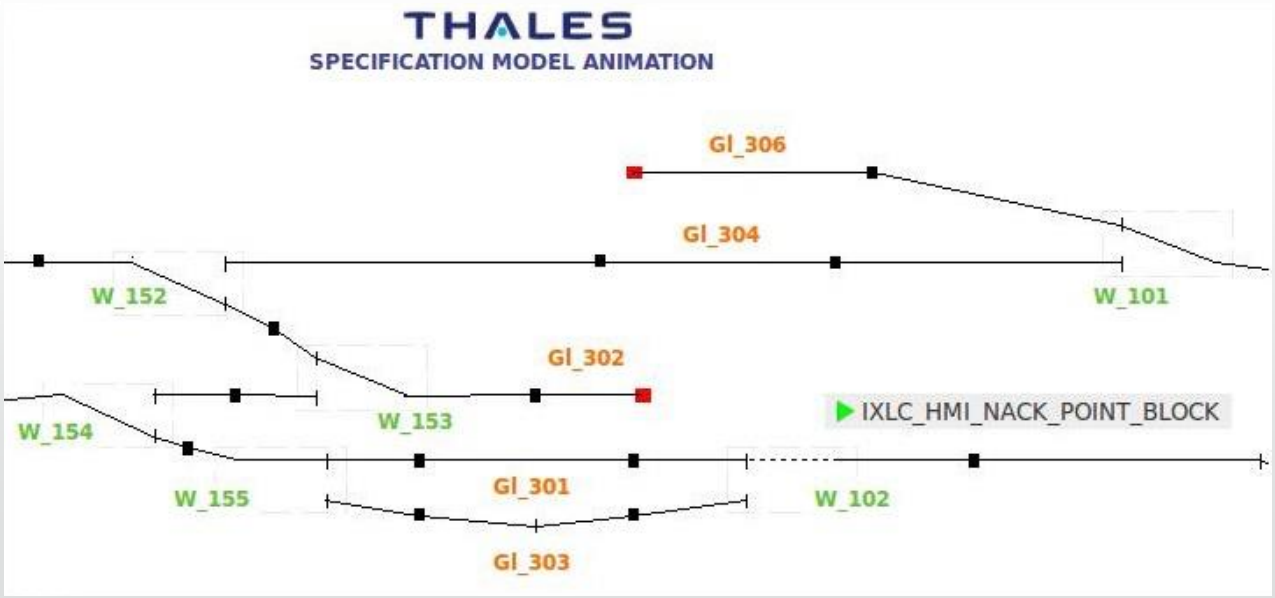
Formal model-based engineering

- Lead: Michael Butler
- Model-based CPS design with Event-B www.event-b.org
  - All stages – early identification of flaws - reduce costs
  - Hazard/vulnerability analysis and mitigation
  - Provide V&V evidence for high assurance
- Open source Rodin toolset supporting
  - Incremental modelling
  - Automated formal verification
  - Co-simulation
  - Visualisation
  - Functional test generation/coverage
  - Code generation









UNIVERSITY OF Southampton

UoS in industrial projects on SW V&V

- AWE/UoS: V&V of safety-critical embedded systems
- Sandia Labs/UoS: V&V of safety-critical embedded systems
- Imagination Technologies/UoS: V&V of many-core memory transactions
- DSTL ASUR Programme/Tekever/UoS: V&V of safety of UAV movements
- SECT-AIR, Aerospace Technology Institute Programme, 3 Year, £10M
  - Methods and Tools for aerospace software V&V
  - Rolls Royce, BAE, GE, MBDA, Selex, Cobham,..., UoS, U. Oxford, U. York,
- ENABLE-S3, EU H2020 ECSEL Programme, 3 Year €68M
  - Methods and tools for safety and security of CPS
  - >50 EU partners
  - Thales/UoS: V&V of railway interlocking product families

UNIVERSITY OF Southampton

Code level Software verification

- *Leads: Dr Gennaro Parlato, Dr Denis Nicole*
- Model checking: algorithms and tools
- ESBMC www.esbmc.org
  - SMT model checker for embedded C/C++ software
  - arithmetic under- and overflow, pointer safety, memory leaks, array bounds
  - multi-threaded software: atomicity and order violations, deadlock and data race

University of Southampton

Internet of Things – IoT@ecs

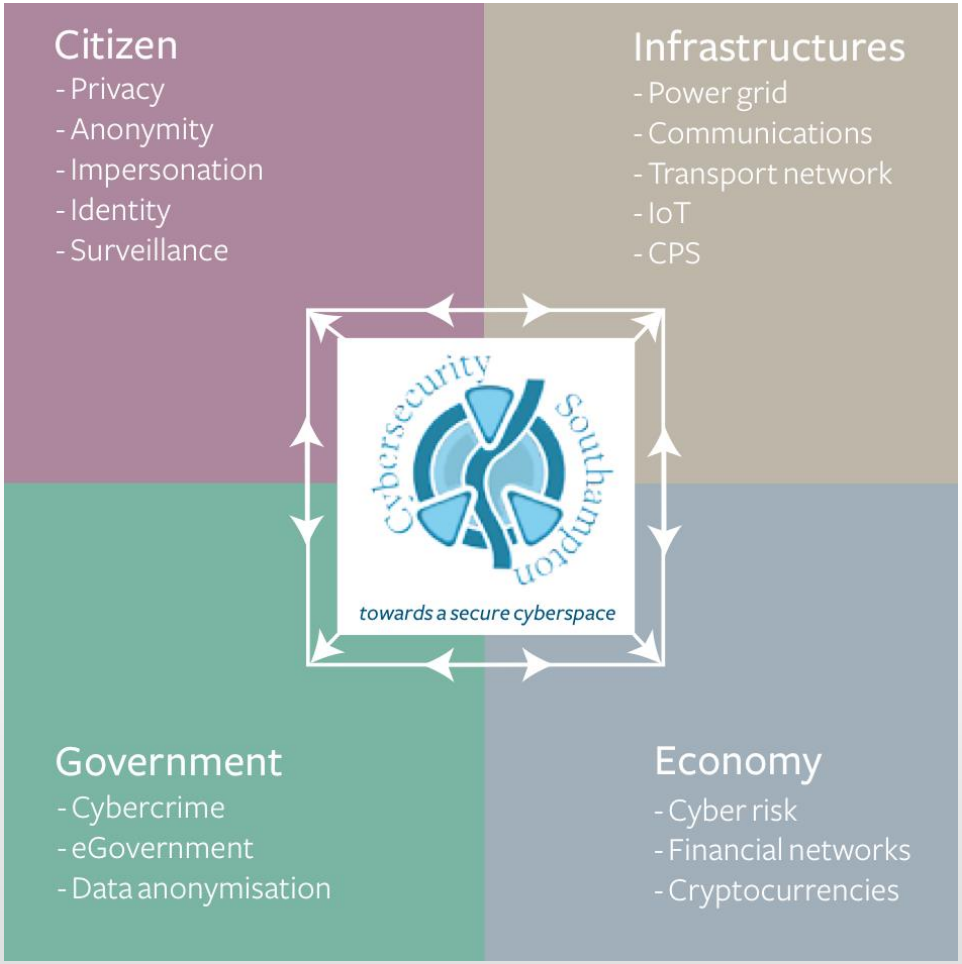
- *Champion: Dr Geoff Merrett*
- Applications
  - environmental monitoring, condition monitoring of infrastructure, …
- Networked sensing
- Wireless communications
- Software and hardware security
- Embedded intelligence
- Low power design, energy harvesting

Cyber Security Academy

- *Lead Prof Vladimiro Sassone*
- Industry/University partnership to advance cyber security through:
  - world class research
  - teaching excellence
  - industrial expertise
  - training capacity

UNIVERSITY OF Southampton

Cyber Security research



University of Southampton

Cyber Security Academy activities

UNIVERSITY OF Southampton

Power-efficient, Reliable, Many-core Embedded systems
£5.6M, 2013-2018

Lead Prof Bashir Al-Hashimi

EPSRC
Engineering and Physical Sciences Research Council

Knowledge Transfer Network
Electronics, Sensors Photonics

nmi Together We're Better

Knowledge Transfer Network
ICT

UNIVERSITY OF Southampton

Imperial College London

MANCHESTER 1824
The University of Manchester

Newcastle University

ARM

Imagination

ALTERA

freescale semiconductor

Microsoft Research

Runtime adaptive management

Step change in energy reduction and reliability improvement through **cross-layer system optimisation**