CITY UNIVERSITY
LONDON

An introduction to the AQUAS project

Aggregated Quality Assurance for Systems

A collaborative project to advance co-engineering of safety, security, performance

Lorenzo Strigini
Centre for Software Reliability, City University London, U.K.

funded by
EU ECSEL

AQUAS SAFETY SECURITY PERFORMANCE

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Aggregated Quality Assurance for Systems (AQUAS)

investigating Co-Engineering techniques for safety, security and performance in critical and complex embedded systems

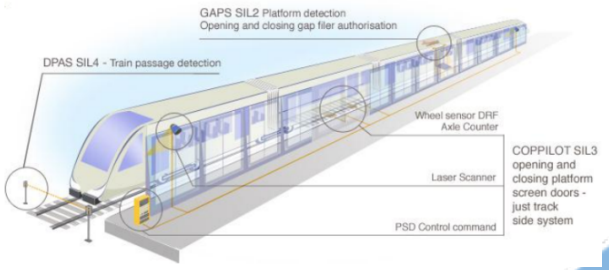
I will sketch the problems addressed and approach followed

- as of interest in this community
- to invite interest comments and interaction

AQUAS Partners

23 partners in 7 countries

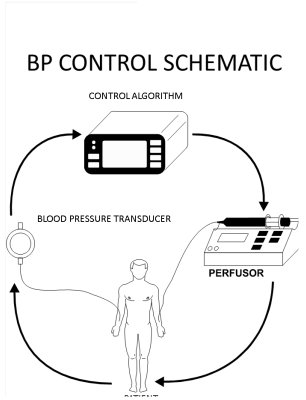
Application Domains

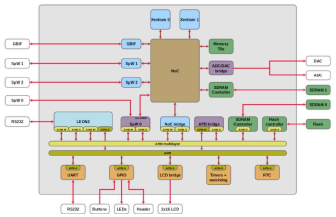


Rail Carriage Mechanisms

Air Traffic Management

Medical Devices





Space Multicore Architectures

Safety, Security, Performance, System modelling

Industrial Drive

External Domains

Background

- embedded systems – long tradition of engineering for safety

  in the absence of attacks
- integration of security concerns still complex, problematic
  - different cultures within companies
  - safety & security people speak different languages, use different concepts
  - often different emphasis
    + e.g. safety people favouring "immutable" designs verified for the long term
    + vs security people desiring fast change to address new threats
  - often requiring trade-offs in design
    + e.g. comms encryption bringing delays that threaten real-time requirements for reliability, safety
    + missing a conflict may cost expensive design rework, or worse
- uneasy evolution in standards
  - with strong opinions about approaches, resistance to change

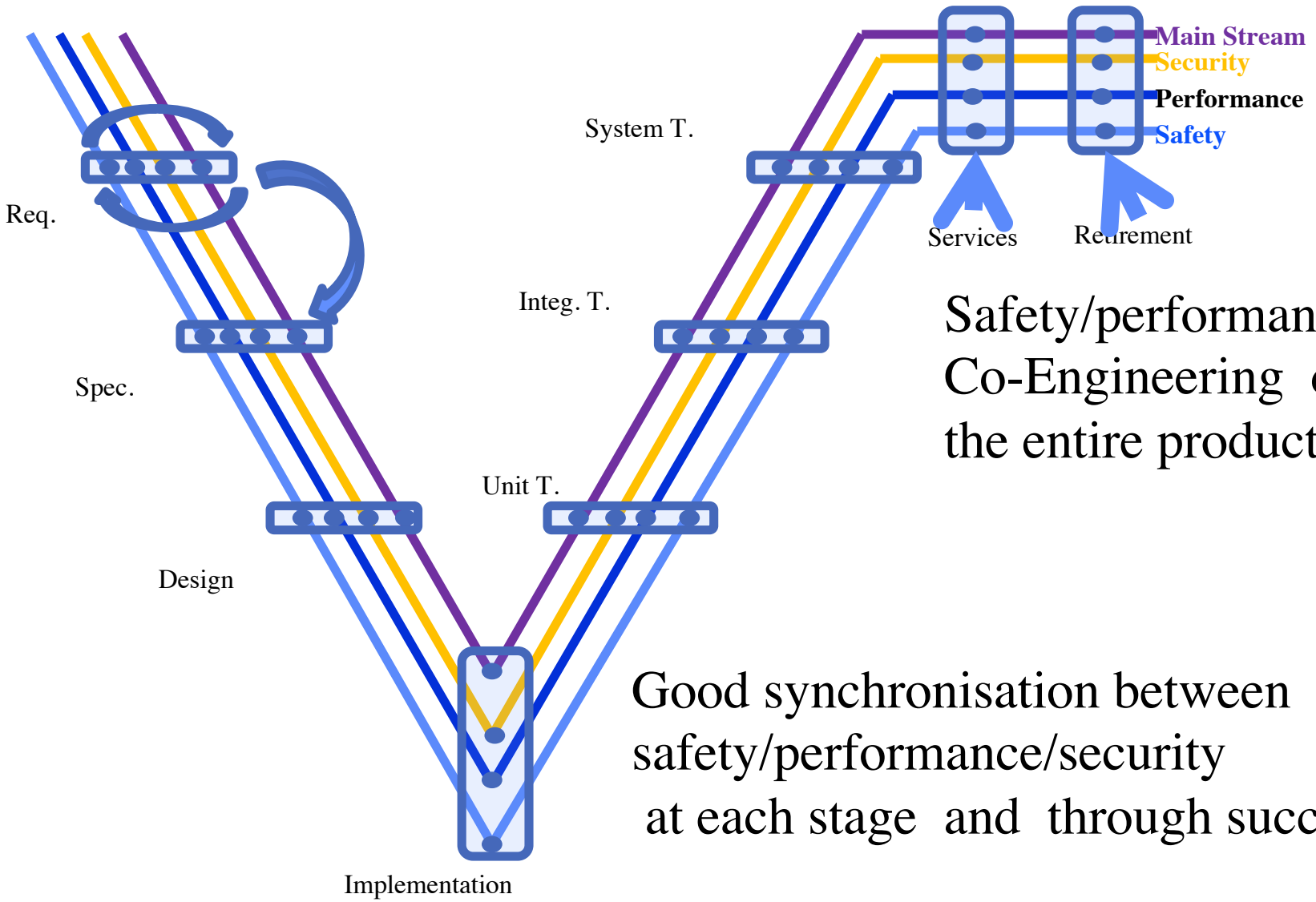
AQUAS aims at advancing ...

- co-engineering for these various qualities at system and subsystem level
  - integrated in current development processes
- supported by tools
  - for detailed modelling of function allocation and timing (e.g. SysML models integrated with WCET estimates
  - for V&V (e.g. formal verification of specs, of code)
  - for probabilistic modelling
  - for documenting certification and assurance cases
  - exploring the concept of *interaction points*
  - through 'use cases' in diverse application areas
- with goal to influence industrial practice and standards

CSR-City's team co-ordinates the *methodology* workpackage

plus more specific analysis work, e.g. combined reliability/safety modelling with attacks and failures, human-machine aspects

The need



Safety/performance/security Co-Engineering comprises the entire product lifecycle.

Good synchronisation between safety/performance/security at each stage and through successive stage

"Interaction points"

- there is an ideal view of how all tis should be done :
  - system "design models" evolve top-down **and** are accompanied all along by evolving integrated verification and certification **with** appropriate coverage of all "non-functional attributes"
- AQUAS follows another view
  - the separate cultures will not magically integrate any time soon [or ever?]
  - "interaction points":
    + points in the lifecycle at which the separate analyses are brought together
    + detecting breaking of contracts agreed at earlier stage of contracts, newly discovered conflicts; managing trade-offs
    + frequent enough to avoid disastrous rework (or deployment)
    + starting crucially with early **risk analysis** stage
  - idea coming from previous industry-academe projects, esp "SeSaMo" (Security and Safety Modelling)
  - approach favoured now in automotive standard environment
    + *cf* e.g. SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", new 26262 std

AQUAS aims at adding practical flesh on this bare-bones concept

What is so difficult with all this?

- combined analysis to deal with more than one concern...
  - e.g. performability analysis? Practiced since 1980s..
  - probabilistic modelling of complex systems subject to failures and attacks?
    + various application examples from colleagues at UIUC..
    + at City, "Preliminary Interdependence Analysis" approach, modelled e.g. power distribution under attack/failure, interdependent infrastructures

    [see papers by Popov & al at openaccess.city.ac.uk]

- So.. why am I claiming that there are hard problems to solve?

What is so difficult with all this?

- ....

- the difficulties
  - need to integrate specialist knowledge, dispersed (e.g. safety vs. security experts) and expressed in heterogeneous languages and models, aided by disparate tools
  - developed differently for valid historical reasons
  - "combined analysis" ≠ "combining separate analyses" that specialists may be very good at
    + e.g. some risks/threats
      ... that will be negligible for experts that focus on accidental hazard only or attacks only
      ... will be shown to be practically relevant when combining the viewpoints

Terminology issues arising with interaction between concerns

[deleted!]

Terminology issues arising with interaction between concerns

- [deleted!]
- will be happy to pick arguments offline
- in the industrial context, "security" means "what the 'security experts' do", and so on
- to avoid being tripped up by words, you need to focus on *risk* only and what creates/controls it
    + e.g. show that an attack type, or human error, or ... matters

Thank you...

Questions, comments?

http://aquas-project.eu/