Security Informed Safety Working Group (SISWG)

How do we manage the impact of (cyber)security on functional safety?

Stephen Bull, Nikita Johnson, Wendy Owen, Paul Hampton

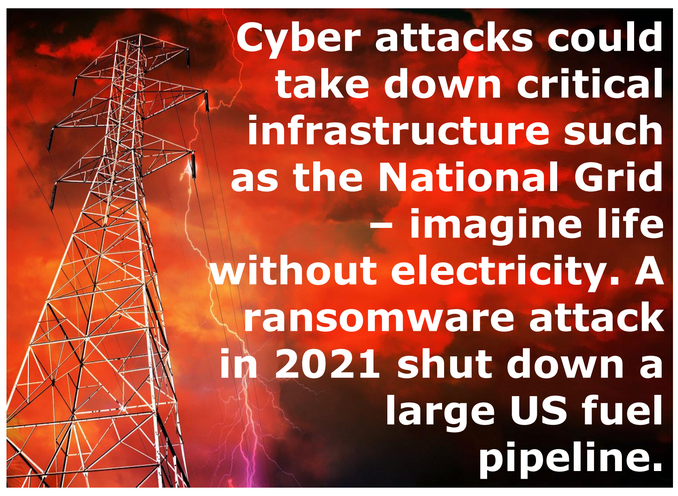
contact: stephen.bull@scsc.uk

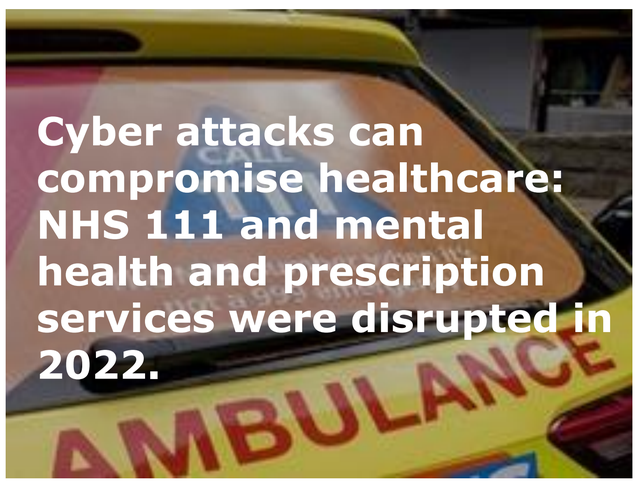


The problem ...

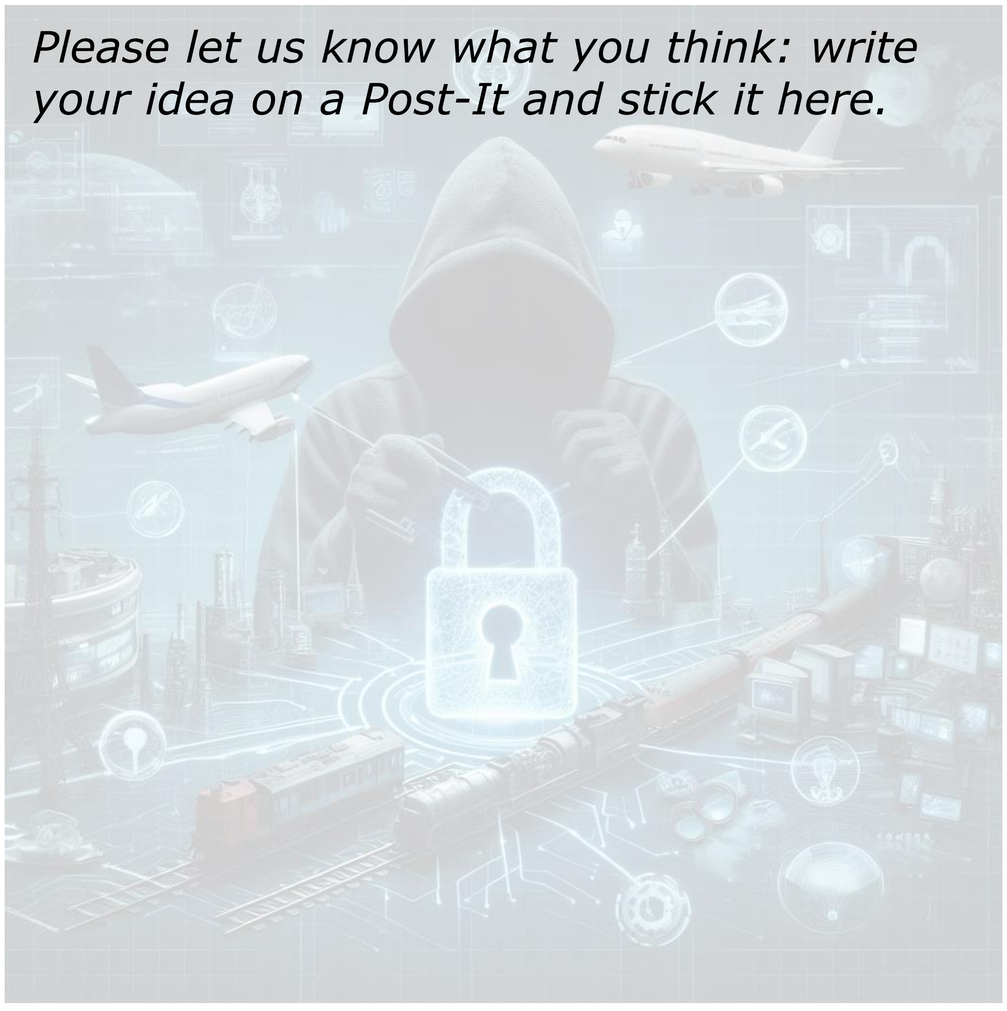
- **(Cyber)security vulnerabilities can be exploited to compromise the safety of systems, causing catastrophic consequences!**
- **This is a complicated and evolving problem as systems become more complex, interconnected and data-driven and threats become more sophisticated.**

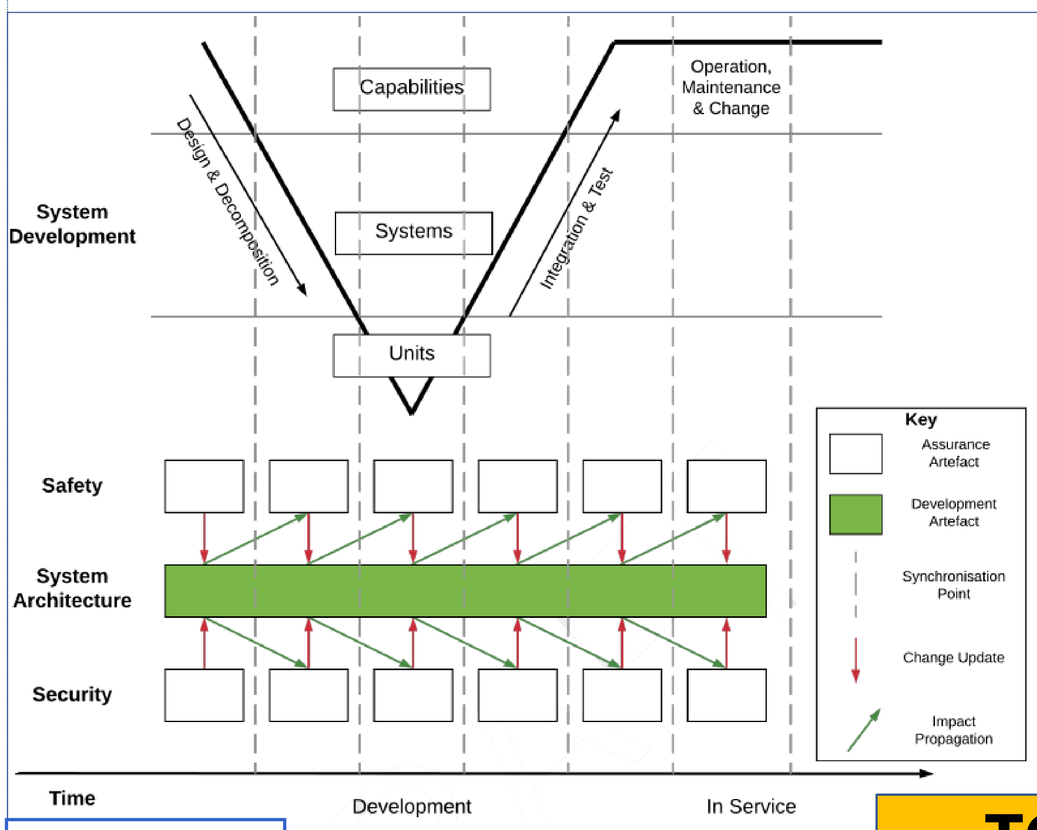
The effects ...





Please let us know what you think: write your idea on a Post-It and stick it here.





Safety-Security assurance framework

- Separate assurance processes, sharing the right information with the right people at the right time.
- Loose coupling across disciplines
- Mutual understanding to facilitate synchronised solution evolution through the whole lifecycle.

Framework Principles:

Which do you find most challenging?

Essential principles:
- Independent Co-assurance
- Synchronisation Points
- Synchronised Lifecycle Phases
- Risk Impact Propagation
- Assurance Surface

Supporting principles:
- Model-based Representation
- Communication by Artefacts
- Separation of Concerns
- Proportionality

scsc.uk/gi

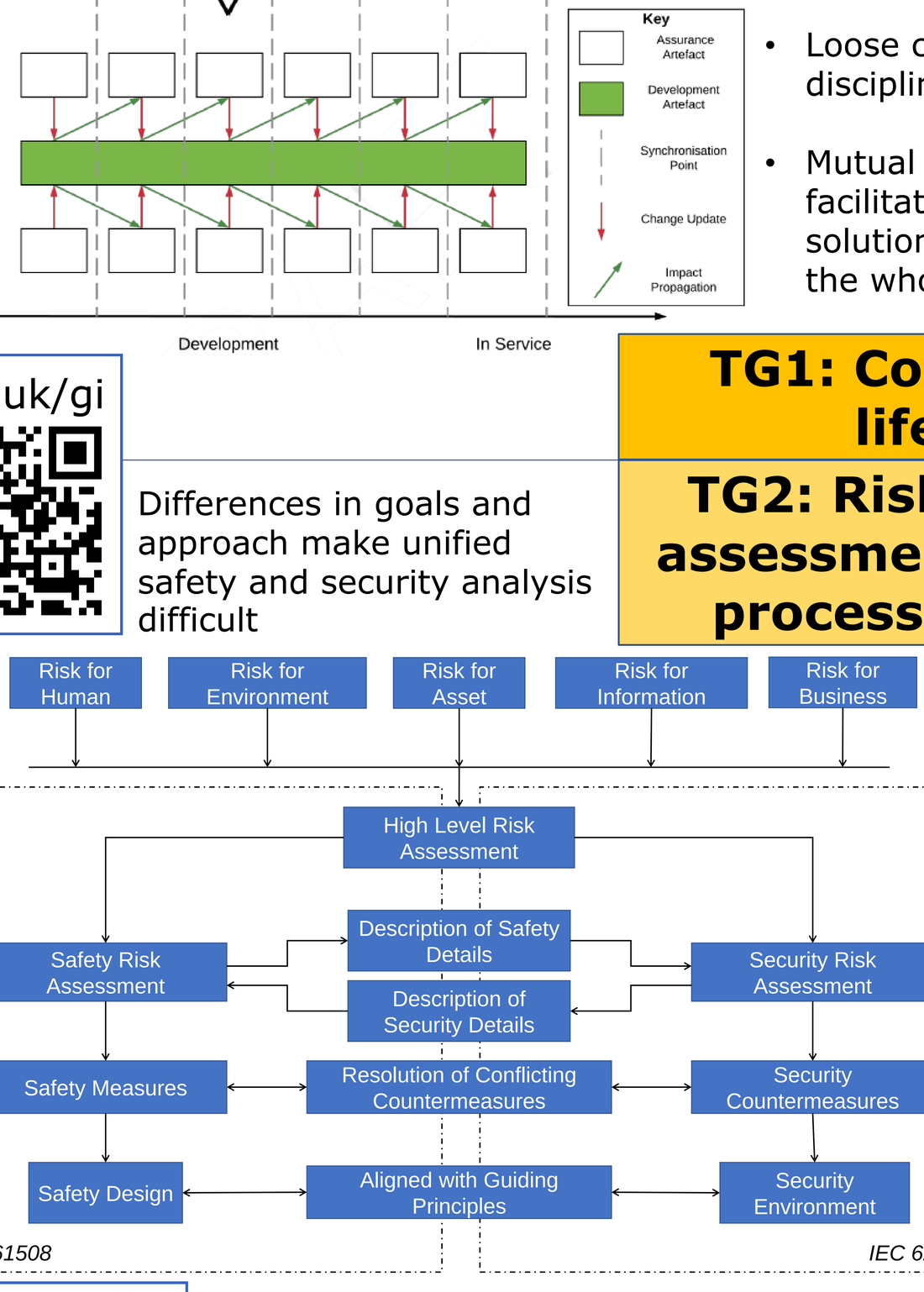
Differences in goals and approach make unified safety and security analysis difficult

TG1: Co-assurance lifecycle

TG2: Risk assessment process

TG3: Common language

TG3 material bridges the language gap between safety and security to aid understanding.



TG2: Key topics

We are developing guidance on the following topics:

- Incorporating security threats into safety analysis
- Risks emerging during operation
- Trade-off between risks

What other guidance would you like to see? Stick a Post-It here.

Poster sponsored by Ebeni

Illustration of a possible risk assessment process: TG2 will provide guidance on addressing security within safety processes.