Standards, Changes and Supply chain

High Integrity Software Conference

Lucia Capogna - 22nd October 2024

SYSTRA

SYSTRA: A global leader for transportation solutions

SYSTRA is one of the world's leading engineering and consulting groups specialising in public transport and mobility solutions

+65 YEARS

Figures as at end of 2023

A turnover of **€1.071Bn**

76% of turnover achieved abroad

Orders of **€1.3 Bn**

An operational presence in **80 countries**

SYSTRA has contributed to **1 in 2** High-Speed lines in the world (>250 kph, outside China)

SYSTRA has designed **1** Metro network in service out of **2** in the world

SYSTRA

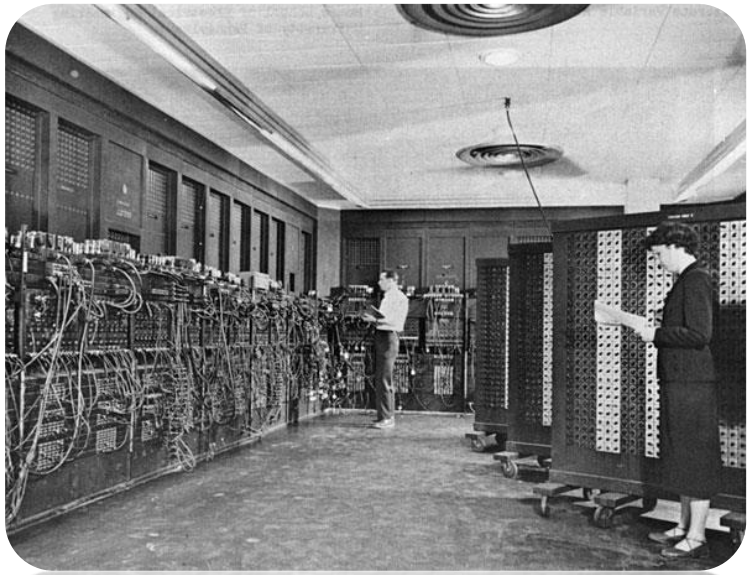
About me

Lucia Capogna

Cyber Security and Software Assurance Team Leader

- Computer Science Engineer (BSc) and Systems Engineer (MSc) with over 17 years of experience in Software, Cyber Security, Requirements Management and Verification & Validation across various industries:
  - Software and Software Assurance Technical Expert
  - Independent Lead Assessor
  - Cyber Security Technical Expert
- Member of several CENELEC (Safety – EN 50129, Cybersecurity - TS 50701 & Software – EN 50716) and IEC Standardisation Groups (Cybersecurity – IEC 63452)
- School of Engineering, University of Birmingham:
  - Industrial Advisory Board member
  - Royal Academy of Engineering Visiting Professor in OT Cybersecurity
- STEM Ambassador & Woman in Rail (WiR) East Midlands committee member

Digitalisation and Software Intro

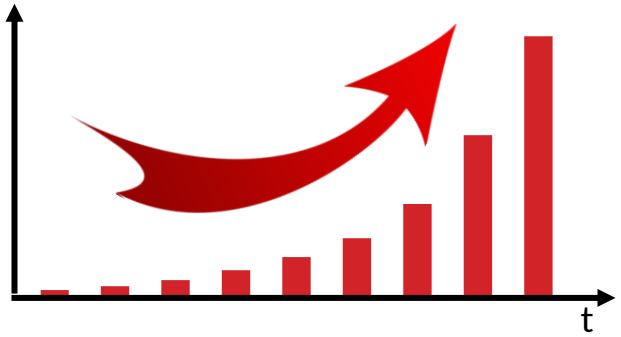


ENIAC (Electronic Numerical Integrator and Computer) - 1945

SYSTRA

Digitalisation – Stating the obvious

Digitalisation has been exponentially introduced in all industries and solutions



- Software is contributing more and more to safety functions.
- System reliability may be affected by poor software quality.
- Many vulnerabilities are due too poor software quality. → Cybersecurity risks!

New technologies and digitalisation provide a railway that is:

- more flexible,
- inter-connected,
- easier to enhance/customise,
- more advanced,
- more responsive to sub-system failures.

Digitalisation is achieved with the introduction of large number of software applications:

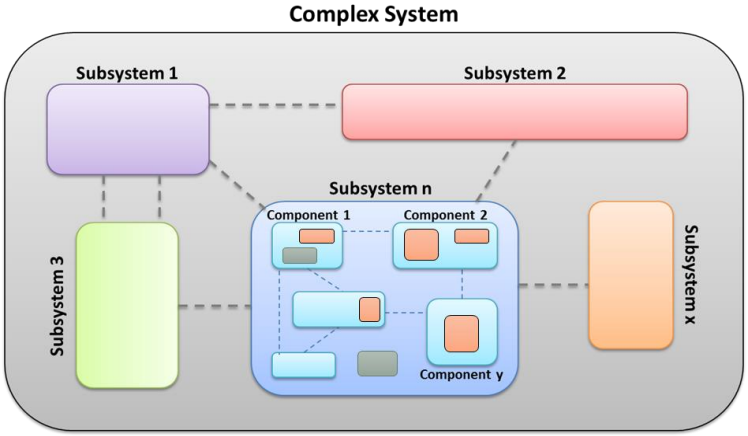
- Systematic failures,
- Unpredictable and almost infinite failure modes,
- Context dependent,
- No exhaustive testing possible

SYSTRA

Software and complex systems

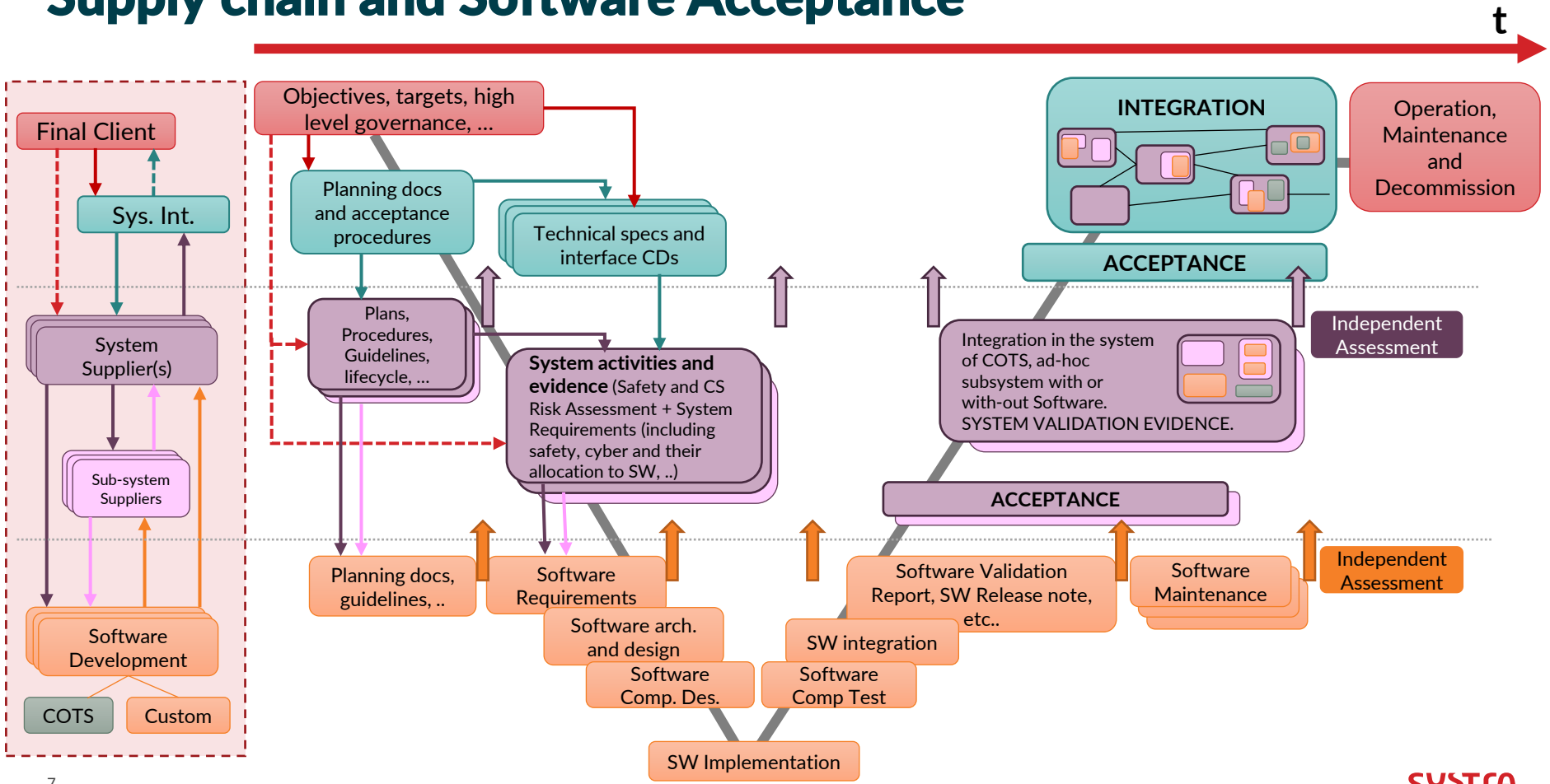
A **complex system** is characterised by the **intricate interactions and interdependencies** among its components. These systems often exhibit **behaviours** and properties **that are not easily predictable from the individual parts alone**. Complexity in such systems can arise from the **interaction** of people, organisations, and the environment, **not just from the technical aspects**.

INCOSE



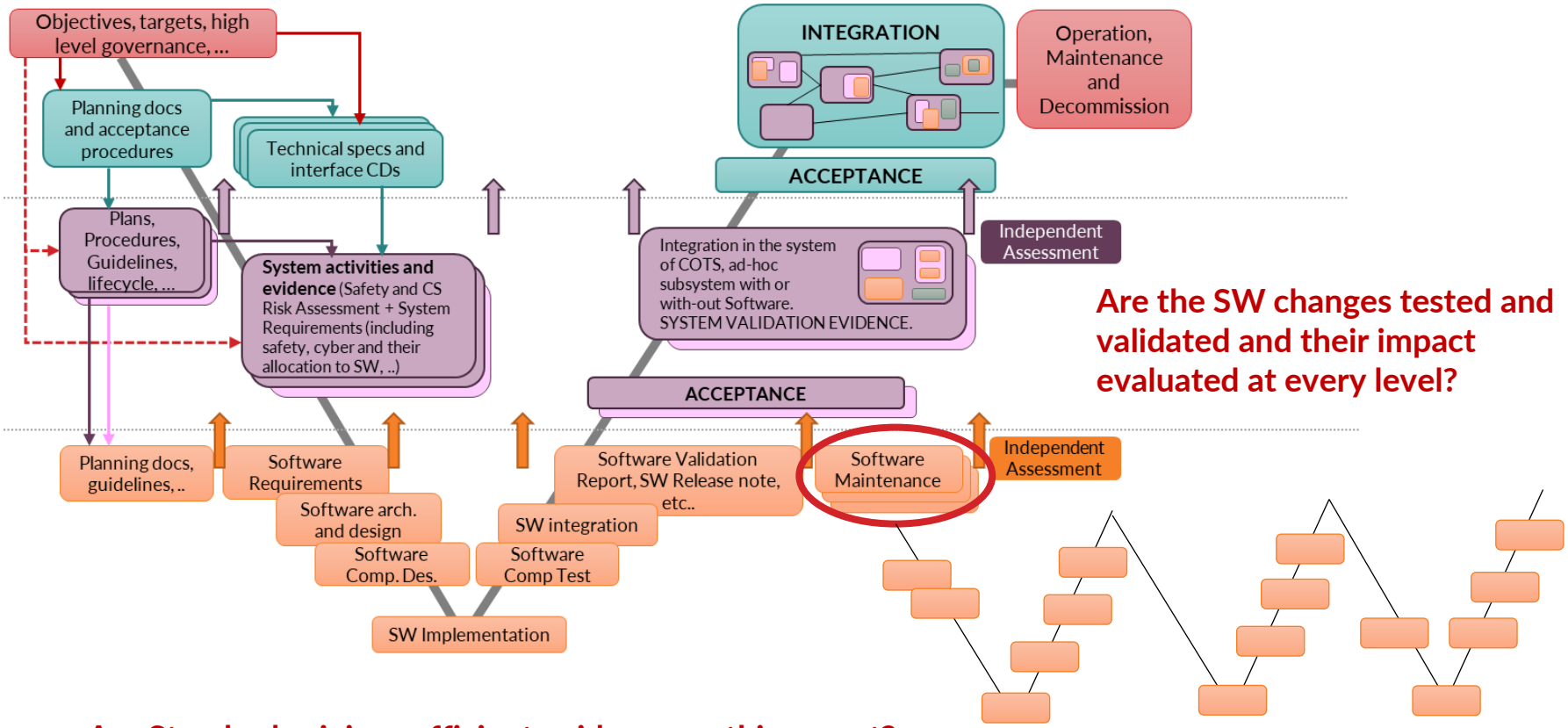
SYSTRA

Supply chain and Software Acceptance



SYSTRA

Software Changes in the systems of system context

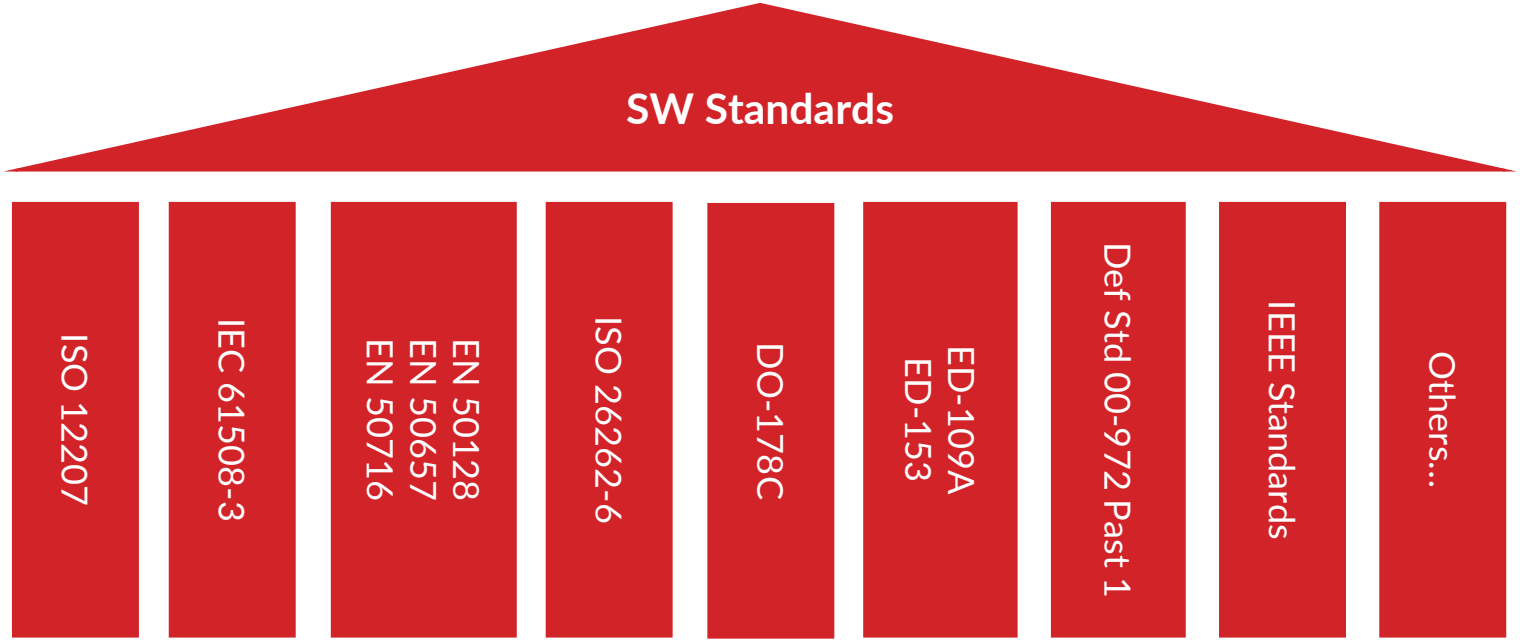


Are the SW changes tested and validated and their impact evaluated at every level?

Are Standards giving sufficient guidance on this aspect?

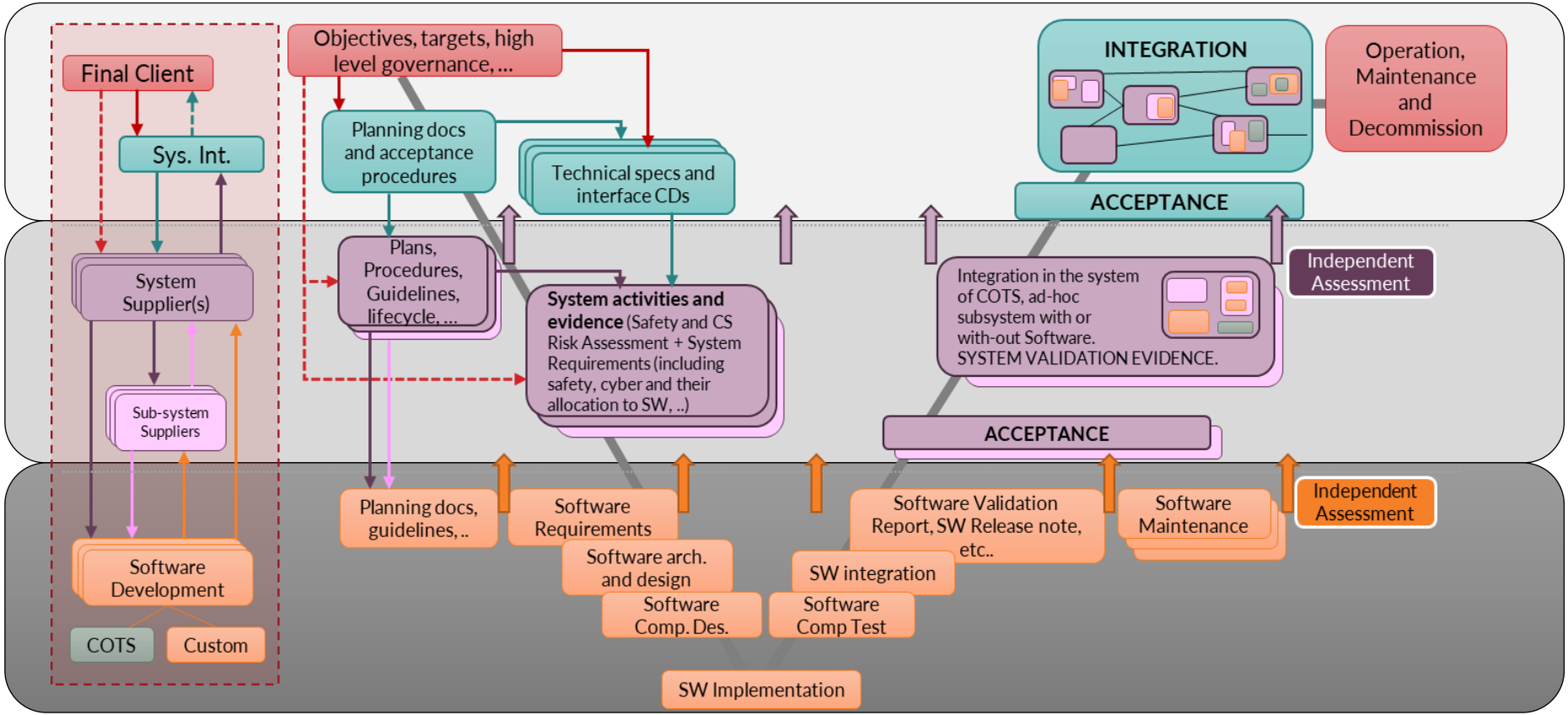
SYSTRA

Standardisation



Do the SW Standards cover the supply chain management or the software acceptance principles and requirements?

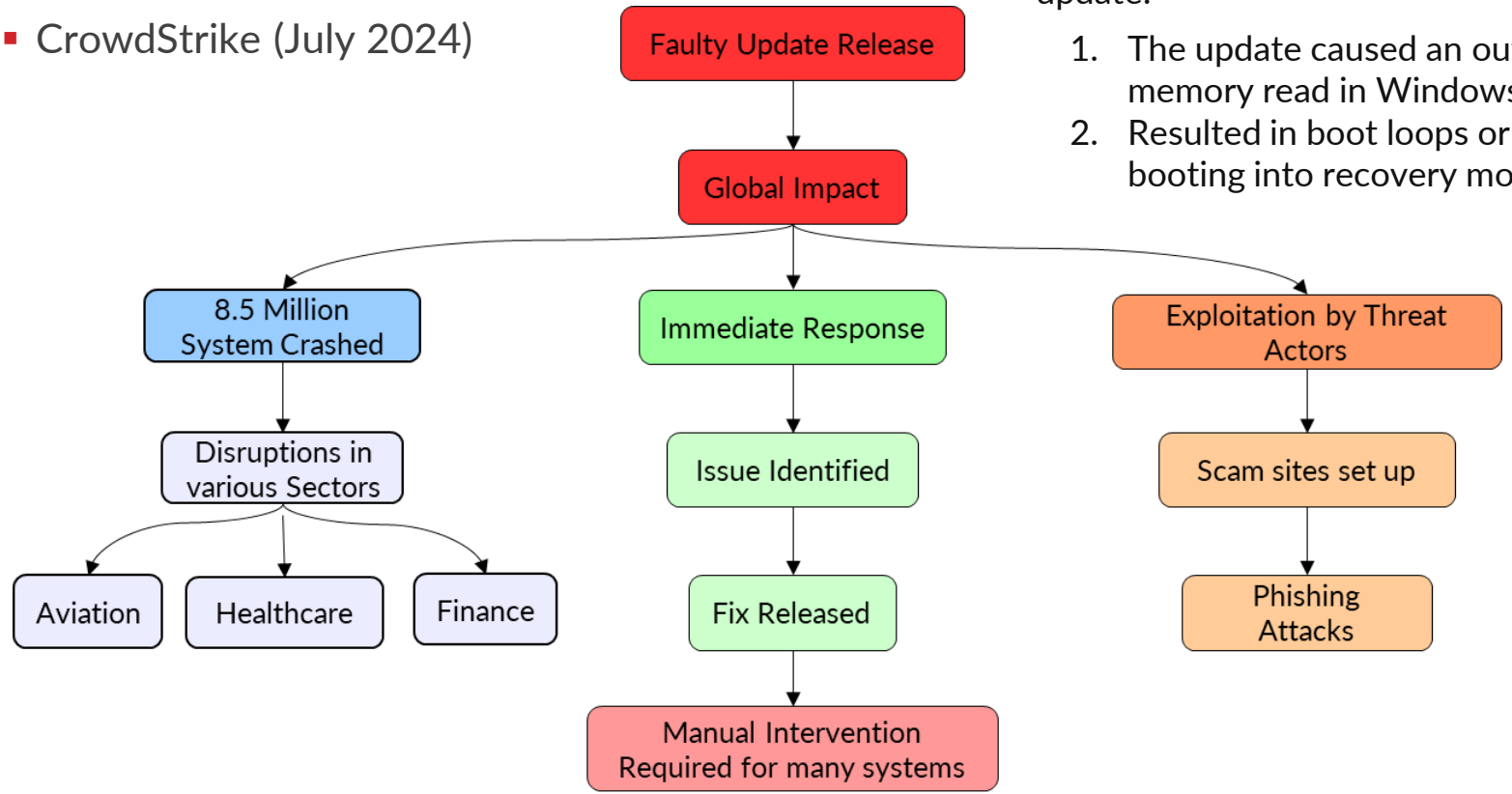
Software Standards



SYSTRA

Example - CrowdStrike

- CrowdStrike (July 2024)

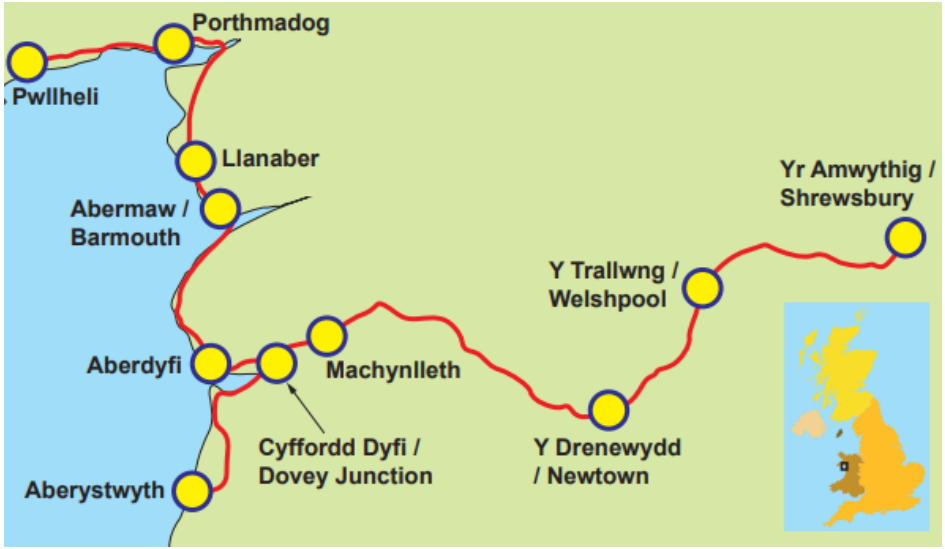


CrowdStrike distributed a faulty configuration update:

1. The update caused an out-of-bounds memory read in Windows systems.
2. Resulted in boot loops or systems booting into recovery mode.

Example – Cambrian Coast Line

- **Cambrian Coast Line, Oct 2017**
  - ✓TSR data not sent via signalling system
    → Loss of safety critical signalling data
    → Excessive speed over Level Crossing
  - ✓The signalling control centre wrongly showed these restrictions as being applied correctly



- ✓TSR data was not uploaded to the RBC (Radio Block Centre) after a software rollover
  → many SW related causal factors, including SW requirements insufficiently defined

SYSTRA

Conclusions

- Industrial automation Standards and sector/industry specific Standards support software development and assurance
- Systems are becoming more complex and integrated/interconnected
- Standards do not cover completely the software supply chain management or the software acceptance in complex systems or in the system of systems context
- Additional best practice and guidance are needed for:
  - Software acceptance
  - Software configuration and compatibility (complex systems/system of systems context)
  - Software change management in a complex supply chain
  - Supply chain management
  - Integration of new technology or new approaches

More information:
systra.com/uk
systra.com/ireland

CONFIDENCE MOVES THE WORLD