THALES

Architecting Railway Systems for Resilience

IRSE ASPECT 2019

Luke Church

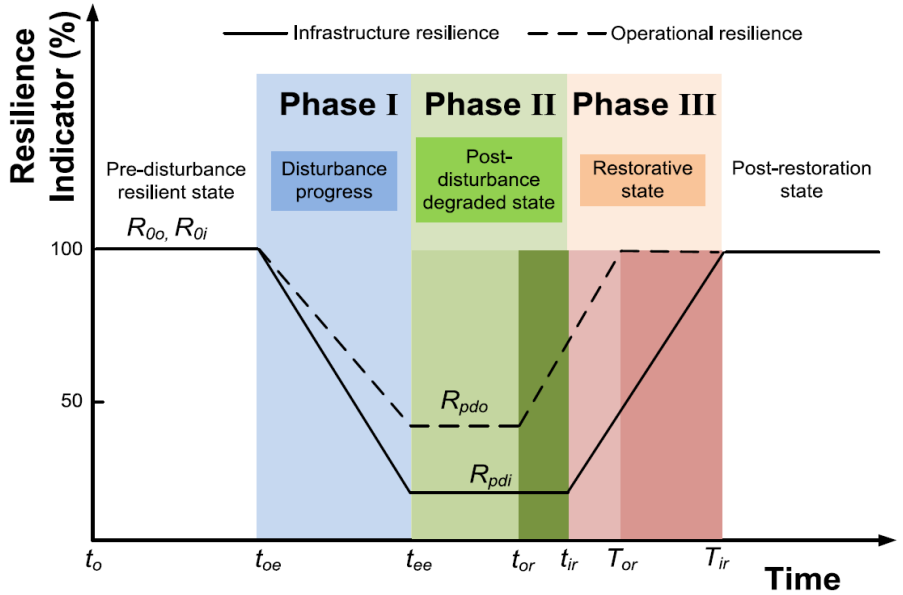
Introduction

Resilience is defined as *"the capacity to recover quickly from difficulties."*

- Maintaining a normal service during minor disruptions and ensuring graceful degradation and swift recovery from major disruptions.

Multi-phase resilience trapezoid; resilience can be enhanced by:

- Graceful degradation and fast stabilisation during phase 1.
- Minimising the duration of phase 2.
- Rapid system restoration during phase 3.



THALES

Principles of Resilience

Capacity

- The ability of a system to withstand disruption in its normal operating state.

Flexibility

- Allows a system to restructure itself when faced with disruption, for example by changing the system architecture or operating concepts.

Tolerance

- Graceful degradation when faced with disruption

Capacity

The capacity attribute can be further broken down into three further attributes

- **Absorption**: Having margins within the system to withstand disturbances.
- **Physical redundancy**: Having back-ups for critical components.
- **Functional redundancy**: Having different means of performing critical functions.

Each of these attributes has been exploited to great effect to deliver resilience to railway systems.

Absorption in Railways

Recovery margins in timetables

- Allows the timetabled service to be achieved without trains being driven at the maximum permitable speed, or with minimum dwell times in platforms.

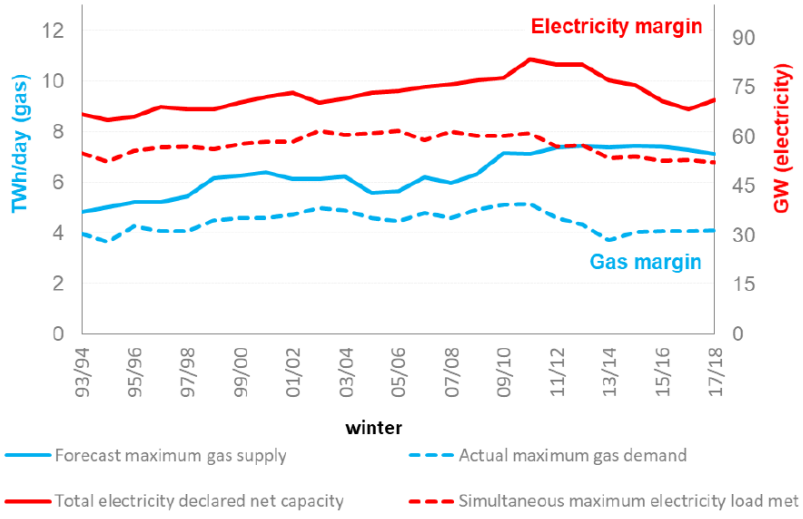
Seasonal timetables

- Leaf fall in autumn.

Direct trade-off between line capacity and recovery margin.

Absorption in Energy Distribution Networks

- **Fluctuations in demand and supply requires supply side infrastructure to maintain a capacity margin**
- **Balance between the cost of spare capacity and need for constant power supply**
- **Smart systems are being deployed to utilise demand-side response.**
  - For example smart charging of electric vehicles, whereby charging is automatically managed to flex with local grid demands



THALES

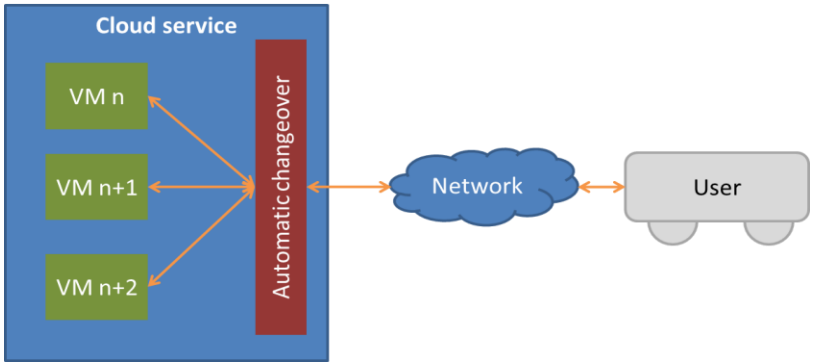
Physical Redundancy

Layered defence against failure, endeavouring to avoid any single points of failure.

- Duplication of critical systems, for example by having a backup as a “hot standby” to switchover to should the primary component fail.

Failure Mode Effect and Criticality Analysis (FMECA) is used to assess redundancy and identify potential vulnerabilities.

Virtual Machines (VMs) and Cloud Computing can be used to enhance redundancy



THALES

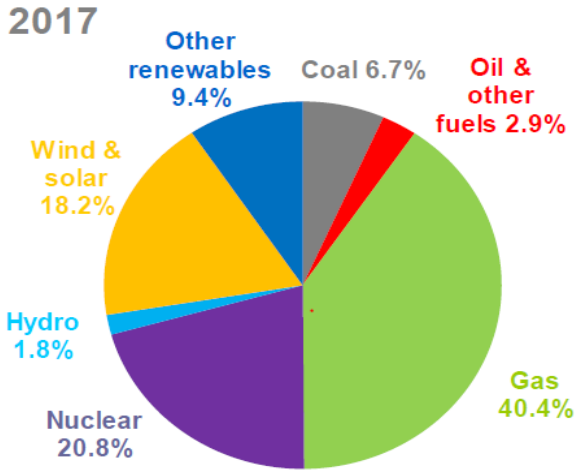
Functional Redundancy

Multiple components of the system performing the same function independently and diversely

- If a component fails it can function with a secondary, fall-back, system.
- High capital cost associated with the design and deployment as well operational cost of maintaining two discrete systems.

Secondary Signalling Systems

- The Downtown Line, in Singapore, uses a CBTC system for Automatic Train Operation (ATO) and also has a coded track circuit system for secondary train detection and fall back ATO train control.



Flexibility

Flexibility allows a system to restructure itself when faced with disruption

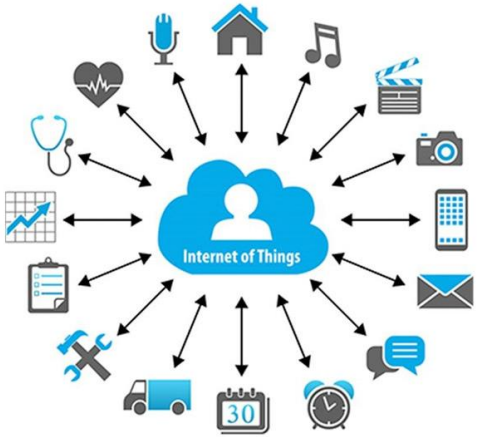
Railways can exhibit flexibility when faced with major disruptions; however these often result in massive reductions in the quality of service

- CBTC systems often utilise secondary train detection in the form of axle counters or track circuits, providing safe train position should the CBTC system fail.
- In this scenario the system is restructured to use fixed block signalling principles.

THALES

Flexibility – Internet of Things (IoT)

Modern communications networks, along with the miniaturisation of technology have enabled the interconnection of physical devices, known as the Internet of Things (IoT).



Signalling systems tend to be highly centralised.

This contrasts with IoT which is highly distributed.

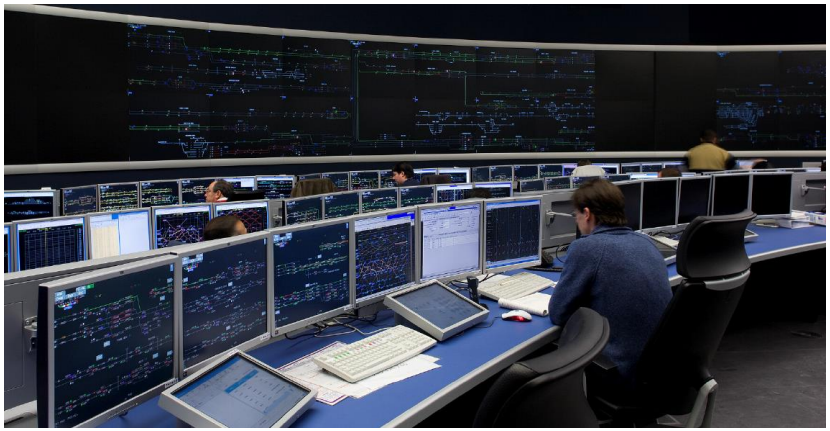
- Signalling systems can use IoT concepts, where the information and intelligence to control the local system is contained within wayside assets and on the train.
- Such system architecture could be highly flexible, with local areas able to operate independently or perhaps take control of adjacent areas in the event of disruption.

Tolerance

Tolerance allows a system to degrade gracefully when faced with disruption.

Traffic Management Systems (TMS) are being deployed to improve tolerance.

- Manipulates the timetable plan in near real-time to return trains to the correct timetable in the most efficient manner possible when there is a disruption.
- Enhancing the networks tolerance to minor disruptions and speed of recovery from major disruptions



Maintainability

Rapid and reliable system restoration can be carried out, using ordinary trained people and reasonable support facilities.

- Speed of fixing a fault so that the system can return to full operational capacity is crucial to minimising service disruption.

Railways have restricted access trackside and are geographically distributed by their nature;

- Minimising trackside intervention needed to conduct both preventative and corrective maintenance activities enhances maintainability

Use of Line Replaceable Units (LRUs).

- Components that can be replaced as a single complete unit by a single person, allowing for fast fault finding and corrective maintenance by replacing an entire LRU on site.

Graceful Degradation

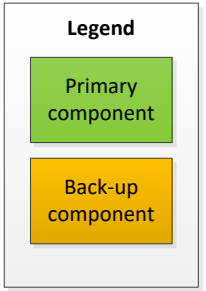
- **Operation with reduced performance during disruption instead of a major or sudden loss of service/ function.**
  - Concept of TMS; however further solutions to ensure the graceful degradation of railway control systems must be explored.
- **In computing low-resolution video is streamed in place of high-resolution when there is insufficient bandwidth is available.**
- **Smart Motorways utilise variable speed limits to increase traffic capacity. This helps to avoid cars bunching and improve average journey times.**

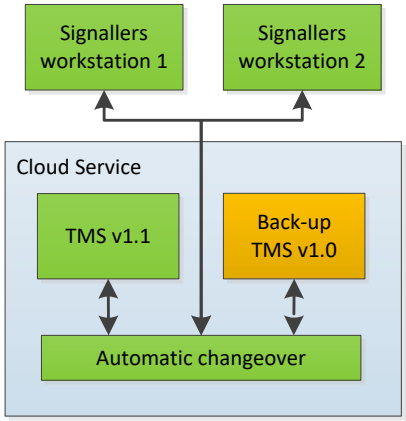
THALES

Designing a Resilient System Architecture

Cloud based TMS

- Hot-standby VMs
- Highly available cloud service provider
- Diverse TMS software

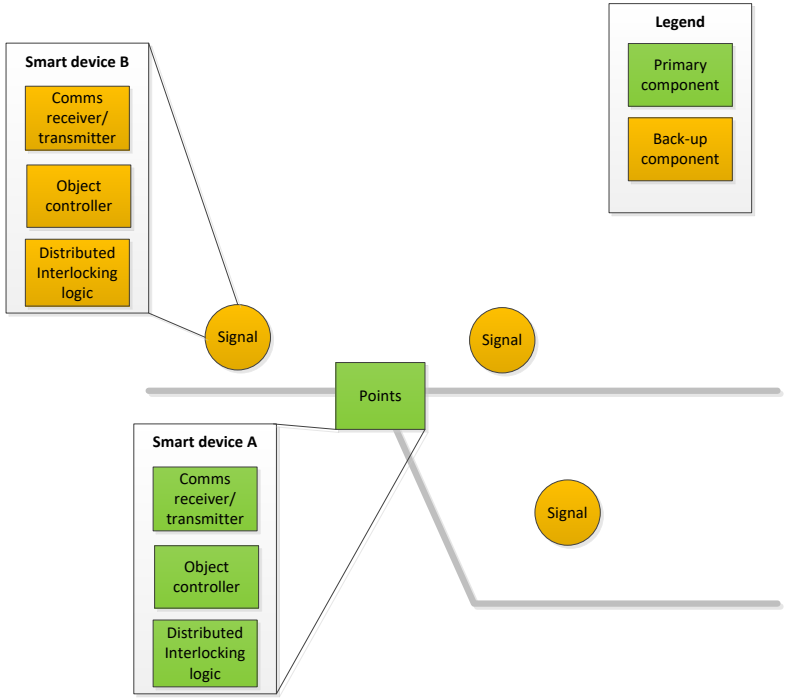




Designing a Resilient System Architecture

Distributed interlocking

- Assets each contain interlocking capability with duplicated functions
- Smart devices capable of taking over adjacent signalling areas

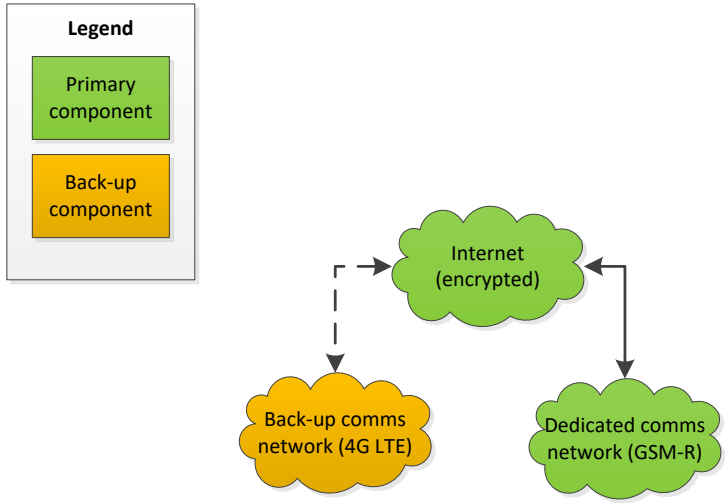


THALES

Designing a Resilient System Architecture

Fall-back communications network

- Dedicated GSM-R and public networks

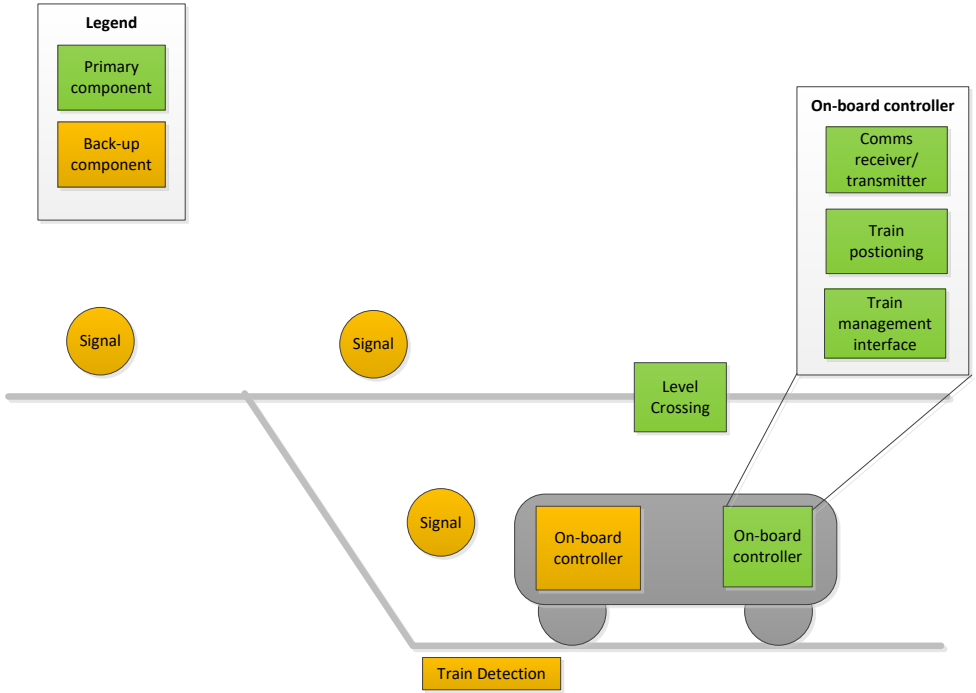


Designing a Resilient System Architecture

Secondary train detection

Redundant on-board systems

- ATO or In-cab signalling



THALES

Designing a Resilient System Architecture

Cloud based TMS

- Hot-standby VMs
- Highly available cloud service provider
- Diverse TMS software

Distributed interlocking

- assets each contain interlocking capability with duplicated functions
- Smart devices capable of taking over adjacent signalling areas

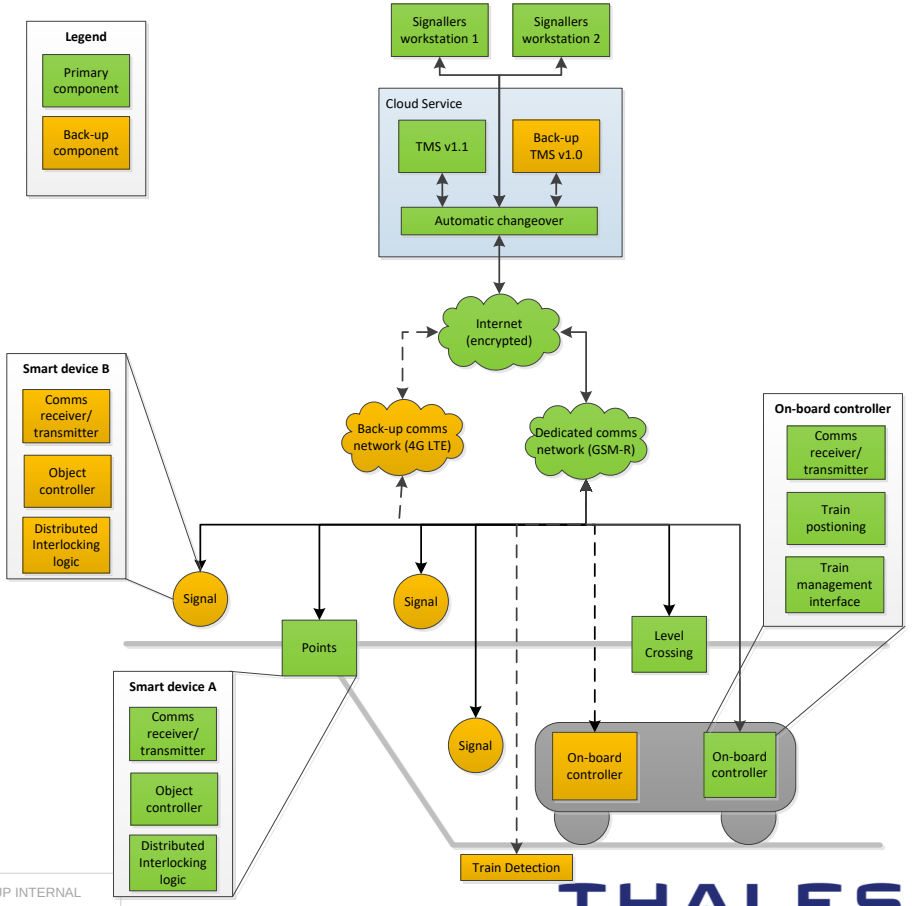
Fall-back communications network

- Dedicated GSM-R and public networks

Secondary train detection

Redundant on-board systems

- ATO or In-cab signalling



Conclusion

- Threats to the railway from sources such as cyber-attacks and extreme weather are increasing.
- More train services are being introduced through modernisation of infrastructure, which reduces the margin to withstand disruption through absorption. Limits are being reached in what can economically be achieved through redundancy.
- Resilience can be enhanced by learning lessons from other industries and embracing new technologies, such as IoT, cloud computing, smart devices, TMS and mobile connectivity.