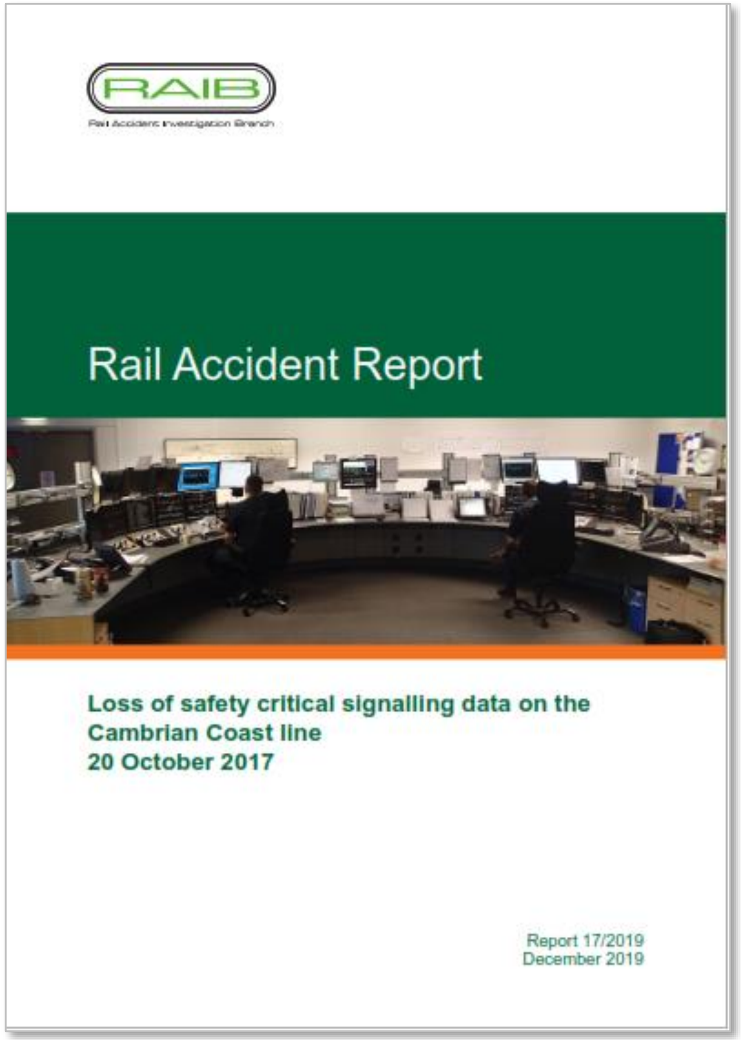
Loss of safety critical signalling data on the Cambrian Coast line



RAIB

Rail Accident Investigation Branch

Rail Accident Report

Loss of safety critical signalling data on the Cambrian Coast line
20 October 2017

Report 17/2019
December 2019

The information to produce these slides has been taken from this RAIB report

- On the morning of 20 October 2017, four trains travelled over the Cambrian Coast line while temporary speed restriction data was not being sent to the trains by the European Rail Traffic Management System (ERTMS) signalling system.

- No accident resulted but a train approached a level crossing at 50 mph, significantly exceeding the temporary speed restriction of 19 mph needed to give adequate warning time for level crossing users.

- The temporary speed restriction data was not uploaded during an automated signalling computer restart the previous evening, but a display screen incorrectly showed the restrictions as being loaded for transmission to trains.

Immediate Cause

The ERTMS signalling system was returned to service following an Radio Block Centre (RBC) software automatic reset, known as a ‘rollover’, without temporary speed restriction information for transmission to trains.

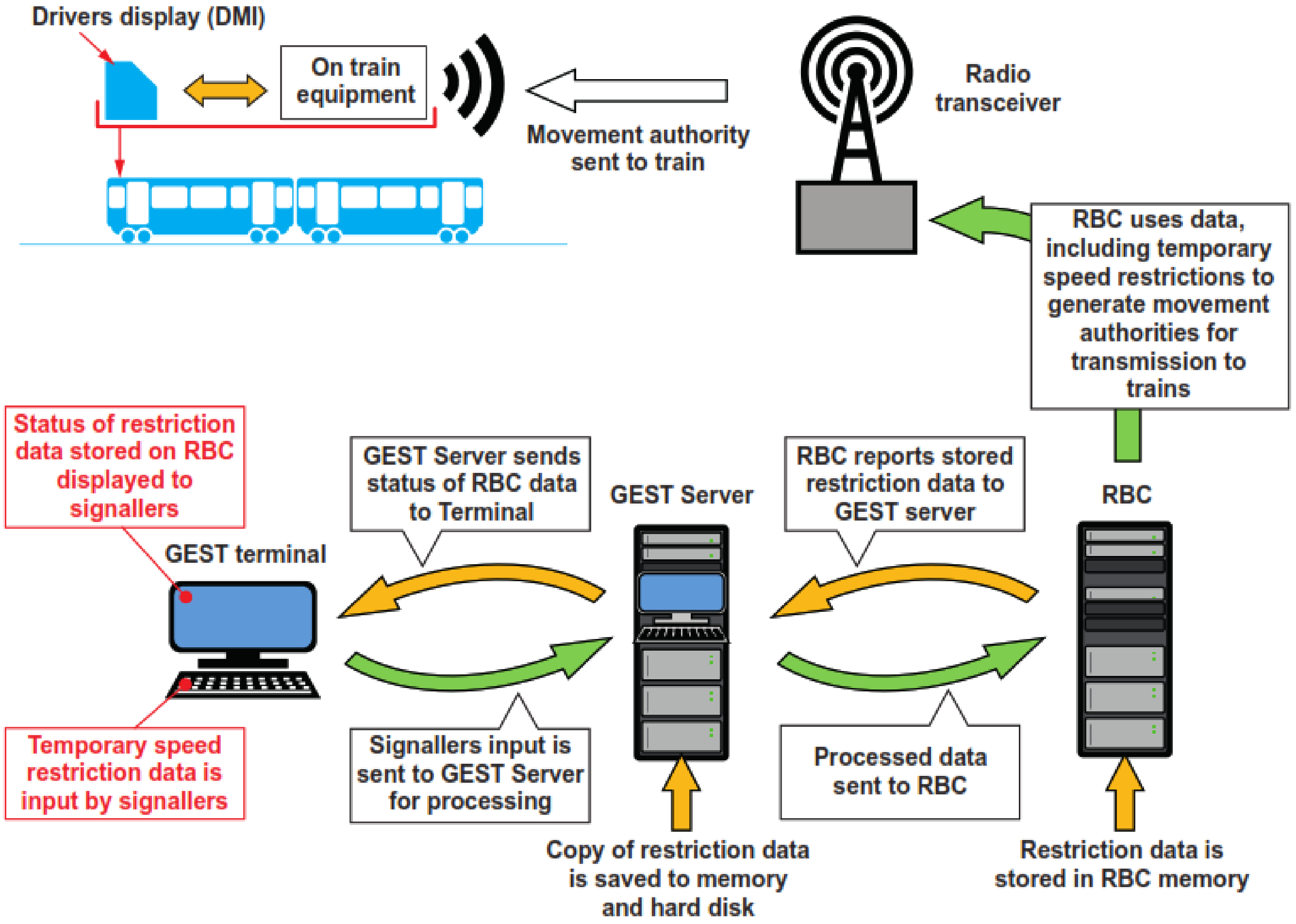

Drivers display (DMI)
On train equipment
Movement authority sent to train
Radio transceiver
RBC uses data, including temporary speed restrictions to generate movement authorities for transmission to trains
Status of restriction data stored on RBC displayed to signallers
GEST Server sends status of RBC data to Terminal
GEST Server
RBC reports stored restriction data to GEST server
RBC
GEST terminal
Temporary speed restriction data is input by signallers
Signallers input is sent to GEST Server for processing
Processed data sent to RBC
Copy of restriction data is saved to memory and hard disk
Restriction data is stored in RBC memory

Figure 6: Simplified arrangement of GEST and signalling control system interface

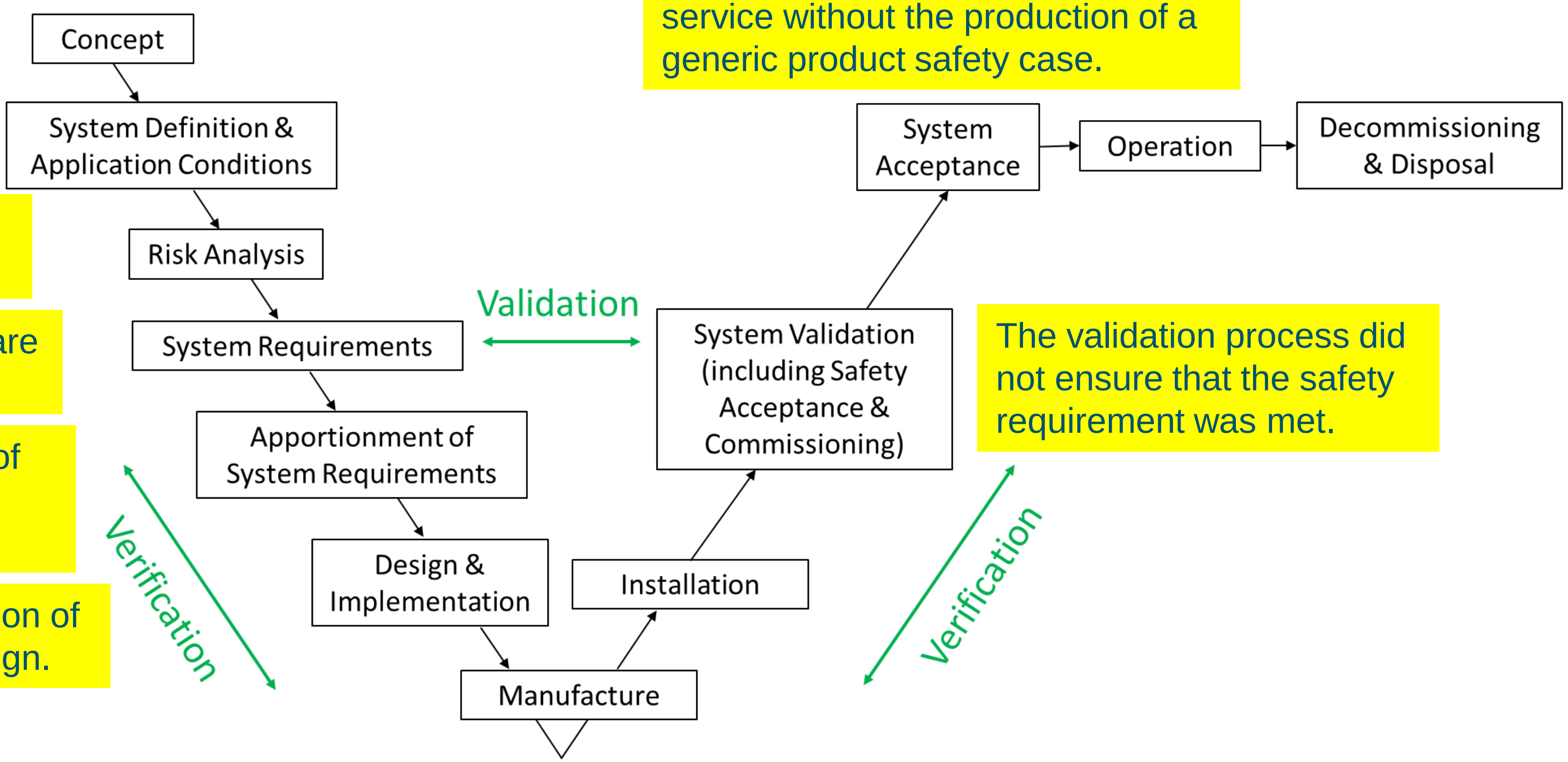
Causal Factors

- Temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition, probably due to a corrupted database.
- No indication that the system had failed was provided to signallers.
- The memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover.
- The required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design.
- GEST server software was unable to detect and manage the corruption of its database.
- The vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project.
- The safety-related software requirements for the GEST software were insufficiently defined.
- The hazard analysis process did not identify, and so did not mitigate against, the GEST software thread failure mode.
- The validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met.
- GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design.

Design Issues

- Key operational data not uploaded to the main system after a software rollover due to a sub-system fault condition.
- No indication provided that the system had failed to the operators.
- Loss of key operational data during system rollover due to use of volatile memory.
- Sub-system software unable to detect and manage the corruption of its own database.

Process Issues



Concept
System Definition & Application Conditions
Risk Analysis
System Requirements
Apportionment of System Requirements
Design & Implementation
Manufacture
Installation
System Validation (including Safety Acceptance & Commissioning)
System Acceptance
Operation
Decommissioning & Disposal
Validation
Verification
Verification

The sub-system was accepted into service without the production of a generic product safety case.

Hazard analysis process did not identify and mitigate against the software thread failure mode.

Insufficient definition of the safety-related software requirements for the sub-system software.

Vulnerability of the system to a single point of failure not detected or corrected during the design, approval and testing phases.

Required level of safety integrity for validation of the data uploaded not achieved by the design.

The validation process did not ensure that the safety requirement was met.