Movares
consultants & engineers

Business Continuity Management in Railway Signalling

Wim Coenraad, 23 oktober 2019, Aspect2019

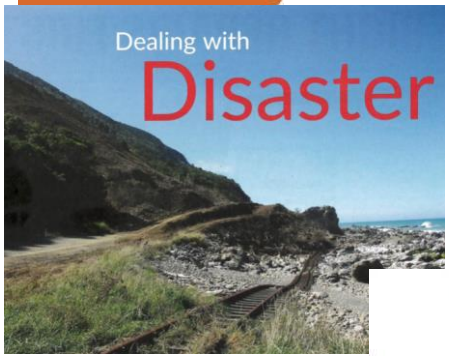
Movares
consultants & engineers

This might *seem* funny

Movares
consultants & engineers

But this is no longer a joke!

Large Scale and Long Disruptions of service



Movares
consultants & engineers

Business Continuity Management in Railway Signalling

the ability to continue operating, perhaps at a reduced performance level, when failures and other events occur, and to recover from such events

By one author with 31+ co-authors:

The IRSE International Technical Committee

Once Upon A Time

- O a hot summer’s day in the mountainous country of Switzerland
- All trains stopped in the evening rush hour

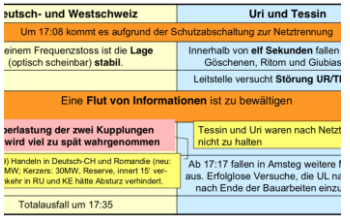
What had happened?
Murphy's law for TPS

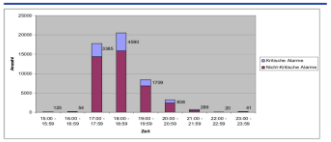
- Three parallel HV 132 kV lines cross the Gotthard, 1 SBB, 2 Joint SBB/CWK/EW
- SBB and 1 joint HV Line out of service to protect piling works
- At 17:08 a *short circui*t is reported in the remaining HV line which shuts it down (later an *over current protection shutdown* is identified as the real cause)
- North and South are now seperated
- The sudden load drop in the south leads to protective generator shutdown in 3 generating facilites
- SBB erroneously suspects failure source to be in the South
- The failure condition prevents bringing the 2 lines back in after building site is cleared and handed back
- 17:17 overload in South leads to shutdown
- No more traction Power in South
- North has 200 MW shortage, backup feeds cannot compensate and North TP collapses at 17:35
- 19:45 partial restoration, 21:30 Traction Power restored
- 200.000 passengers, 1500 trains affected
- 3 Million SFr in compensations
- ?? M SFR Reputation damage
- SBB CEO (who was aboard a stranded TGV 😳) and Infrastructure Director eat copious amounts of humble pie afterwards

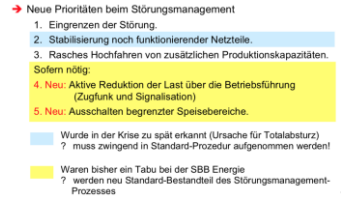
SBB Lessons from that National Traction Power Failure

In a major disruptive event we want to be able to:

1. Stabilise the situation
2. Configure installations for optimal availability and containment of knock-on effects
3. Keep a reduced/skeleton service going
   - Contain the disturbance.
   - Stabilise still functioning systems.
   - Rapid ramp-up of additional production capacity.
4. If necessary:
   - Active reduction of the load via operational management
   - Switch off parts and contain
5. In the crisis, the most important alarms/disturbance messages must be displayed separately.
   - Prevent overwhelming staff in the flood of information
   - Focus on the essentials
   - Keep processes going
6. Analyze risk of unimaginable situations and conceive mitigations





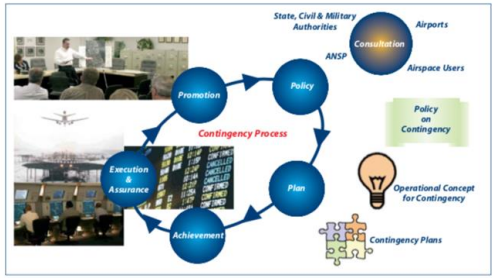


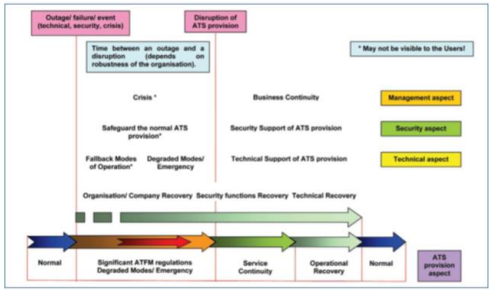
Busines Continuity Management

Normal->Fall-back->Degraded/Emergency->Service Continuity->Recovery

The ability to continue operating, perhaps at a reduced performance level, when failures and other events occur, and to recover from such events

- *Operational Technology (OT)*
- *Information Technology (IT)*
- *Signalling Technlogy*
- *Disaster Recovery*
- *Security*
- *Contingency Planning*



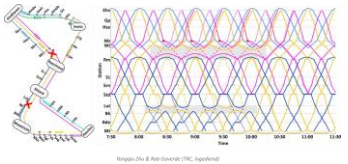


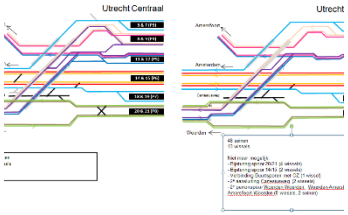
Operational Technology (OT)
Signalling within normal parameters

Design Operations for Robustness

- *Robust timetable design without conflicts*
- *Conflict detection and resolution with dynamic rescheduling*
- *Graceful degradation of service provision*
- *Scenarios for the predictable*
- *Flexibility and Intelligence for the unimaginable*

- *Signalling systems implement and interface to the controls*
- *Design RCS for operational resilience*
- *Crisis and Evacuation Centre*





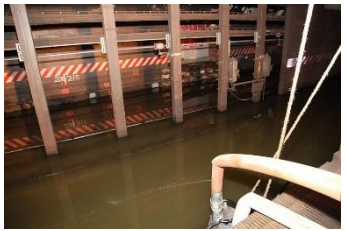
Signalling Technology

Signalling outside normal operating parameters

- Primary Signalling System
  - Fail safe or Fail functional
- Rapid Recovery from Service Affecting Failures
- Redundancy
- Graceful degradation
- Spatial diversity
- Secondary systems
- Communications
- Evacuation of Control centres

Safety and Security
Ambiguous terms

- Ambiguous terms in many languages often used interchangeably
- System Safety
- Social Safety/Security
- Personal and Personell safety
  - Track Worker Safety
- Fire, Storm, Flood…. etc safety
  - MTA Hurricane Sandy and Brisbane 2011, Budapest flooding
  - What would you do if your TC's axle counters and Point Machines had been flooded for days?
  - Where are your Technical rooms and Location cases?
- Vandalism
  - Hardening of assets, No-go areas for maintenace staff during night hours
- Terrorism
- Cyber security
  - CyRail, New Cenelec Standard,
  - Paradigm change for signalling industry and practitioners
  - Heaven for Consultants



Degraded mode operation introduces new hazards!

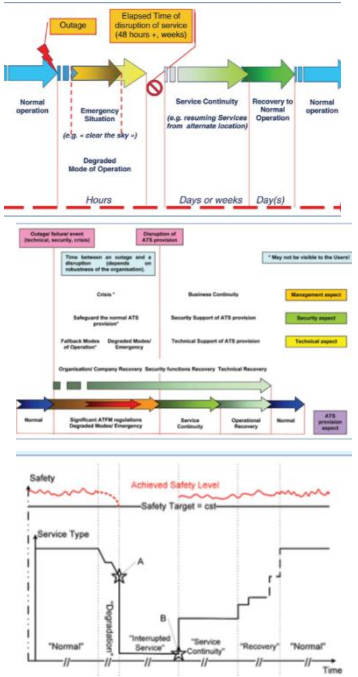
"Problems in training did not create the degraded modes of operation but may have prevented the engineers or drivers from responding to mitigate failures that were associated with these degraded modes"

Degraded modes are not just failure situations, but are "the result of technical systems that fail to meet expected levels of service".

Normal->Fall-back->Degraded/Emergency->Service Continuity->Recovery

New Hazards arise from:

- Pressure for service continuity
- Indequate training – Safety Culture- w.r.t. degraded mode operation
- Human Factors and Operator Performance during Degraded Modes of Operation
- Operational Rules



The IRSE International Technical Committee

The remit of the IRSE ITC (Institution of Railway Signal Engineers – International Technical Committee) is to provide an International and Independent perspective on Railway Control, Command and Signalling (CCS) by a group of widely recognised experts, to both IRSE members and the signalling community worldwide.

The International Technical Committee of the IRSE will promote an international perspective within the Institution by studying and analysing signalling and telecommunications requirements, technology, engineering practice and business methods across different countries. It will make recommendations to advance the knowledge of the profession to the IRSE membership throughout the world.