RAMS application in Railway signaling system

Lei Jiang
Laboratory of Traffic Information Engineering and Control, Southwest Jiaotong University, China
Email: lei.jiang@ntnu.no
L.jiang@swjtu.edu.cn
Ph.D. Candidate--
Traffic Information Engineering & Control, 2014-up to now, Southwest Jiaotong University
Master Degree--
Transportation Engineering, 2012, Southwest Jiaotong University
Bachelor Degree--
Telecommunication Engineering (Railway Signaling Control), 2009, Southwest Jiaotong University Emei Campus
Form 2012 to now, lecturer, Department of Railway Information Engineering, Southwest Jiongtong University. Major Courses Include the Reliability and Safety of Railway Signaling System and Chinese Train Control System (CTCS).
1. Introduction of SWJTU

Southwest Jiaotong University (SWJTU) was founded in 1896 and is one of China’s oldest higher education institutions. Known as the cradle of China’s railway engineers and "the Cornell of the East", SWJTU is the birthplace of China’s modern education in transportation, mining & metallurgy.

More information: http://www.swjtu.edu.cn/SWJTU, Chengdu
• SWJTU has achieved the goal of having national-level platforms for all specialty disciplines of civil engineering, mechanical engineering, electrical engineering, traffic & transportation engineering and surveying & mapping.
1.1 Major faculties

- Faculty of Civil Engineering
- Faculty of Mechanical Engineering
- Faculty of Electrical Engineering
- Faculty of Information Science and Technology
- Faculty of Economics and Management
- Faculty of Foreign Languages
- Faculty of Transportation and Logistics
- Faculty of Materials Science and Engineering
- Faculty of Geosciences and Environmental Engineering
- Faculty of Architecture


## 1.2 Projects related to HSR

<table>
<thead>
<tr>
<th>National 973 Key Project</th>
<th>Fundamentals of broadband wireless communication networks under high mobility scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major Project, Ministry of Education</td>
<td>Research on the key technologies of intelligent railway traffic safety and engineering structure health monitoring</td>
</tr>
<tr>
<td>Major/Key Project, Ministry of Railways</td>
<td>Research on the key technologies of in railway signaling security</td>
</tr>
<tr>
<td>Major Research Project, China Railway Corporation</td>
<td>Research on railway signaling equipment security authentication technologies</td>
</tr>
<tr>
<td>Major Research Project, China Railway Corporation</td>
<td>Research on Maintenance technologies for signal detection—Study of communications monitoring and maintenance technologies</td>
</tr>
<tr>
<td>Major Research Project, China Railway Corporation</td>
<td>Research on Maintenance technologies for signal detection—Study of signaling monitoring and maintenance technologies</td>
</tr>
</tbody>
</table>
1.3 Research on Traffic Information Engineering and Control

- High-speed railway signaling technology
- Railway signaling network security
- Intelligent operational condition monitoring
- CTCS-2/3 simulation, design and verification
- CBTC-based signaling system, ATO, ATS, etc.,
- Automation of railway marshalling
- RAMS application in railway signaling

Diagram:
- TCC
- CBI
- CTC (Station)
- CSM
- RBC
- CBI Secure communication LAN
- CBI Secure communication WAN
- CTC Secure communication LAN
- CTC Secure communication WAN
- GMS-R
- Protocol adapter
- Key management center
- Maintenance center
- TSRS
- Local terminal of RBC
- CTC LAN (Station)
- Monitoring LAN (Station)
Health Monitoring and Detection for High-speed Railway Turnouts

Functions:

On-line monitoring the temperature, current, voltage of point machine

On-line monitoring the transforming force, close of turnout

On-line monitoring and detecting the flaw at the bottom of turnout
Integrated Railway Signaling and Communication Monitoring System
Key Laboratory of Traffic Information Engineering and Control

Dispatching simulation system

Signaling control testing and verification system

SWJTU ATS system

DCS monitoring system
Key Laboratory of Urban Rail Operation & Control

Simulation platform

Metro vehicle model

High speed railway dispatch center and Metro Operation control center
2. Introduction of CTCS

- Two direction of railway development
  - Heavy haul railway for Freight Transportation
  - High speed railway for Passenger Transportation
CTCS: Chinese Train Control System
The Control principle of CTCS-2

**Track circuit Function:**
- Train occupancy and location
- Moving authority

**Balise Function:**
- Temporary limited speed
- Line profile

**Onboard system Function:**
- Supervises the movement of the train to which it belongs, on basis of information exchanged with the trackside sub-system

2FSK signal
The Control principle of CTCS-3

- **Interlocking**
- **Radio Block Center RBC**
- **Centralized Traffic Control System (CTC)**

**Track circuit**

**Route information**

**Limited speed**

**Train location and speed**

**Moving authority**
3. RAMS application of CTCS

- EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);
- EN 50128: Railway Applications - Software for Railway Control and Protection Systems;
- EN 50129: Railway Applications - Communications, signaling and processing systems – Safety related electronic systems for signaling.
The characteristic of Railway signaling system

**Complex:** hardware/software/human error/working environment

**Large scale:** the number of interacting components and subsystem has increased drastically.

**Phased mission system:** accelerate, decelerate and constant

**Cyber-physical system:** computer-based system
RAM in railway signaling system

FMEA and FTA for the reliability assessment of ZPW-2000 track circuit.
RBD and Markov Chain Model
Bayesian Network
Dynamic Fault Tree
combining DS evidence and BN
data-driven model for maintenance
Resilience Quantitative Evaluation
dependability analysis
safety and availability analysis
Availability assessment using Statecharts
Onboard subsystem failure

- C3-VC failure
- C2-VC failure
- BTM failure
- BSA permanent error
- Invalid BTM port
- BTM hardware failure
- DMI failure
- TIU failure
- Interface relay failure
- VDX failure
- SDU failure
- Speed sensor failure
- Distance sensor failure
- SDP software failure
- Driver failure
- Driver subjective error
- Driver objective error

Train working environment

Wireless communication timeout
Safety in Railway signaling system

HAZOP Study on the CTCS-3 Onboard System
Formal method for computer-based interlocking software
Multiformalism Modeling
Model-driven V&V assessment of railway control systems
A Markovian–Bayesian Network for Risk Analysis of High Speed and Conventional Railway Lines Integrating Human Errors
Bayesian Networks-Based Probabilistic Safety Analysis for Railway Lines Using catastrophe theory to describe railway system safety
Cyber Security Analysis of the European Train Control System
Vulnerabilities analysis for cyber physical system (balise-based train control)
4. High-speed train collision analysis

• Although HSRs have had only four fatal accidents in their 50-year history, three of them occurred over the past six years as HSR systems in operation have grown.

• Two types of train accident
  train collision and derailment
110km/h over limited speed in Spain in 2013
80km/h over limited speed in France in 2015
In 2011, a collision of two high speed trains occurred in Wenzhou, China, killing 40 passengers (Wenzhou train collision). A flaw in the signaling systems and several managerial problems were behind the tragedy.
## Analysis of Yong-Wen train collision

<table>
<thead>
<tr>
<th>Time</th>
<th>Station operator</th>
<th>Dispatcher in CTC</th>
<th>The front train D3115</th>
<th>The following train D301</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ordered D3115 to transferred to On Sight mode (V&lt;20km/h) if there is a red light in the interval</td>
<td>Reached 5829AG and stopped automatically for the TC Failure. Failed to transfer to On Sight mode</td>
<td></td>
</tr>
<tr>
<td>20:17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:21</td>
<td>Failed to call D3115</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:22</td>
<td>Failed to call D3115</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:24</td>
<td>Ordered D301 to leave</td>
<td></td>
<td></td>
<td>Left Yongjia Station</td>
</tr>
<tr>
<td>20:28</td>
<td>Failed to call dispatcher and station operator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:29</td>
<td>Transferred to on-sight mode successfully and restart</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:30</td>
<td></td>
<td></td>
<td>D301 (90km/h) crashed into D3115 (16km/h)</td>
<td></td>
</tr>
</tbody>
</table>
CTC Dispatching Center
Route information
Wrong track occupancy status

CTC Station Workstation
Route information
Wrong track occupancy status

TCC
Safety Requirements and Constraints Violated:
- Provide safe train movement limit.
- Prevent train to train collision.
- Fail safe software design principle.
- Fail safe hardware design principle.
- Failure management in software to protect against hazardous situations.

Failures and Inadequate Controls:
- Equipment failure caused the system to use outdated track occupancy status.
  - Communication channel with wayside broken due to lightning.
  - PIO board power circuit broken due to lightning.
- PIO provides the previous non-occupancy status to the system.
- The control system output control information based on the old information PIO provided.
- Inadequate failure management process in TCC:
  - TCC only transferred component failure information to its monitoring system, no further preventive actions taken.

Physical Contextual Factors:
- Abnormally strong lightening activities along the rail lines from Wenzhou South to YongJia station about 1 hour before the accident.
- The passenger train operation interval is designed to be 4 minutes.

Wrong control message
Track occupancy

Track Circuits
- Track Circuit 5829AG failed due to lightening

D3115 Onboard ATP
Wrong codes

D301 Onboard ATP
Wrong codes

CTC Dispatcher
Safety Related Responsibilities Violated:
- Must track the route status in failure situations.
- Must track the train status in failure situations.
- Must take preventive actions in case of unknown situation.

Context:
- Work on a 12 hour shift.
- Schedule, performance and image pressure.
- Received and dispatched 8 other trains within 7 minutes after dispatching D3115 and before D301.
- D3115 was 4 min behind schedule.
- D301 was 36 min behind schedule.

Inadequate Decisions and Control Actions:
- Did not track TC 5829AG failure status.
- Did not track where the leading train D3115 is after dispatching it.
- Dispatch D301 to run normally into the blocks with failed equipment and failed train.
- Did not warn D301 train operator of the failure situation ahead.

Mental Model Flaws:
- Incorrect model of track occupancy status.
- Incorrect model of D3115 location.
- Incorrect model of the station and wayside failure.
- Believed the system is itself fail-safe.

D3115 Train Operator
Report of D3115 failed to start in OS mode 2 minutes before accident.

D301 Train Operator
No warning provided until 33 seconds before the crash.

Command to switch to abnormal station control mode
Station Operator

Command to switch to CTC about D3115 status

Failure to report to CTC about D3115 status

Command to switch in TC normally
Future research

- utilizing the field data to reliability analysis
- Bayesian Networks-Based Probabilistic Safety Analysis in railway signaling system
Reference:

Thank you!