# 2005 Asia-Pacific Conference on Risk Management and Safety

## Safety Assurance for Chinese Railway – Interfacing with International Practice and Standards


Simon Zhang

北京交通大学与阿特金斯联合

轨道交通安全研究中心

Atkins & Beijing Jiaotong University Joint

**Safety Research & Certification Centre**

# Introduction

- Railway Safety Assurance
- International Standards & Practice
- Chinese Practice

# Railway Safety Assurance

- Train control system is safety-critical system
- Problem:
  - Introduction of electronic & computer in train control
  - Impact of privatisation

# Past vs. present - technology

- Past:
  - Mechanical and relay based interlocking are inherently fail-safe
- Present:
  - Electronic components, PLC, computers are not inherent fail-safe
  - Software could introduce systematic error to the system

# Past vs. present - organisation

- Past:
  - State run railway
- Present:
  - Railway privatised
  - Both the railway and suppliers are in an open market
  - Operators, suppliers have to satisfy share holder

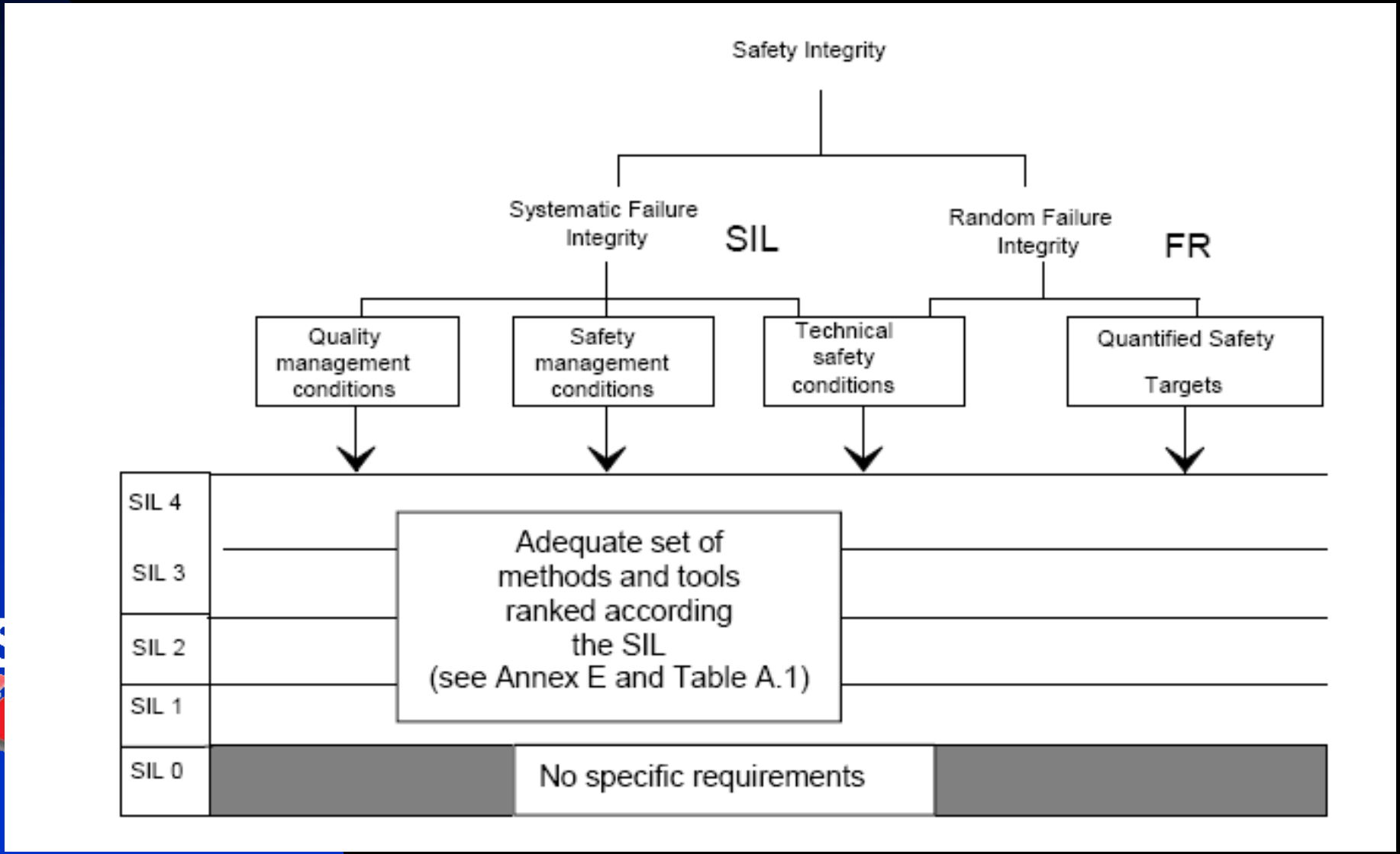
# International Standards & Practice

- Generic Safety-related system: IEC61508
- Military Standards:
  - MIL-STD-882C
  - Def Stan 00-55, Def Stan 00-56
- US
- Japan
- UK: Yellow Book
- CENELEC: EN50129 suites

# Current European Standards & Practice

- EN50126 – RAMS
- EN50128 – Software
- EN50129 – Safety
  - SIL
  - Safety Case Regime
  - Safety Acceptance

# SIL


Safety Integrity
Systematic Failure Integrity
SIL
Random Failure Integrity
FR
Quality management conditions
Safety management conditions
Technical safety conditions
Quantified Safety Targets
SIL 4
SIL 3
SIL 2
SIL 1
SIL 0
Adequate set of methods and tools ranked according the SIL (see Annex E and Table A.1)
No specific requirements

# Safety Case and Safety Acceptance

- Safety Case:
  - Quality Management
  - Safety Management
  - Functional & technical safety
- Safety Approval by Safety Authority
  - Independent Safety Assessment
  - Safety approval
  - Safety acceptance & Cross-acceptance

# Chinese Railway - Marketisation:

- Railway is one of the last few monopolies left in China
- Marketisation trial has been going on for some time
- Railway suppliers, institutes, universities etc have been gradually made independent from MOR in the past few years
- Recent changes: sub-administration layers has been chopped off in March
- BBC reports MOR to sell off part of its network last month
- MOR is slim down, changing its role from “everything to do with railway” to modern regulator/supervisory type government agency

# Chinese Railway – Interfacing with International market

- Railway need investment to build new lines and upgrade existing ones, state investment is far from enough
- Foreign/private investors (like MTR) are interested, recent law/regulation changes have made this legally possible
- Chinese railway need to buy from international market at present
- Chinese suppliers need to sell into international market in future – as every industry else in China

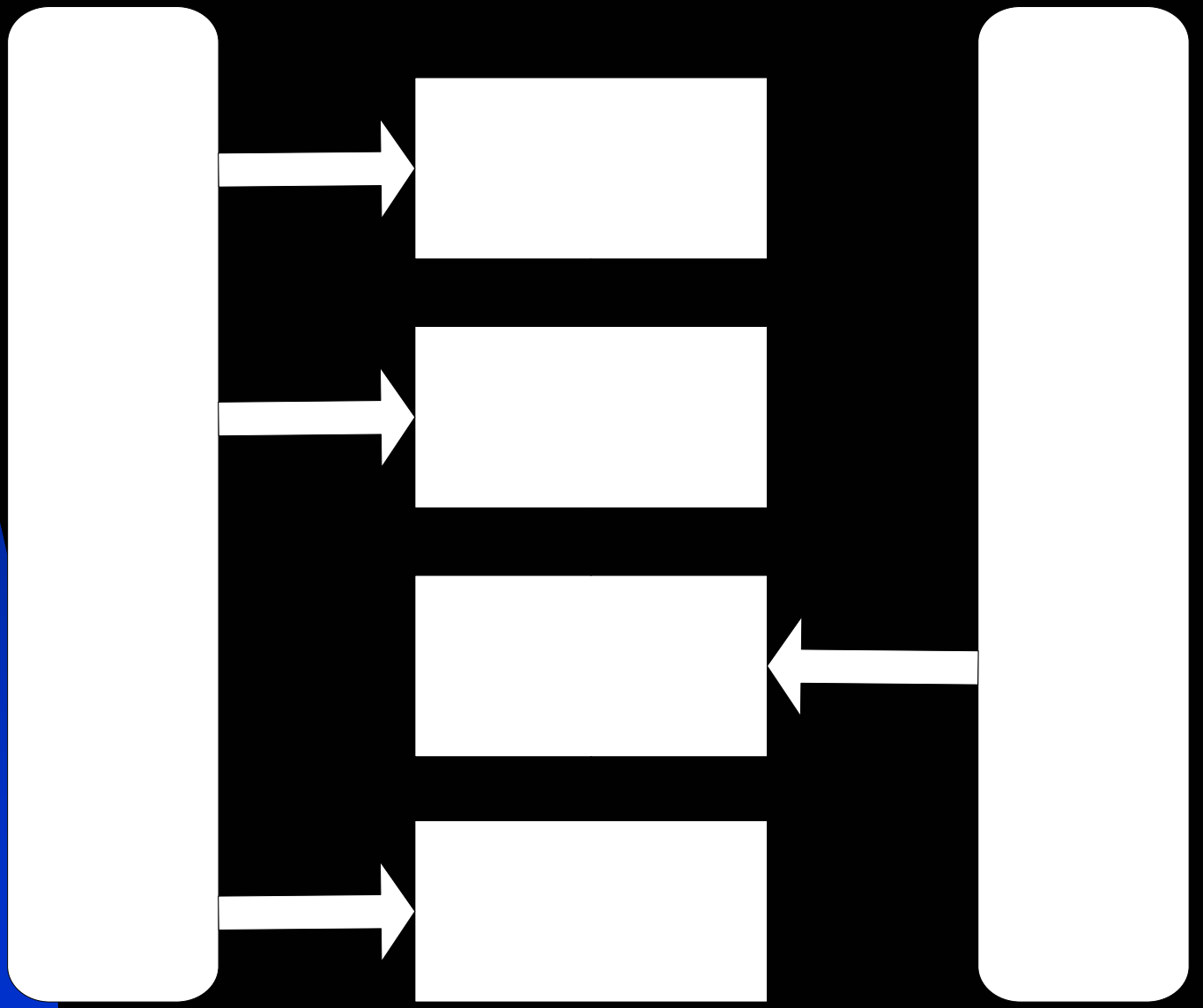
# What the industry is doing now to prepare themselves

- Now:
  - Writing a lot of new standards
  - Eager to exchange with them international colleagues
- Next:
  - ?
- EN50129s equivalent standard - GB10495

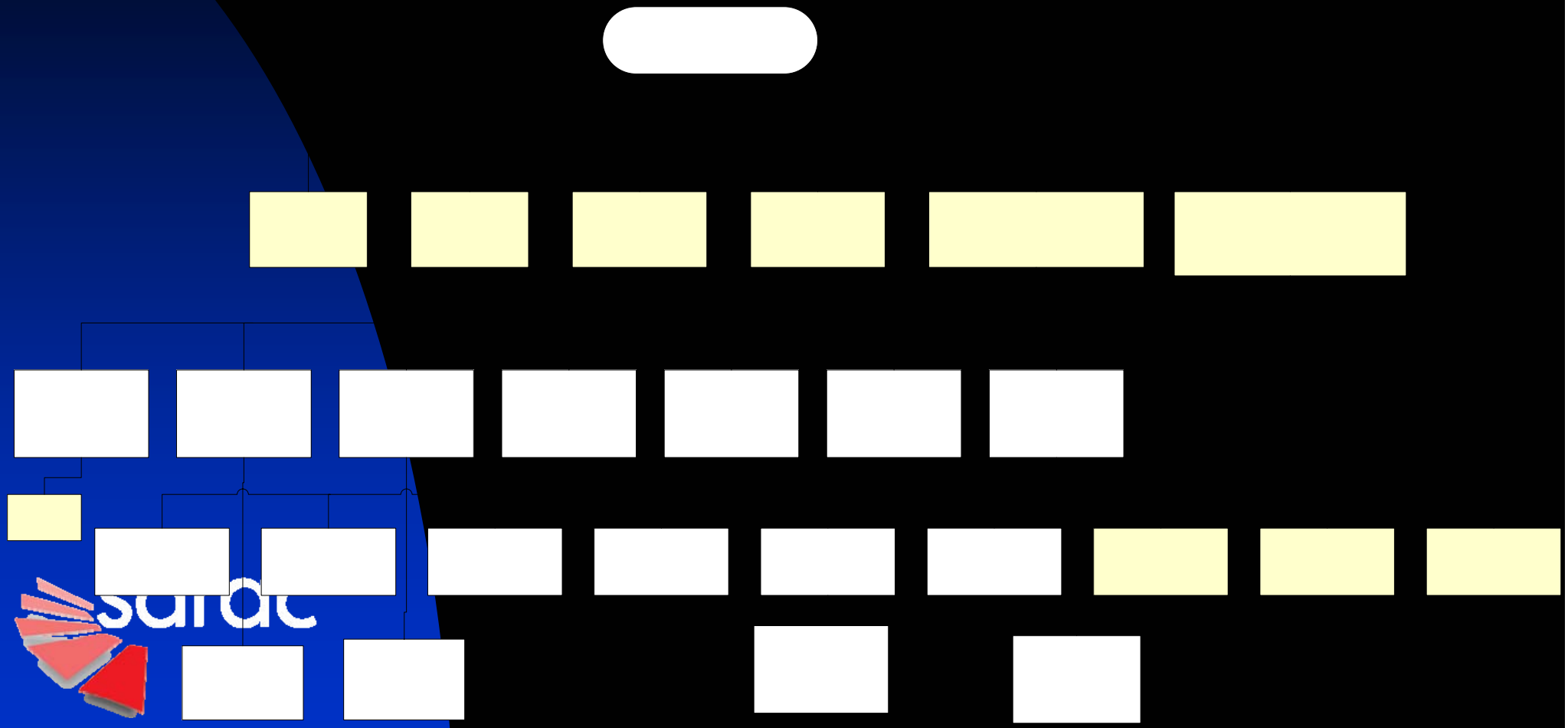
# GB10495

- First appeared the 80's, Chinese equivalent of UIC7381-1980
- MOR commissioned CARS to rewrite GB10495 in 2003
- Coordinated by CARS, industry participants incl.: universities, design institutes, supplies etc
- Lots of traces and ingredients of EN
- In September's review meeting, two foreign companies are invited: Atkins and Siemens – signalling MOR's willingness to take international players opinion

# GB10495 comparison with EN50129



# GB10495 Structure



# GB10495 Suggestions

| *Item* | *Section* | *Comment* |
|---|---|---|
| 1 | 3.1 | This definition is too generic and unhelpful |
| 2 | 3.11 | Incorrect definition |
| 3 | 3.15 | Improper definition |
| 4 | 4.11 | Mixing deliberate and unintended random errors together is inappropriate |
| 5 | Table 5 | $P_f$ is not failure rate |
| 6 | 5.1.1.2 | The methods mentioned are incomplete and inadequate for linking hazards to consequences |
| 7 | 5.3.2.1 | The concept of competence does not apply to software products. Compliance with QMS is not adequate for safe software either |
| 8 | 5.4.2.2 | FMEA is not a method for quantitative analysis |
| 9 | 5.6.1 | Redundancy and fail-safety are not the same concepts |
| 10 | 6.3.2 | Software validation is not about quality system |
| 11 | 6.3.2 | There's no mention of technology requirements as the title implies. The role of Independent Safety Assessor is not clearly stated |
| 12 | 6.5 | This section does not cover safety verification of a transport system as the title implies |
| 13 | 6.6 | The alphabetical list of verification and validation activities is incomplete. Validation is not the same as having a quality system either |
| 14 | 6.7.5 | A test is a useful method to assist but is not entirely an adequate proof of safety assessment in a complex product |

# Way Forward for Chinese Railway Safety Assurance

- Safety assurance framework & Practice:
  - Adopt European style one?
  - Opportunities for us?
- Sample projects:
  - MTR SkyPlaza Project
  - CRSCD (China National Railway Signal & Comm. Corp.) interlocking system certification

# MTR SkyPlaza Project

- Typical example for a Chinese supplier interfacing international market
  - MicroUnion and DaCheng to supply signalling system for MTR
  - Atkins Beijing commissioned by MTR to Independent Check supplier's design – this is just part of design process familiar to European players, nowhere near ISA!
  - And what we found out? …!!!

# CRSCD Initiatives

- One of the few MOR authorised computer interlocking suppliers in China
- CRSCD has realised the advantages of product compliance with European Standards
- Working towards certification of its product

# Thank You

Simon.zhang@atkinsglobal.com

www.sarac.org.cn

www.atkinsglobal.com