PSAM 9

Case Study in the Assignment of Safety Integrity Requirements for Driverless Metro System in Singapore

Singapore Land Transport Authority (LTA)

Chin Nang Tang

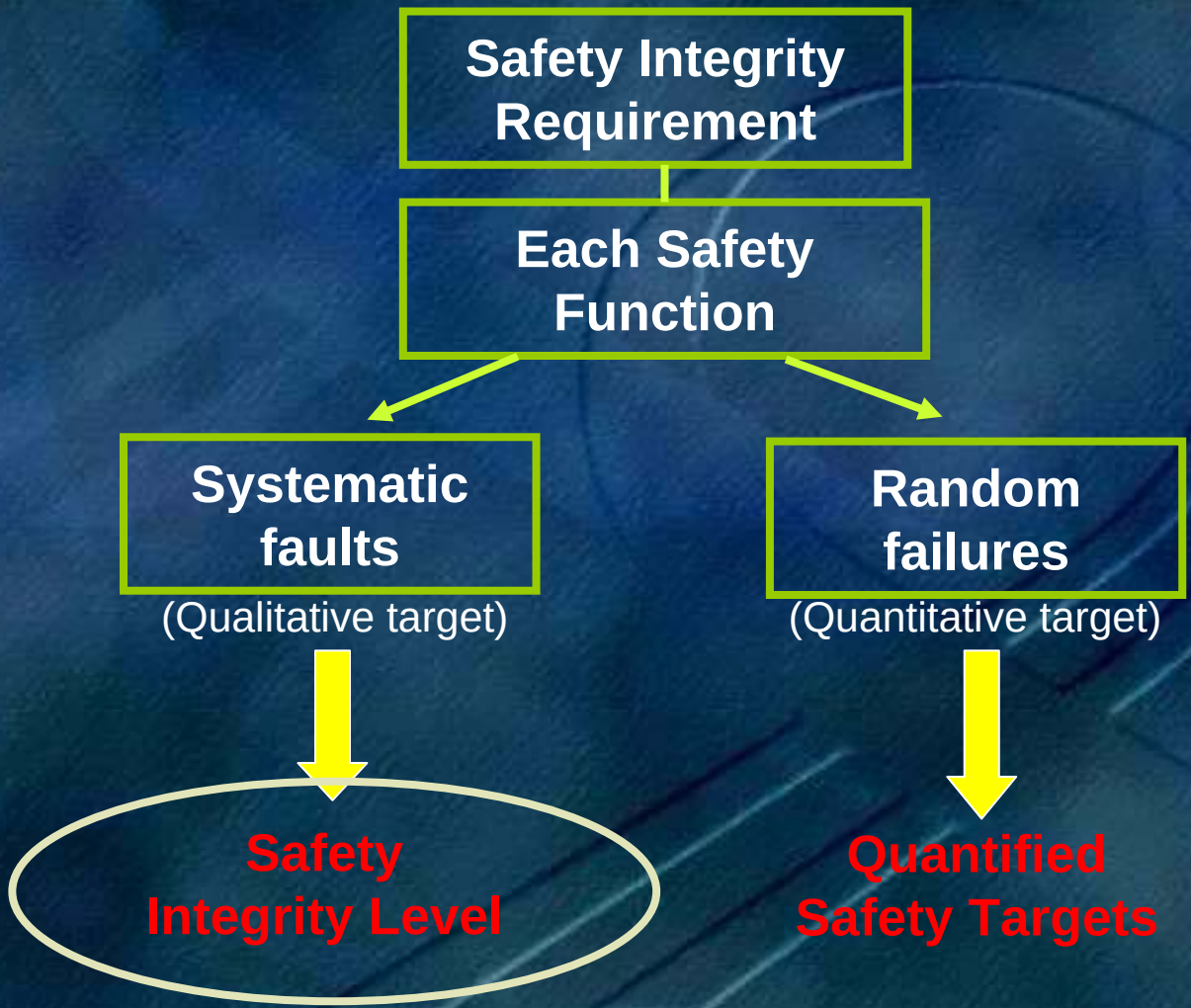
Content of Presentation

- About This Assessment
- Definitions of Safety Integrity Requirements
- Process of Assignment
- Demonstration of Safety Integrity Requirements

About this Assessment

- Develop High Level SIL targets for similar application in Singapore RTS
- Provide justifications for the development of Lower Level SIL targets
- Define Criteria for Demonstration
- Establish a reference for Driverless Railway System

Definitions of Safety Integrity Requirements

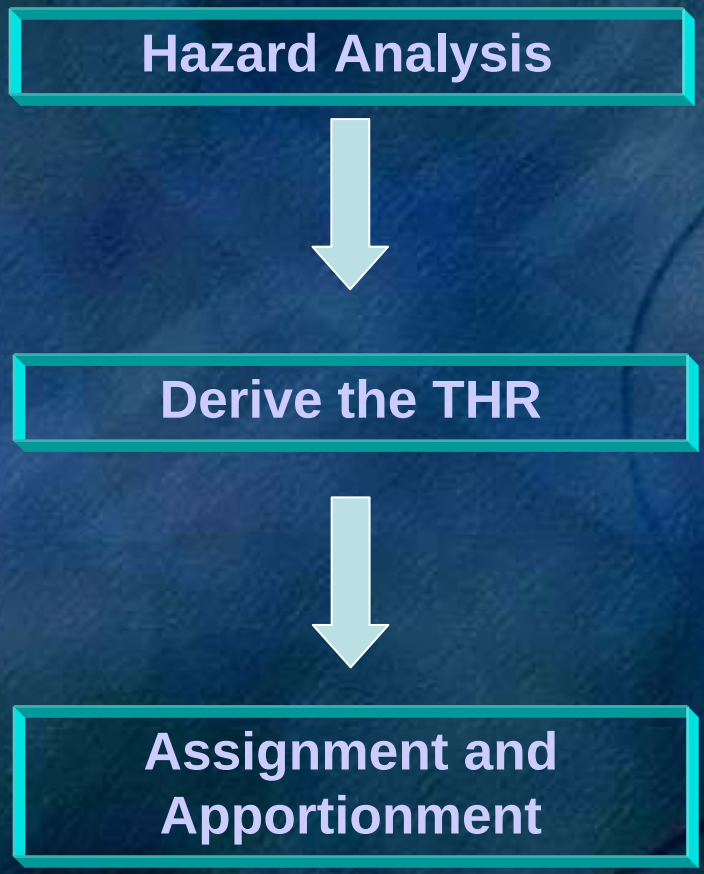


Definitions of Safety Integrity Requirements

EN50129:2003 (Table A.1-SIL Table)

Tolerable Hazard Rate (THR) per hour and per function	Safety Integrity Level
$10^{-9} \leqslant THR < 10^{-8}$	4
$10^{-8} \leqslant THR < 10^{-7}$	3
$10^{-7} \leqslant THR < 10^{-6}$	2
$10^{-6} \leqslant THR < 10^{-5}$	1

Process of SIL Assignment



- Hazard Identification
- Mitigation Measures analysis
- Identification of Safety related Functions

- Define Tolerable Risk Level
- Define Tolerable Accident Rate
- Define Tolerable Hazard Rate
- Define their Relationships with SIL

- Assign to High Level Safety Function
- Functional Breakdown
- Assign to Subsystem Safety Functions

Process of SIL Assignment

Hazard Analysis

Hazard	Potential Accident	Safety Requirement	Safety Function	Accident Severity
Train departure with opening door	Fall of passenger from train to track	The train and platform screen doors closing process should be provided in safety	Provide safe train door opening/closing operation by interlocking with train propulsion system; Signalling system ensure train starting off moving when both PSD and train doors are closed	Fatalities and/or multiple severe injuries (I)

Process of SIL Assignment

Define Tolerable Hazard Rate

- Tolerable Risk Level
- Tolerable Accident Rate (TAR)
- Tolerable Hazard Rate (THR)

Process of SIL Assignment

Define Tolerable Hazard Rate

(LTA Risk Matrix)

Risk Category			Accident Severity Category			
			I	II	III	IV
			Catastrophic	Critical	Marginal	Insignificant
Accident Frequency Category	Frequent	⩾1acc per 100 hrs	Intolerable	Intolerable	Intolerable	Undesirable
	Probably	$1x10^2$ hrs < 1acc ⩽ $1x10^4$ hrs	Intolerable	Intolerable	Undesirable	Tolerable
	Occasional	$1x10^4$ hrs < 1acc ⩽ $1x10^5$ hrs	Intolerable	Undesirable	Undesirable	Tolerable
	Remote	$1x10^5$ hrs < 1acc ⩽ $1x10^6$ hrs	Undesirable	Undesirable	Tolerable	Negligible
	Improbable	$1x10^6$ hrs < 1acc ⩽ $1x10^8$ hrs	Tolerable	Tolerable	Negligible	Negligible
	Incredible	$1x10^8$ hrs < 1acc ⩽ $1x10^{10}$ hrs	Negligible	Negligible	Negligible	Negligible

Process of SIL Assignment

Define Tolerable Hazard Rate

Tolerable Accident Rate =

Tolerability Hazard Rate (THR) x Probability of Accident Occurrence (P)

Probability of Accident Occurrence (P) is determined by:

- Probability of Hazard Occurrence leading to the Accident

Process of SIL Assignment

THR Table		Probability of Accident Occurrence								
Sev	TAR	1	0.5	0.1	0.05	0.01	0.005	0.001	0.0005	0.0001
I	1.00E-10	1.0E-10	2.0E-10	1.0E-09	2.0E-09	1.0E-08	2.0E-08	1.0E-07	2.0E-07	1.0E-06
II	1.00E-08	1.0E-08	2.0E-08	1.0E-07	2.0E-07	1.0E-06	2.0E-06	1.0E-05	2.0E-05	1.0E-04
III	1.00E-06	1.0E-06	2.0E-06	1.0E-05	2.0E-05	1.0E-04	2.0E-04	1.0E-03	2.0E-03	1.0E-02
IV	1.00E-04	1.0E-04	2.0E-04	1.0E-03	2.0E-03	1.0E-02	2.0E-02	1.0E-01	2.0E-01	1.0E+00
SIL Table		Probability of Accident Occurrence								
Sev	TAR	1	0.5	0.1	0.05	0.01	0.005	0.001	0.0005	0.0001
I	1.00E-10	4	4	4	4	3	3	2	2	1
II	1.00E-08	3	3	2	2	1	1	0	0	0
III	1.00E-06	1	1	0	0	0	0	0	0	0
IV	1.00E-04	0	0	0	0	0	0	0	0	0

Process of SIL Assignment

Assignment and Apportionment

- The train and platform screen doors closing process should be provided in safety

  - Accident Severity I
  - Tolerable Accident Rate 1E-10
  - Probability of Occurrence 0.1
  - Tolerable Hazard Rate 1E-9
  - SIL Target 4

Process of SIL Assignment

Assignment and Apportionment

- when Lower Level Safety Functions are independent
- when they are redundant each other

then
Additional Apportionment Factor 0.01
will be assigned to “P”

Accident Frequency Category	Frequent	$\geqslant$1acc per 100 hrs
	Probably	$1x10^2$ hrs < 1acc $\leqslant$ $1x10^4$ hrs
	Occasional	$1x10^4$ hrs < 1acc $\leqslant$ $1x10^5$ hrs
	Remote	$1x10^5$ hrs < 1acc $\leqslant$ $1x10^6$ hrs
	Improbable	$1x10^6$ hrs < 1acc $\leqslant$ $1x10^8$ hrs
	Incredible	$1x10^8$ hrs < 1acc $\leqslant$ $1x10^{10}$ hrs

Process of SIL Assignment

Assignment and Apportionment

Safety Requirement	THR	SIL	Safety Function	P	THR	SIL
The train and platform screen doors closing process should be provided in safety	1E-9	4	Provide safe train door opening/closing operation by interlocking with train propulsion system	0.01	1E-7	2
			Signalling system ensure train starting off moving when both PSD and train doors are closed		1E-7	2

Process of SIL Assignment

Assignment and Apportionment

Demonstration of Safety Integrity Requirements

Safety Integrity Requirement for Safety Function

Systematic Faults

- Quality Management requirements
- Safety Management requirements –compliance with Codes, Industrial Practices, Statutory Regulations, etc.

Random Failures

Quantitative Target is met

Thank You