A Systems Assurance Perspective Towards Generic Systems Engineering

By Joyce Hong
Systems Assurance & Integration Division
Land Transport Authority, Singapore

Land Transport Authority

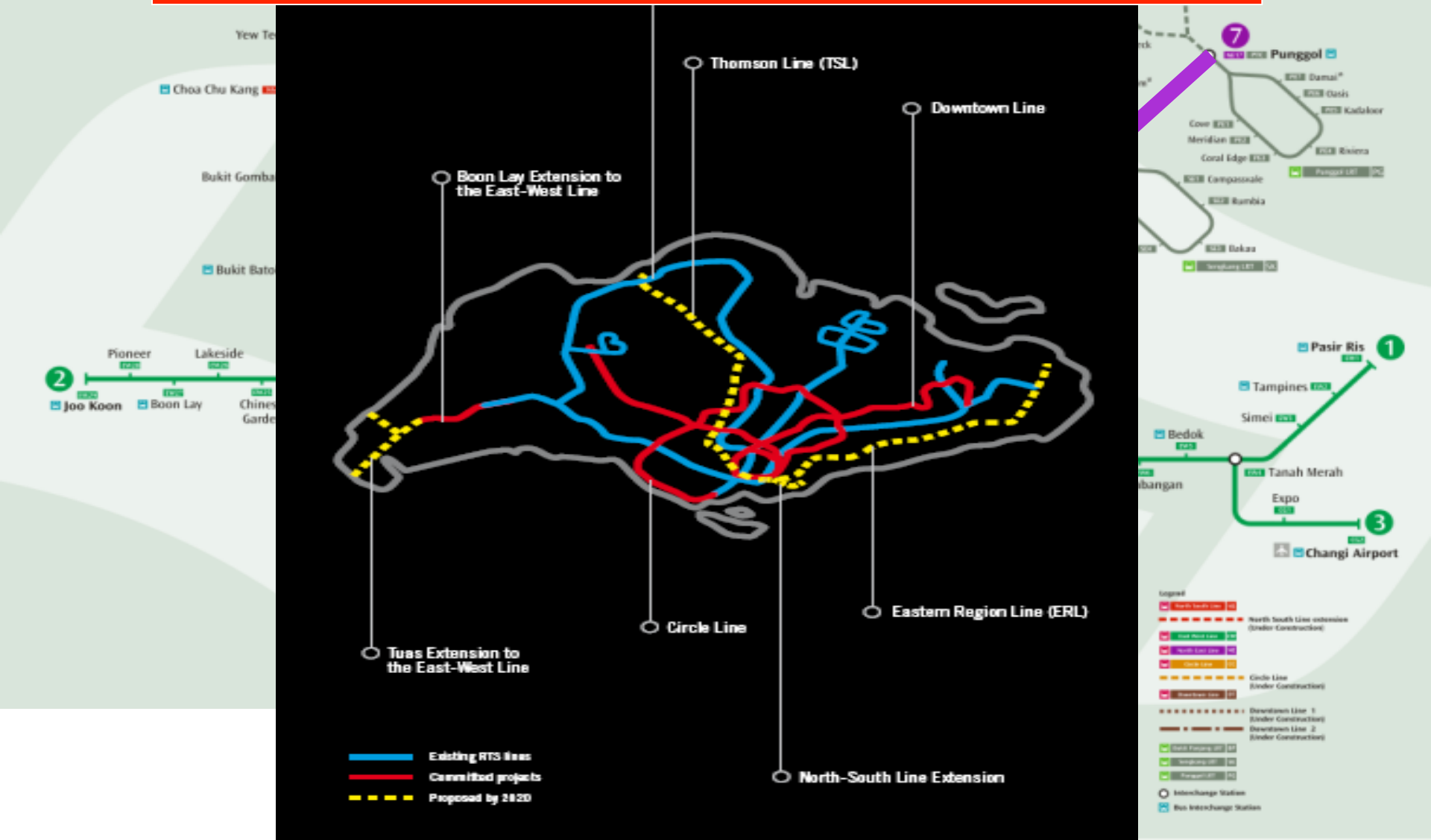
Topics

- Chronicle of RTS Experience
- Previous Problems and Constraints
- New Concept for Future RTS Projects
- Project Safety Review (PSR) Process
- Generic Systems Engineering Process
- Building the Generic Requirements Model
- Requirements-based Hazard Management
- Requirements Management
- Continuous Process Refinement
- Challenges and Uncertainties
- Expected Benefits

Land Transport Authority

Chronicle of RTS Experience

The complete rail network as of 2020



Previous Problems and Constraints

- Lack of a clear system-of-systems (SoS) design concept prior to contract award
- Lack of a consistent systems engineering (S.E.) process to support & guide all systems design and risk management activities
- Shorter Project Life Cycle constraints and higher public expectations for new Rail Transit Systems (RTS) rollout
- Lack of in-house expertise from a pool of new engineers

Previous Problems and Constraints

Example: Hazard Management

- Circle Line design and build in 5 Stages
- Different Contractors are appointed for the Building Services Contacts comprising Environmental Control System/ Tunnel Ventilation System (ECS/TVS), Electrical Services (ELE) and Fire Protection System (FPS)
- Each Contractor identifies similar design, interface and operational hazards repeatedly with different hazard descriptions
- A review needs to be conducted to ensure consistency in hazards and the approach to risk reduction

Previous Problems and Constraints

System	Hazard	Hazard Cause	Trigger	Accident	Confirmed Risk Reduction Contractor A	Confirmed Risk Reduction Contractor B	Confirmed Risk Reduction Contractor C	Confirmed Risk Reduction Contractor D
TVS	Loss of Tunnel Ventilation	Fan / fan damper fails	Train air condition cut off	Possible passenger discomfort	Fan damper failsafe position is open.	(1) MCC dual fed (2) Fail safe - Bypass damper default position is closed to support emergency ventilation mode (3) 1 fan out of 8 is allowed to fail in emergency mode (4) Flow switch provided to prove fans are operating (5) At the last resort, ventilation could be provided from adjacent stations.	(1) Jet fans are provided in pairs, in case whereby one fan fails, some air flow will be provided to the tunnel (with the operation of the TVF) for ventilation. (2) Regular maintenance or testing on fan operation.	Piston effect will be able to ventilate the tunnel during normal operation. 2 nos. UPEF are designed to serve both trackways. The UPEF shall operate during the entire revenue hour except under emergency / fire condition.
ECS	Loss of chilling effect	Chiller or associated equipment failure	Equipment aging	Loss of air condition in public / non-public areas and equipment rooms. Railway system equipment failure and disruption to railway operations.	(1) Redundant cooling tower, chiller, etc. are provided. (2) Split A/C unit is provided for essential rooms.	Confirmed Fault tolerance and/or graceful degradation (2 out of 3 for all critical rooms (ECS plant)) (ECS/5605 - Water schematic)	Major ECS equipment shall be provided with redundancy.	(1) Full redundancy is provided for all ECS equipment including the control. (2) Regular maintenance shall be conducted by competent staff.
Hosereel Water Tank	Inadequate / no water supply to fire protection system	No mains water available, Make up water valve fails closed, Storage tank emptied for maintenance, Drain valve fails open, Float valve fails to open, Firewater tank leakage/failure, Water tank leaking, Hosereel valve fails to operate	Maintenance / inspection procedures fail to identify fault system., Emergency or fire mode	Escalation of fire, station evacuation; asphyxiation; severe injuries, potential for fatalities.	(1) Low water level warning alarm signal is monitored by MAP which updates PSC and OCC. Refer to: Layout for sprinkler water tank and pump room.	(1) Storage tanks designed to local standards (FSRTS, SS CP52); provision of 2 separate compartments with concrete partition within storage tanks; provision of water level sensors (high/low level). (2) Regular maintenance.	Regular maintenance. Storage tanks proposed with 2 separate compartments with concrete partition within storage tanks and provision of water level sensors (high/low level)	Low level alarm in storage tank and tank provides a reservoir. Tank split into two sections & only 50% drained for maintenance. Valve always locked closed in normal operation and only opened for maintenance. Hose reel, breeching inlet and manual fire extinguishers are independent of Sprinkler system.

Previous Problems and Constraints

System	Total Number of Hazards for 5 Stages	Total Number of Common Hazards	Percentage Reduction
TVS/ECS	507	260	44.60%
ELE	469	263	42.64%
FPS	331	188	38.07%
Total	1307	711	42.23%

New Concept for Future RTS Projects

Four Key Concepts

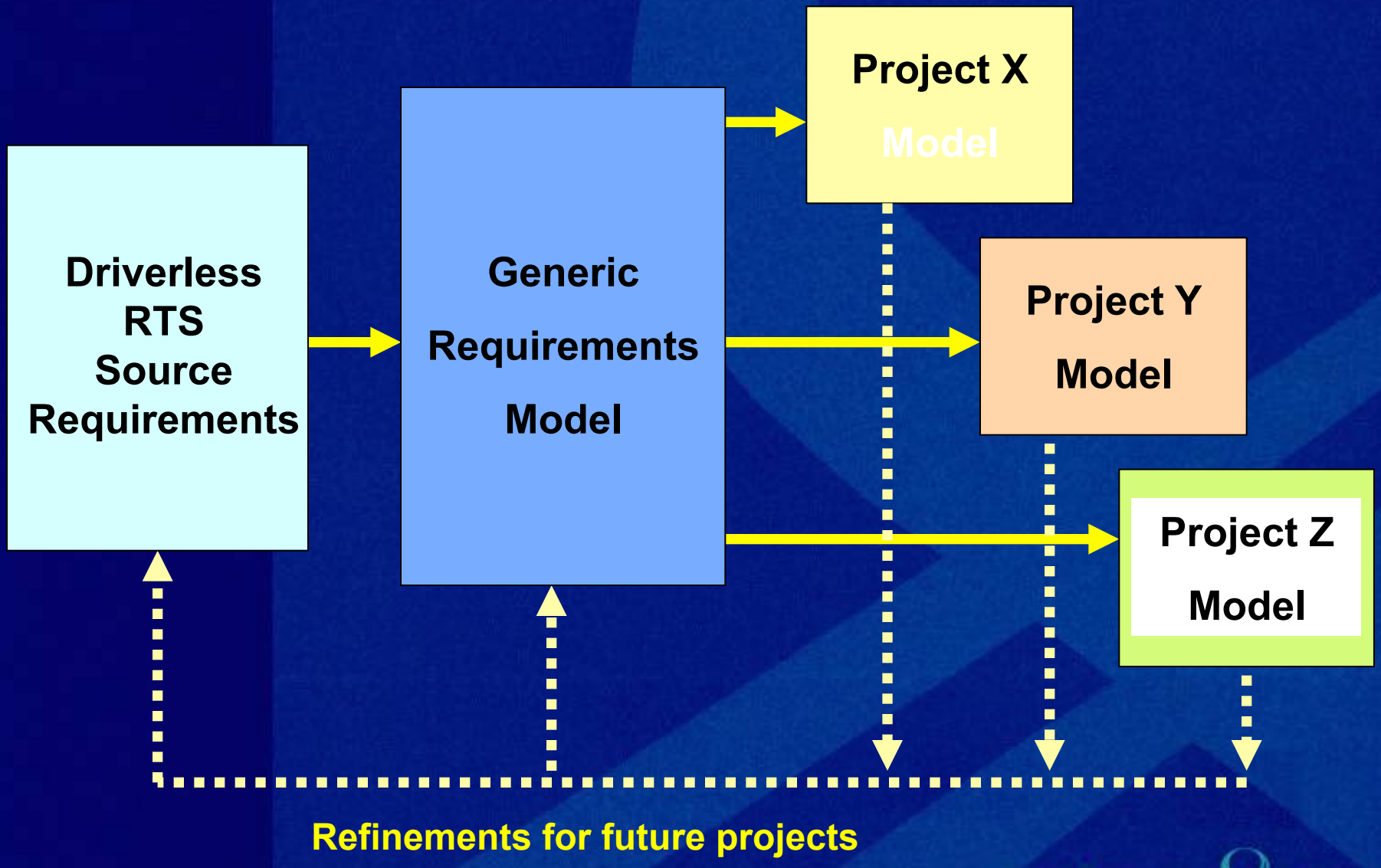
Complete systemic elicitation of RTS source requirements

Generic SoS requirements modeling

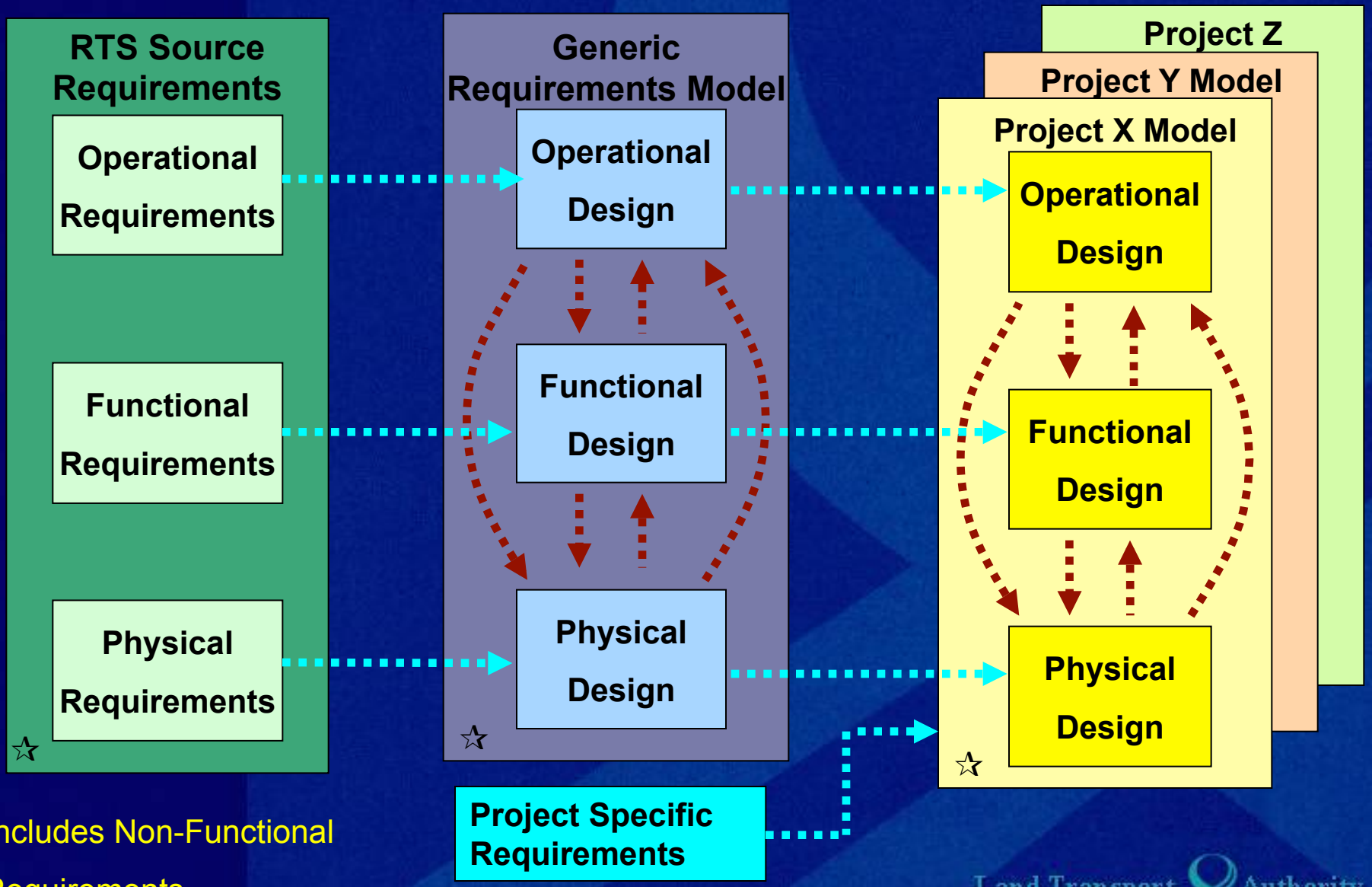
Reuse of generic SoS requirements

Continuous refinement for future changing needs

New Concept for Future RTS Projects



New Concept for Future RTS Projects

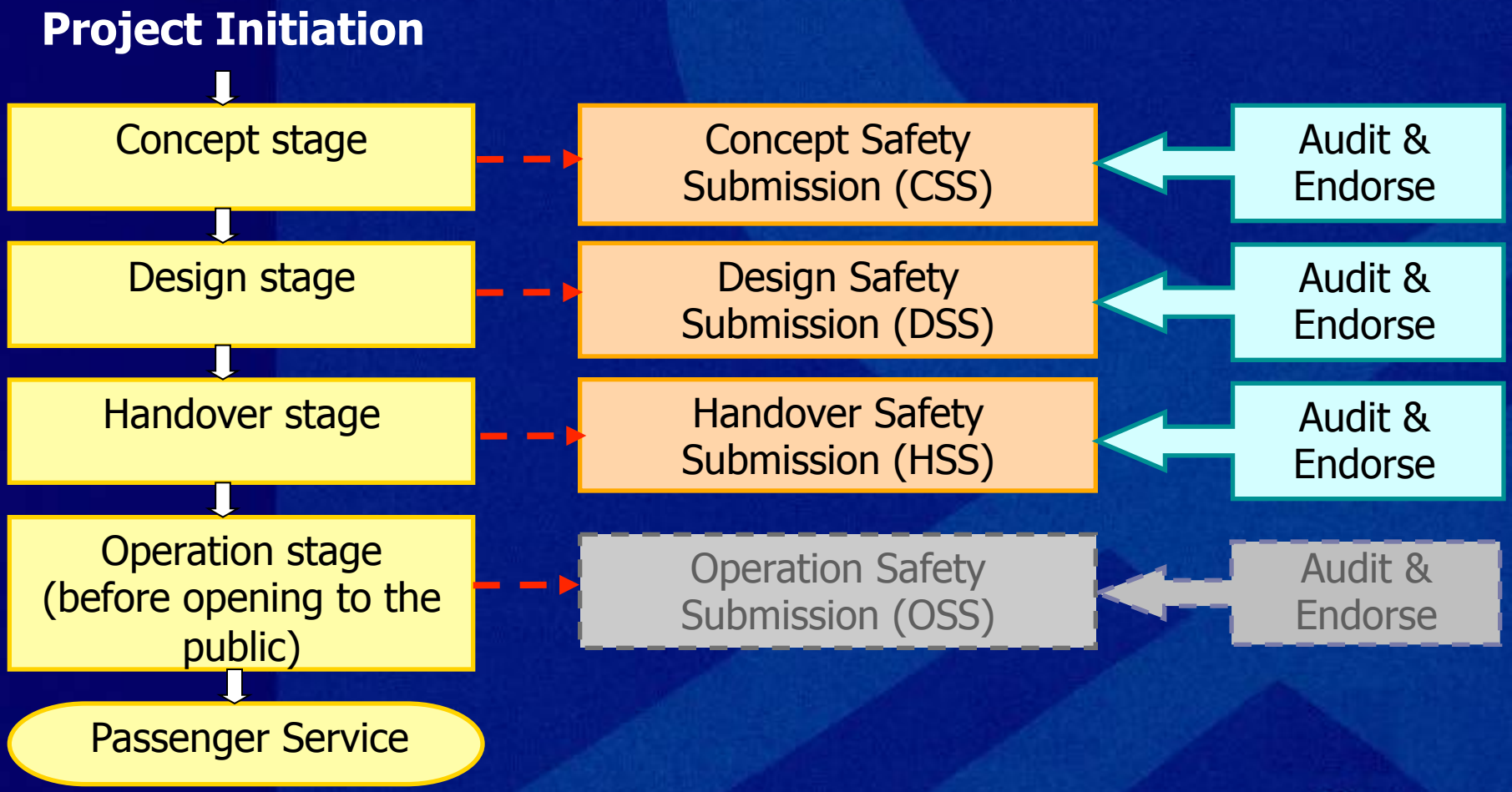


☆ Includes Non-Functional Requirements

Land Transport Authority

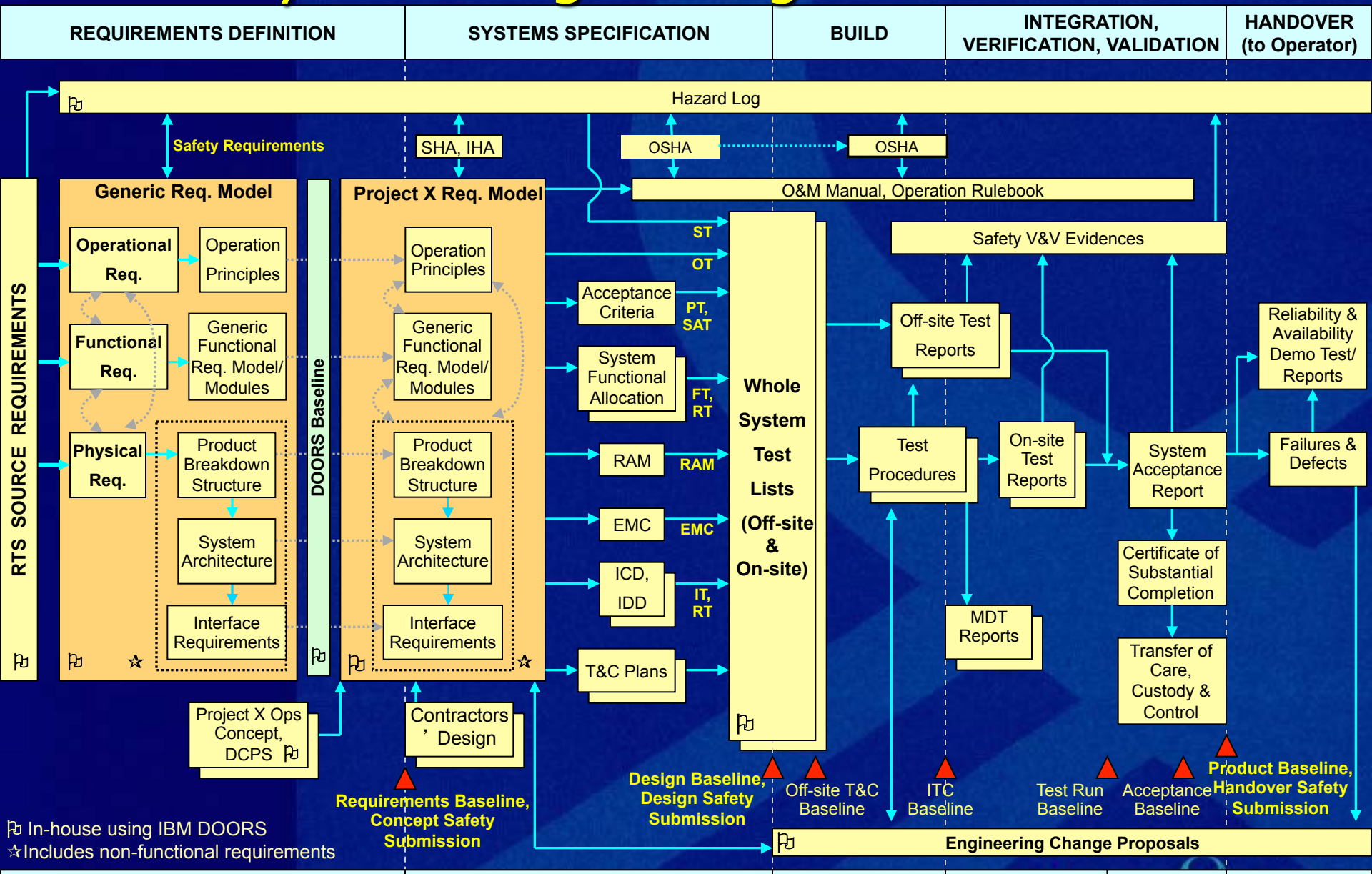
Project Safety Review (PSR) Process

* PSR is developed with reference to IEC 62278, IEC 62279 & IEC 62425



Land Transport Authority

Generic Systems Engineering Process



Building the Generic Requirements Model

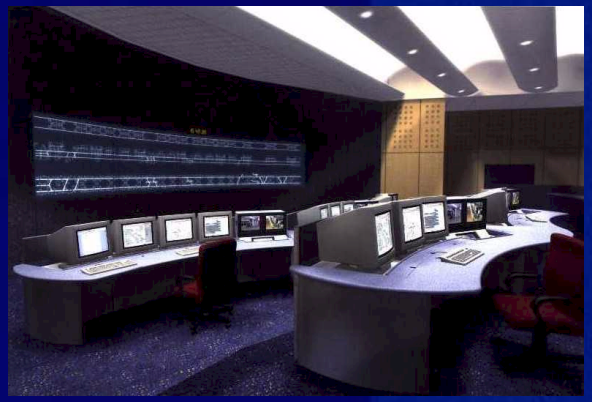
- Constructed using a combination of:
  - ✓ Scenario-based Requirements Analysis
  - ✓ Top-Down Partitioning Technique
- Scenario-Based Requirements Analysis:
  - Operation Control Centre (OCC) Operation
  - Depot Operation
  - Station and Trackside Operation
  - Trainborne Operation
- Top-Down partitioning
  - Product Breakdown Structure (System model)
  - Dataflow Diagram

Building the Generic Requirements Model

- Reuse of Generic Requirements Model
  - Reuse for future RTS projects with similar Operational Concepts
- Proper Configuration Baseline ensures
  - Each project will have a common base requirements
  - Each project will develop its distinct Project Requirements and Design Baseline
  - Project specific requirements will be uniquely addressed

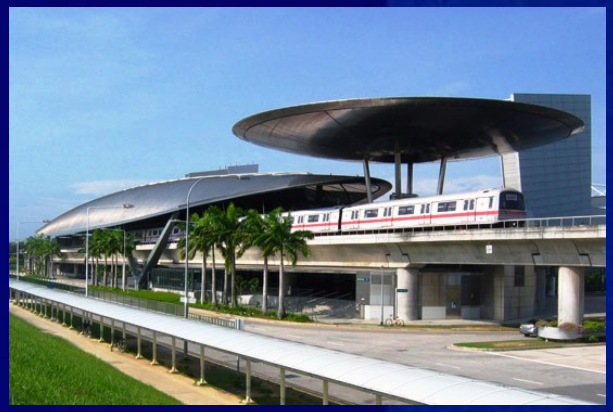
Generic Requirements Model

OCC Operation (FO-0)



Depot Operation (FD-0)

Station/Trackside Operation (FS-0)



Train Operation (FT-0)

Generic Functional Requirements

FT-0 Train Operation

FT-1 Prepare Train

FT-1.1 Startup/Close Railway Line

FT-1.1.1 Wakeup Train

[Functional Description]

[Operation Conditions]

[Safety Requirements]

[System Allocation]

…

FT-1.2 Manage Train Op Modes

FT-1.2.1 Determine Driving Mode

[Functional Description]

[Operation Conditions]

[Safety Requirements]

[System Allocation]

…

FT-2 Protect Train Movement

FT-3 Move Train

FT-4 Provide Train Communication

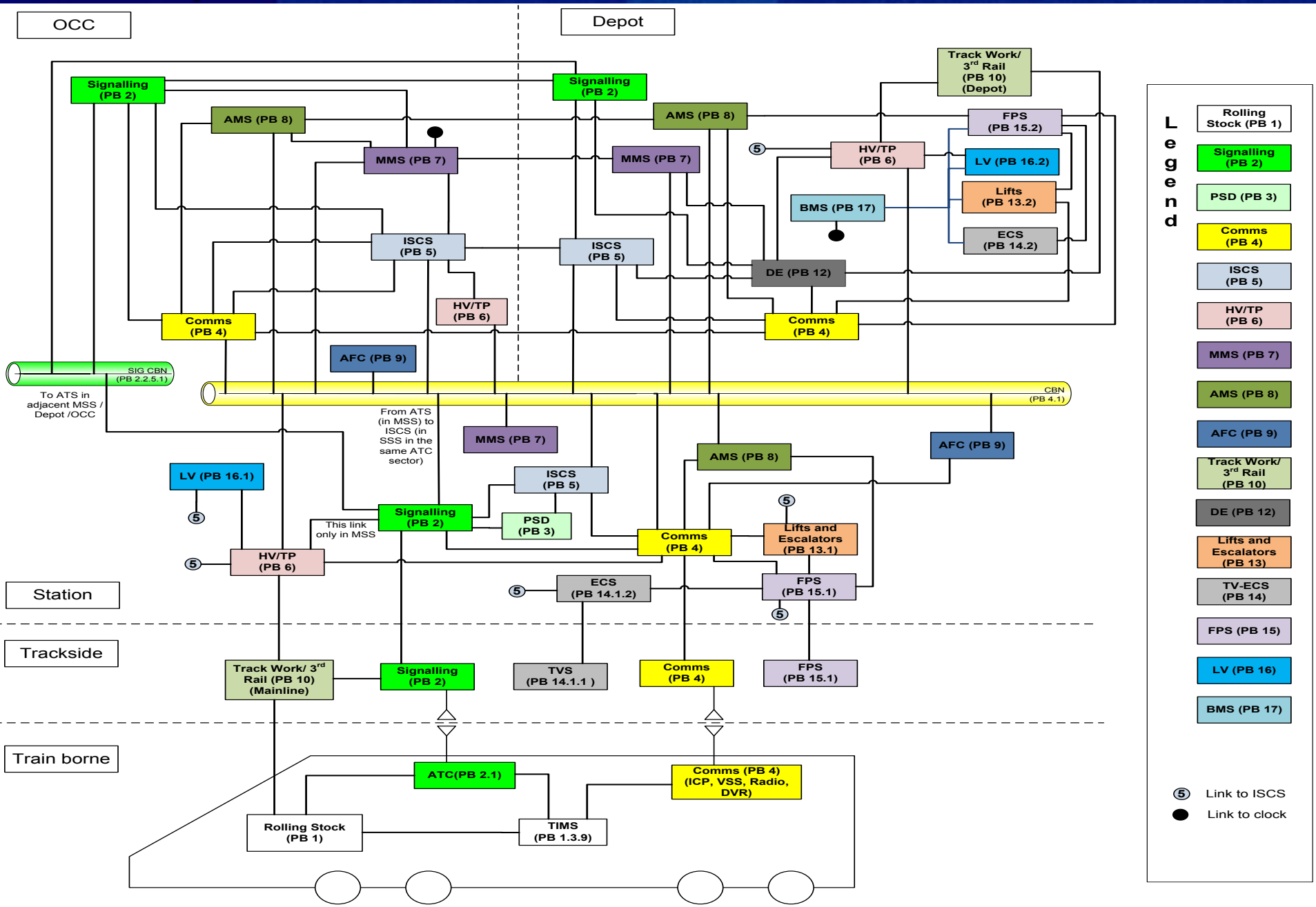
FT-5 Monitor Train

…

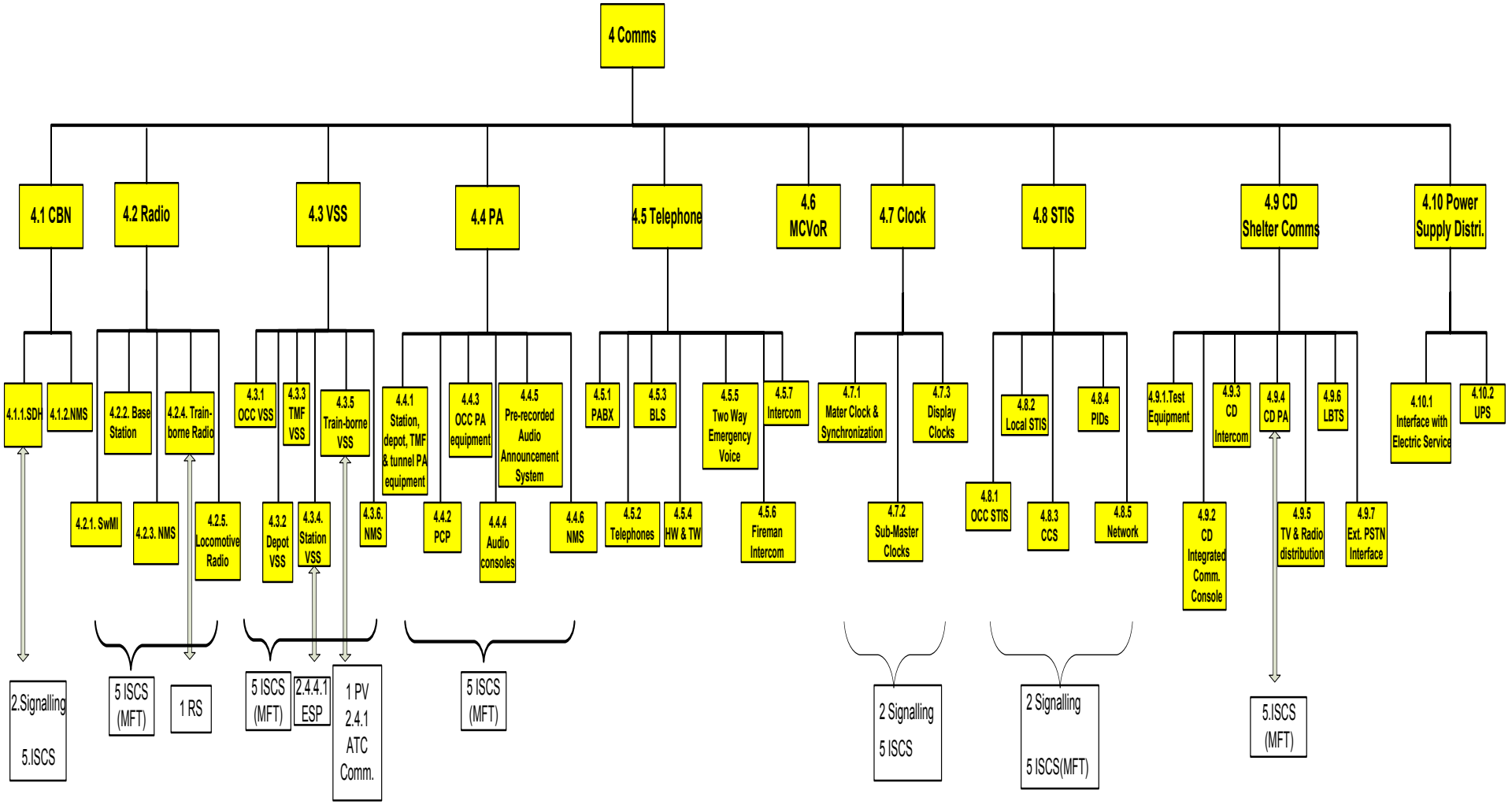
FS-0 Station/Trackside Operation

…

RTS System Model

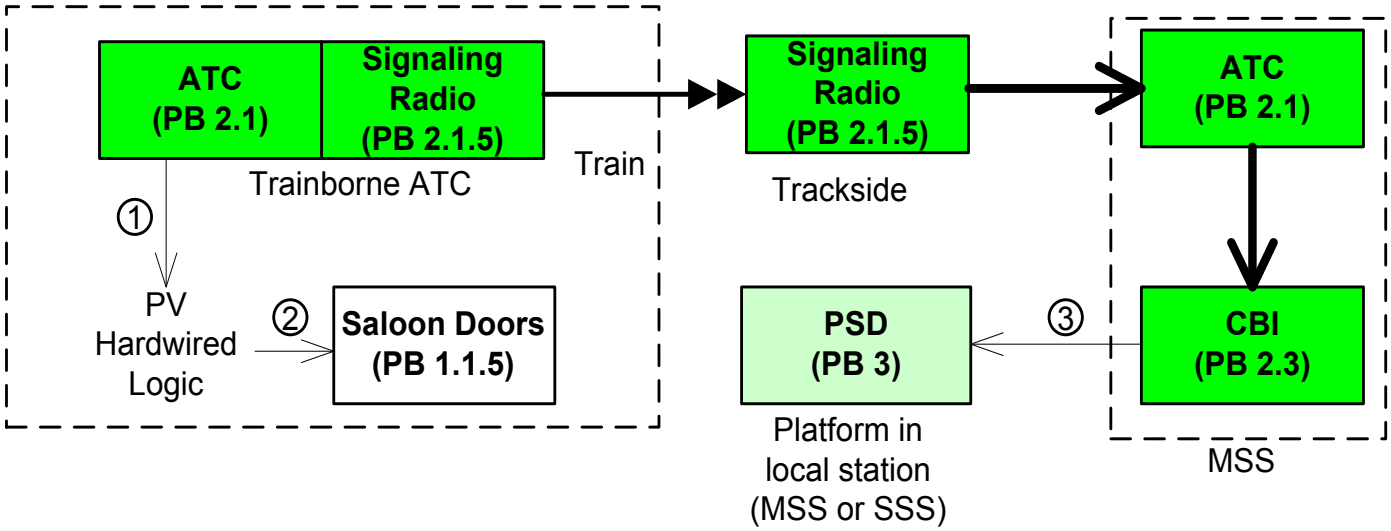


Architecture Tree – Communication System



Functional Dataflow Diagram

Manage synchronized train door (saloon doors) and PSD opening/closing sequence (Automatic mode/ Remote Control)



Command transmit:

① Hardwired VITAL authorization (left doors or right doors) and NOT VITAL command to open saloon doors.

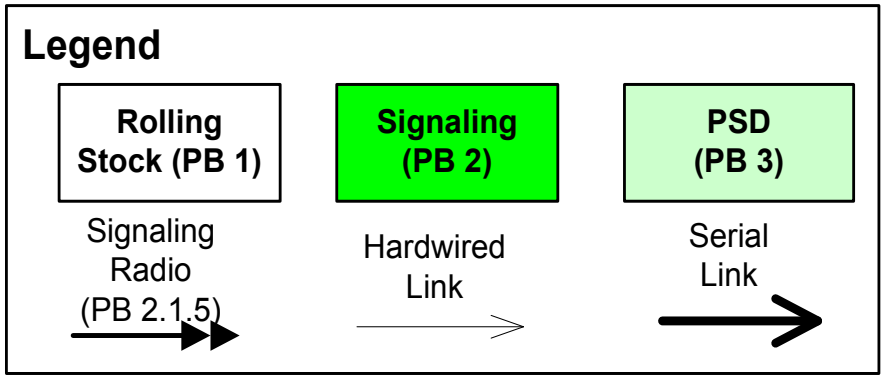
② Command to energise the correct doors open train line.

③ Hardwired VITAL command to open PSD.

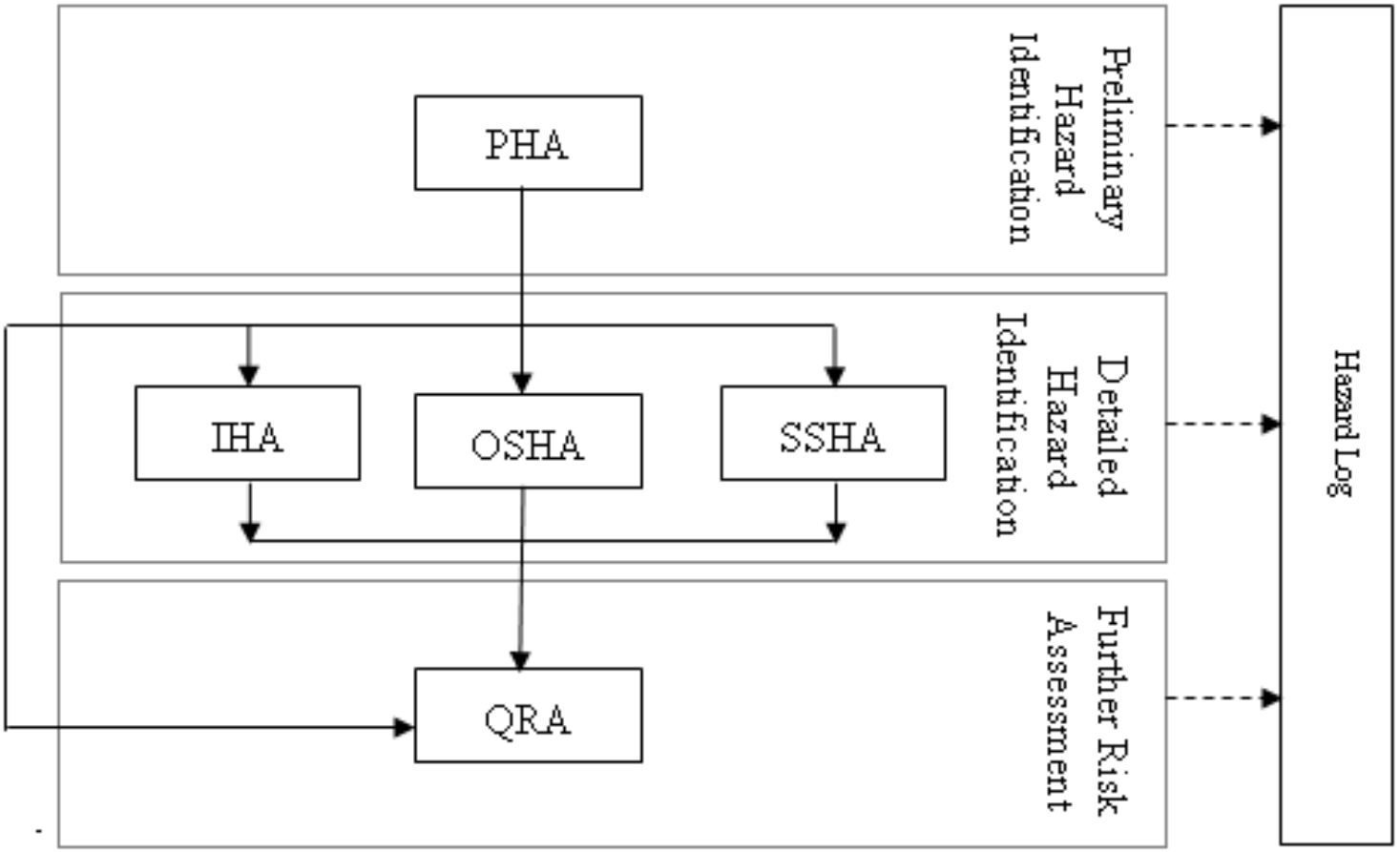
④ Hardwired VITAL authorization (left doors or right doors).

⑤ Command to illuminate the open push buttons on the driving console, and door open command to ATC

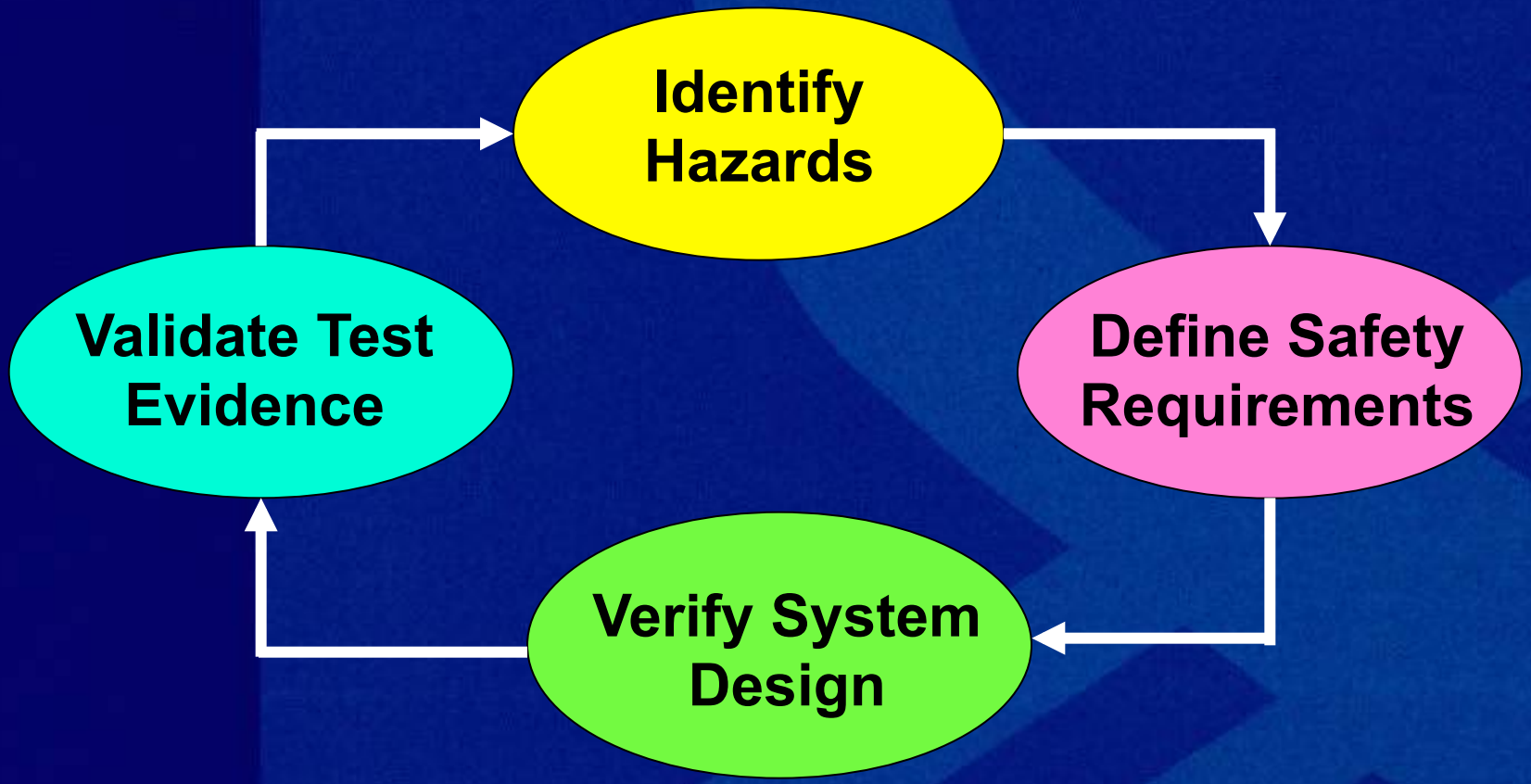
⑥ Drivers to issue door open command by pressing open push buttons.



Requirements-based Hazards Management



Requirements-based Hazards Management



Requirements-based Hazards Management

- Generic safety requirements is developed at to address all high-level hazards identified at concept phase
- References:
  - IEC 62267 Railway applications – Automated urban guided transport – Safety Requirements (2009-07)
  - Best practices e.g. UK Railway Safety Principles and Guidelines (a.k.a. Blue Book)
  - Project experiences

Requirements-based Hazards Management

Generic Safety Requirements

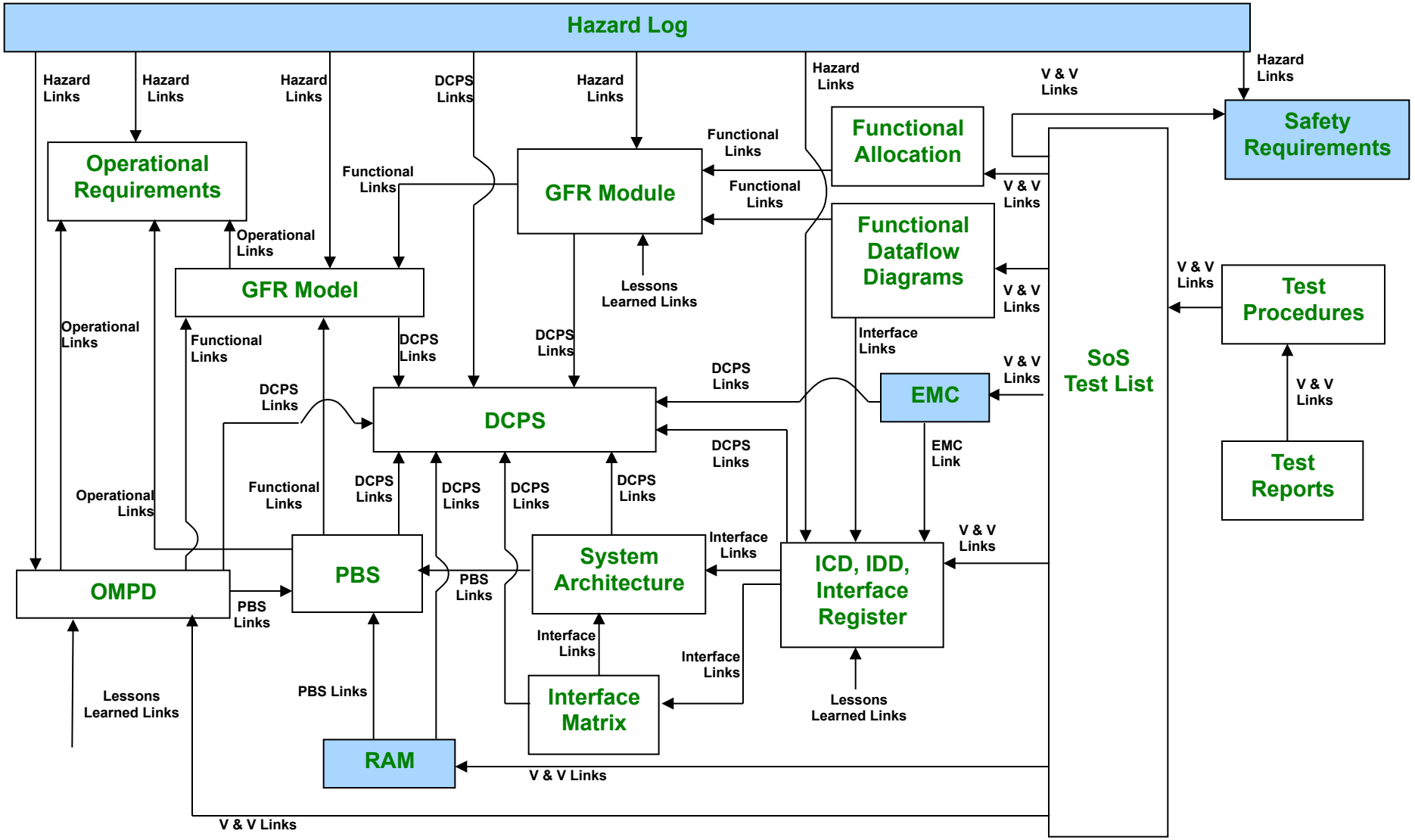
Land Transport Authority

Source	SR_ ID	Sub.No	Requirement	ST	GFR	O&M	DCPS	Others
IEC 62267 (8.1.3.5)	9		**Traction Power Cut-Off**	√	√	√	√	X
IEC 62267 (8.1.3.5)		9.1	Traction power cut-off may be implemented automatic by the system, by OCC or by local staff as necessary	X	FS5.1.3 FO3.4.2	OPS1-13.6 OPS1-13.9	√	X
IEC 62267 (8.4.1.6)		9.2	In the event where a manual activated device for traction power cut-off is provided on the station platform, the function shall be integrated with the functions of other manual activated devices (i.e. emergency stop switch) on platform.	√	FS5.1.3 FO3.4.2	OPS1-13.6 OPS1-13.9	MCKS, BLS, TSSS	X
IEC 62267 (8.4.1.6)		9.3	Provisions for cutting off traction power shall be provided in locations/events where a hazardous situation from electrocution exists. This include (but not limited to):	√	FS5.1.3 FO3.4.2	OPS1-13.6 OPS1-13.9	√	X
IEC 62267 (8.4.1.6)		9.3.1	Track area that can be reached from platform (where risk of person fall/intrusion and inadvertently touching system elements energised with traction power exist). In the event where risk of electrocution is detected, an automatic traction power cut-off device shall be initiated.	X	FS5.1.3 FO3.4.2	OPS1-13.6 OPS1-13.9	√	X
IEC 62267 (8.5.3)		9.3.2	In the event there is an EVAC request and train stopped partially outside the platform track with train doors opened, traction power in the designated area shall be cut-off	√	√	√	√	X

Requirements Management

- Managed in-house using IBM® Rational® DOORS® requirements management tool
- Houses the Generic Model and Project Models
- Facilitates the management of different project folder hierarchies and their configuration baselines
- Streamline task assignments for job specializations

Requirements Management - DOORS



Generic Functional Requirements Module

ID	Function	Design Considerations	Triggering Events	System Allocation	Related Functions	Safety Related	IEC6
	authorises the 750V network section turn-on/shutdown.			breakdown.	FD2.2 Provide Power Supply	breakdown.	
FS4.1 Distribute Power Supply	To distribute the 22KV, 750V, 415V power supply.	Refer to FO2.1.1 Distribute Power Supply.	Refer to FO2.1.1 Distribute Power Supply.	PS (L)	FS4.1 Distribute Power Supply, FO2.1.1 Distribute Power Supply, FD2.2.1 Distribute Power Supply	Yes	6.4.
FS4.2 Monitor/Control Power Supply	To supervise the monitoring and control of the power distribution network.	Refer to FO2.1.2 Monitor/Control Power Supply.	Refer to FO2.1.2 Monitor/Control Power Supply.	ISCS (L), PS, Operator	FS4.2 Monitor/Control Power Supply, FO2.1.2 Monitor/Control Power Supply, FD2.2.2 Monitor/Control Power Supply	Yes	6.4.
FS4.3 Manage Traction Power Shutoff	To protect staffs from the risk of injury due to train movement and electrocution using available switches.	Refer to FO2.1.3 Manage Traction Power Shutoff.	Refer to FO2.1.3 Manage Traction Power Shutoff.	SIG (L), PS, COM, Operator	The functions related to traction power shutdown include: FT5.6 Manage Loss Of Traction Power, FS4.3 Manage Traction Power Shutoff, FO2.1.3 Manage Traction Power Shutoff, FD2.2.3 Manage Traction Power Shutoff The functions related to evacuation include: FT5.3 Provide Train Evacuation, FS2.2.2 Supervise Station/Tunnel Evacuation, FO1.5.11 Supervise Train Evacuation	Yes	6.4.
FS5 Provide Supervisory Control System	To provide, monitor and communicate station/trackside equipment status to detect failures or incidents which could lead to operational disturbances.	Refer to function breakdown.	Refer to function breakdown.	Refer to function breakdown.	The functions related to SCADA include: FS5 Provide Supervisory Control System, FO2.2 Provide Supervisory Control System, FD2.2 Provide Supervisory Control System	Refer to function breakdown.	6.5
FS5.1 Monitor And Display Operation Data	To monitor and display the train traffic and systems equipment's real time data, historical and	1) The ATS and ISCS GUI shall be integrated on the MFTs provided by ISCS.	1) Automatic by ISCS/ATS.	ISCS (L)	The functions related to send/display equipment data include:	Yes	6.3.

Operational Modes and Principles Definition (OMPD)

'OMPD' current 0.0 in /Generic Req. Model/Operational Requirements/Operational Modes and Principles Document (Formal module) - DOORS

File Edit View Insert Link Analysis Table Tools Discussions User Help

Save (Ctrl+S)

All levels

ID	
117	**3 Emergency Mode Operations**
118	3.1 Evacuation Process
119	3.2 General Description For evacuation of train, the normal evacuation strategy is always to bring the incident train to station platform and then evacuate passengers to station. However, there are situations whereby passengers have to evacuate the train before the train is brought to the station platform. The primary route of evacuation then is through the end detrainment doors onto the trackway. The secondary mode will be via the side (saloon) doors. The saloon doors will only be used for detrainment during train evacuation at station or as otherwise decided by staff on board the train or appropriately by OCC. Generally, passenger evacuation procedure from train in between stations initiates from either Passengers onboard train or Operation Control Centre (OCC) operator. Evacuation of train passengers would be generally to the station. Train passengers can also evacuate to an escape shaft if there are more advantages or that the situation requires so.
120	3.3 Cases of application (a) Evacuation Initiated by Passenger from Train in Tunnel (b) Two stalled trains between stations (c) Evacuation Initiated by OCC Operator in Tunnel (d) Evacuation triggered by equipment failure affecting passengers on train (e) Station evacuation
121	3.4 Evacuation initiated by passengers from train in tunnel
122	3.4.1 General Description An evacuation initiated by passenger is one where passengers attempt to leave the train without or prior to being initiated by OCC operator. A passenger initiated evacuation from the train can result from either activation of the end detrainment door or manual door release device for the saloon door. **End Detrainment Door** It is to be noted that should it be necessary to evacuate the train passengers following the activation of the manual door release device for saloon door, the route of evacuation is through the end detrainment door.

Land Transport Authority

Continuous Process Refinement

Continuous refinement for future changing needs

- The Generic Model is regularly updated for:
  - New requirements
  - Design initiatives for new technology
  - Lessons learned from past and current projects
  - Process and design enhancements due to better understanding of emergent properties
- All new Projects will benefit from an up-to-date SoS Requirements
- Improved interactions among different stakeholders, in-house designers, contractors and operators

Challenges and Uncertainties

1. Extensive design considerations, experiences and discussions required to select a solution
2. Reaching design agreement among stakeholders, in-house designers, contractors and operators
3. New requirements are harder to assess compared to tried and tested design requirements
4. Design uncertainties introduced by the Contractors' system constraints
5. Teamwork, communication and commitment are essential ingredients for successful implementation

Expected Benefits

1. Enables a structured, reference starting point to guide a project from concept to design stage	
2. Uncovers the 'real' SoS requirements and secures the desired emergent properties at an early stage	
3. Evaluates the complete problem before selecting a balanced solution	
4. Provides a clear understanding on the design consequences before construction	
5. Accelerates the design conceptualization and development without losing the flexibility to iterate these requirements in details	
6. Provides ease of work breakdown and allocation and effective contract interface partitioning	
7. Facilitates configuration management, requirements trace and test activities sequencing	

Thank You.