MODSafe

Modular Urban Transport Safety and Security Analysis

Final Conference
25 – 26 June 2012, Cologne

Hazard Mitigation Measures

presented by Rajinder Sadheura
Bombardier

SEVENTH FRAMEWORK PROGRAMME

BOMBARDIER MODSafe

Main activities performed

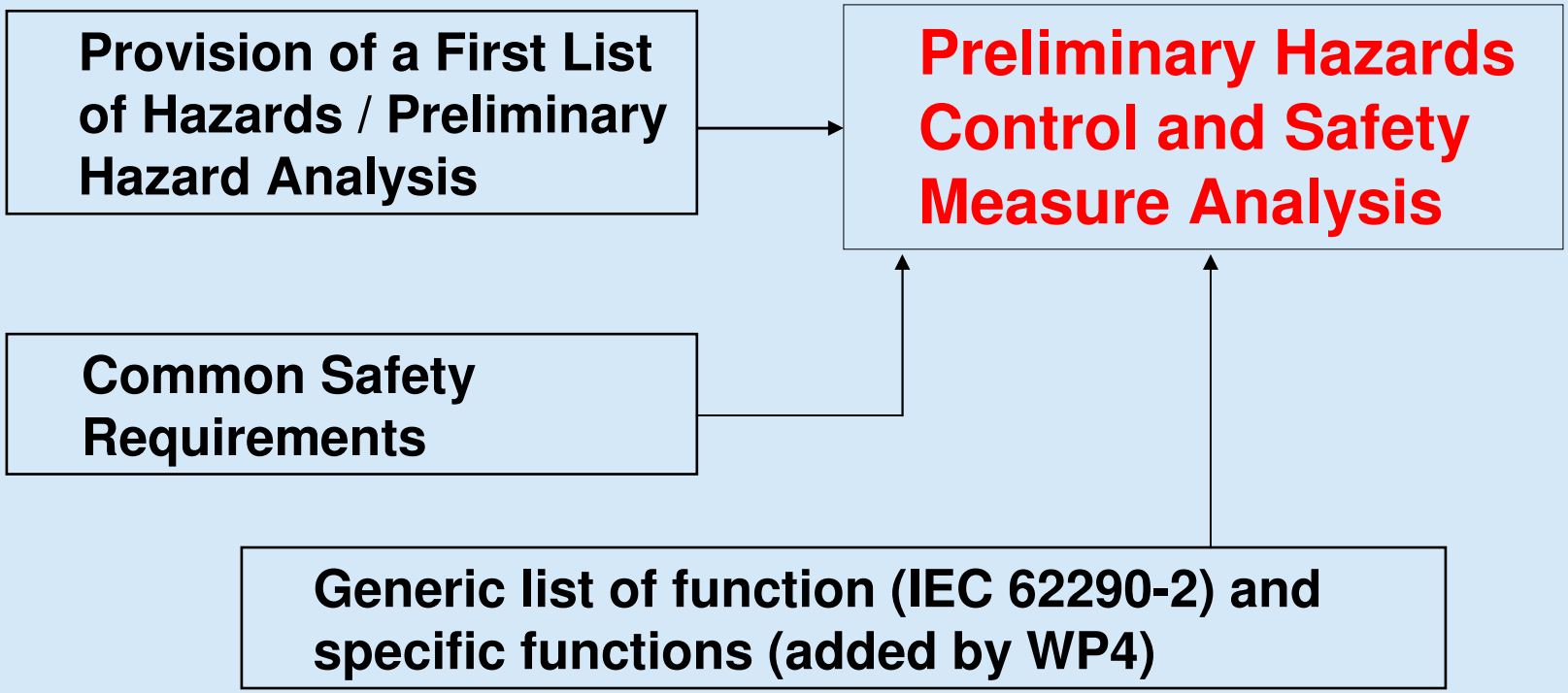
- Analysis of existing safety functions from MODURBAN D80 and UGTMS IEC 62290 projects and other generic safety functions of supply industry mapped against the hazards and risk analysis.
- GOA identified
- Non safety functions are excluded
- Mitigation measures to eliminate or control risk (Technical, Procedural or Maintenance) added

Grades of automation (GOA)

- There are 5 grades of automation defined ranging from 0 to 4:
  - GOA0: On-sight train operation. For example, TRAMs.
    Not considered within the scope as driver has full responsibility for the train in this mode.
  - GOA1a: Non-automated train operation with intermittent supervision
  - GOA1b: Non-automated train operation with continuous supervision
  - GOA2: Semi-automated train operation
  - GOA3: Driverless train operation
  - GOA4: Unattended train operation
- GOA (1a, 1b, 2, 3 & 4) are marked as Not Applicable (N/A), Mandatory (M) or Optional (O)

Method for MODSafe WP3 Delivery – Preliminary version

Mapping of hazards to existing generic safety functions from previous EC projects and other generic safety functions of supply industry



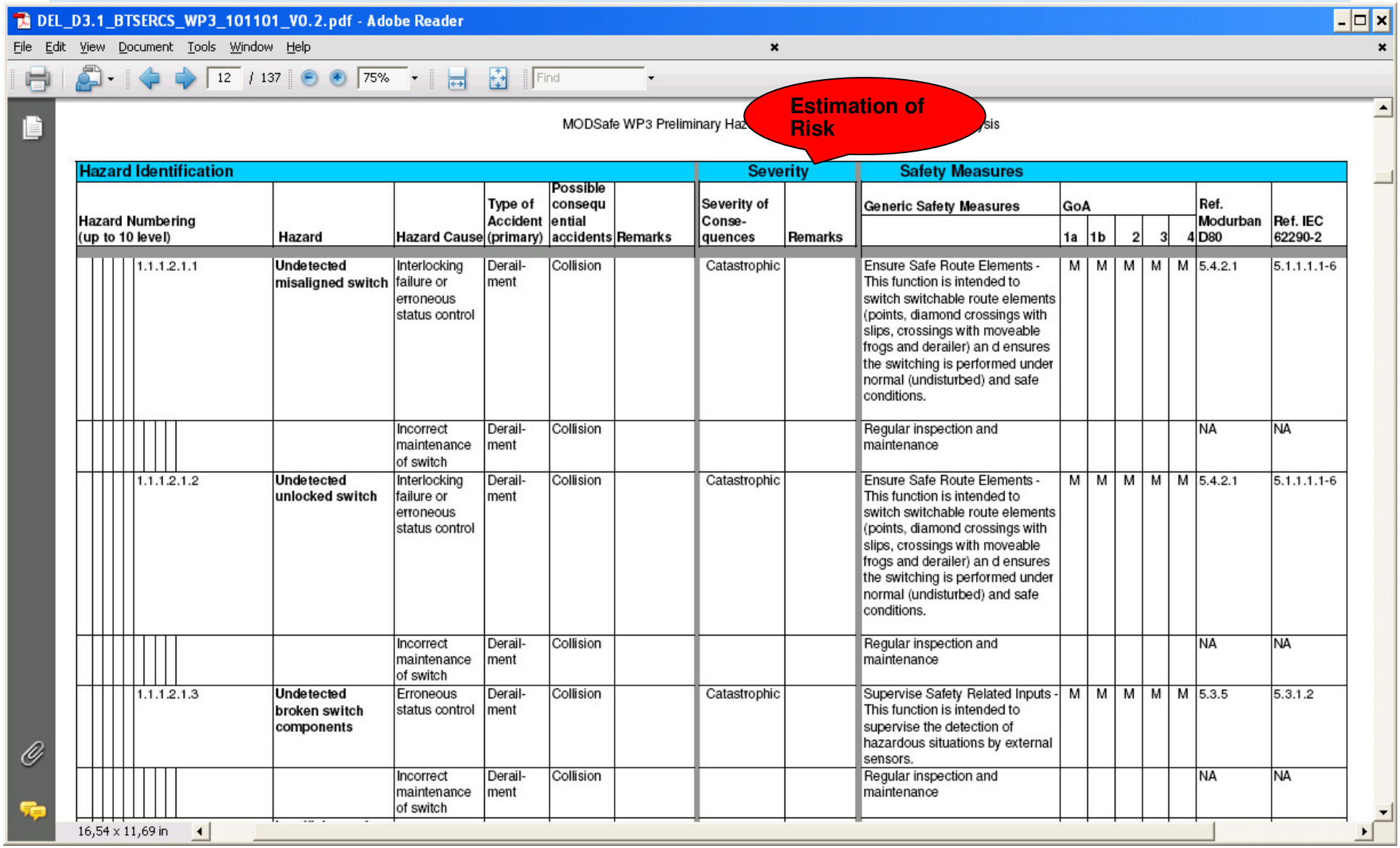
Category of hazards considered

- Train movement
- Train interior
- Train station interface (with train already in station)
- Train station interface (without train in station)
- Depot
- Operations Control Centre
- Maintenance
- Emergency – Evacuation
- Environment (weather conditions and force of nature)

Safety function areas considered in Interim version

- Loading of infrastructure data and internal tests
- Temporary speed restrictions
- Supervision of rolling stock (train integrity, closed doors)
- Supervise intrusion or fall on track
- Supervise sensors for obstacles, derailment, smoke, broken rail etc.
- Ensure safe route
- Ensure safe train movement within its route
- Manage door opening
- Authorise train departure
- Establish zone of protection due to hazard or trackside maintenance
- Respond to train rollaway
- Supervise evacuation
- Provide communication with staff

Interim Annex Layout



DEL_D3.1_BTSERCS_WP3_101101_V0.2.pdf - Adobe Reader

File Edit View Document Tools Window Help

12 / 137 75% Find

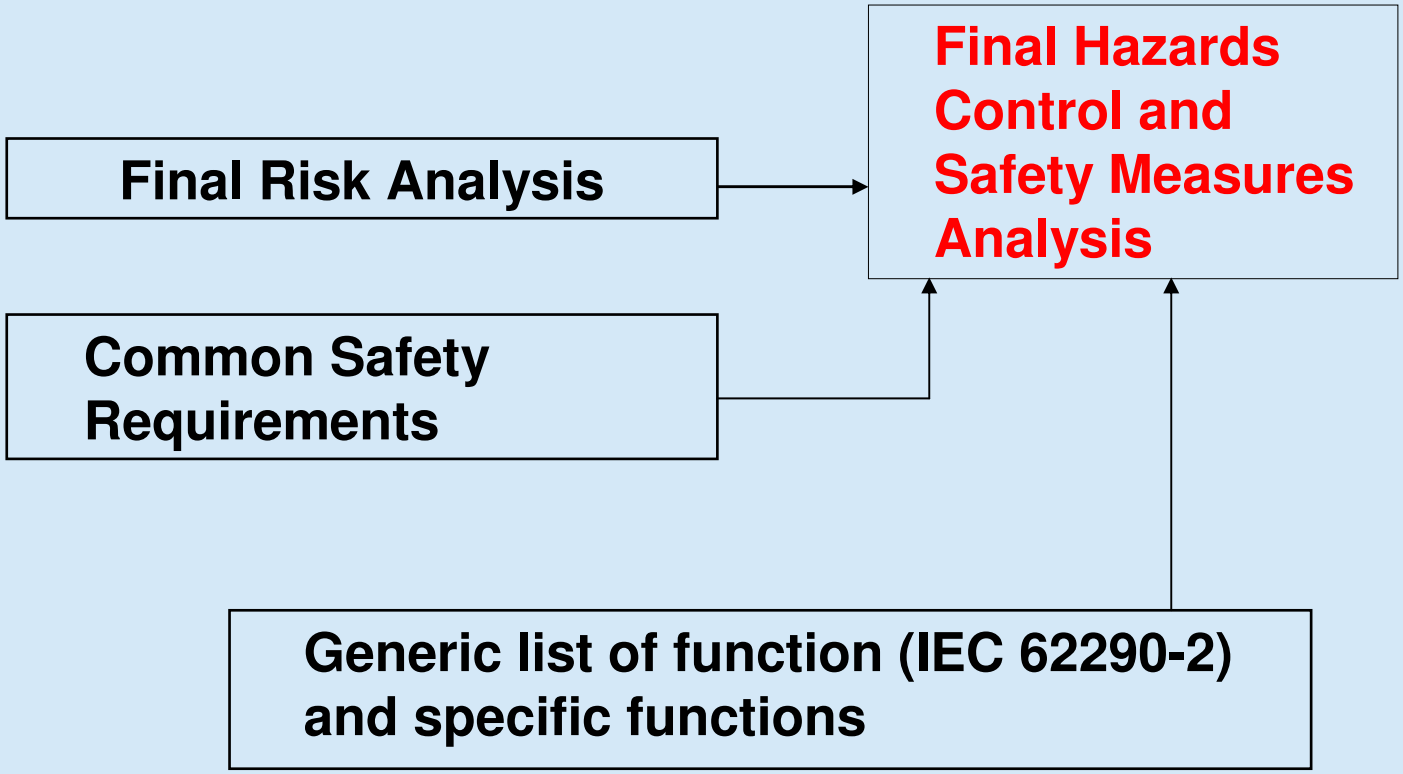
Estimation of Risk

MODSafe WP3 Preliminary Haz sis

Hazard Identification						Severity		Safety Measures							
Hazard Numbering (up to 10 level)	Hazard	Hazard Cause	Type of Accident (primary)	Possible consequential accidents	Remarks	Severity of Consequences	Remarks	Generic Safety Measures	GoA 1a	GoA 1b	GoA 2	GoA 3	GoA 4	Ref. Modurban D80	Ref. IEC 62290-2
1.1.1.2.1.1	**Undetected misaligned switch**	Interlocking failure or erroneous status control	Derail-ment	Collision		Catastrophic		Ensure Safe Route Elements - This function is intended to switch switchable route elements (points, diamond crossings with slips, crossings with moveable frogs and derailer) an d ensures the switching is performed under normal (undisturbed) and safe conditions.	M	M	M	M	M	5.4.2.1	5.1.1.1.1-6
		Incorrect maintenance of switch	Derail-ment	Collision				Regular inspection and maintenance						NA	NA
1.1.1.2.1.2	**Undetected unlocked switch**	Interlocking failure or erroneous status control	Derail-ment	Collision		Catastrophic		Ensure Safe Route Elements - This function is intended to switch switchable route elements (points, diamond crossings with slips, crossings with moveable frogs and derailer) an d ensures the switching is performed under normal (undisturbed) and safe conditions.	M	M	M	M	M	5.4.2.1	5.1.1.1.1-6
		Incorrect maintenance of switch	Derail-ment	Collision				Regular inspection and maintenance						NA	NA
1.1.1.2.1.3	**Undetected broken switch components**	Erroneous status control	Derail-ment	Collision		Catastrophic		Supervise Safety Related Inputs - This function is intended to supervise the detection of hazardous situations by external sensors.	M	M	M	M	M	5.3.5	5.3.1.2
		Incorrect maintenance of switch	Derail-ment	Collision				Regular inspection and maintenance						NA	NA

16,54 x 11,69 in

Method for MODSafe Final Delivery



Additional Safety functions identified by WP4

- Supervise rolling stock speed restriction
- Authorise train movement by wayside signals
- Restrict train entry to station or inhibit stop at station
- React to unauthorised movement of non-operative and unequipped trains
- Protect passengers at platform (platform edge warning, emergency stop requests, platform doors)
- Supervise doors closing
- Manage depot and stabling areas
- Manage different stopping positions at a station
- Coupling and decoupling
- React to passenger alarm device

Constitency between Risk analysis and safety measures:

- Special consideration to hazards where human procedure is quoted as reduction measure for intolerable risks.
- These hazards are highlighted or technical mitigations added whenever possible. This is Because safety cannot rely only on a single human failure.
- Where technical mitigations not possible then such hazards are identified.

Final Annex Layout

1 2 3

Hazard Identification				Estimation of initial risk				Safety Measures										
Hazard Numbering (up to 10 level)	Hazard	Hazard Cause	Type of Accident (primary)	Severity of Consequences	Assumed Probability	Risk reduction	Risk	Generic Safety Measures	Category of Safety Measure (T, P, M)	GOA 1a	GOA 1b	GOA 2	GOA 3	GOA 4	Ref. Modurban D80	Ref. IEC 62290-2	Remarks
1.1.1.2.1.2	Undetected unlocked switch	Interlocking failure or erroneous status control	Derail-ment	Catastrophic	Frequent	1	Intolerable	Ensure Safe Route Elements	T	M	M	M	M	M	5.4.2.1	5.1.1.1.1-6	Safety function This function is intended to switch switchable route elements (points, diamond crossings with slips, crossings with moveable frogs and derailer) and ensures the switching is performed under normal (undisturbed) and safe conditions.
		Incorrect maintenance of switch	Derail-ment					Regular inspection and maintenance	M						NA	NA	Non functional requirement. Maintenance manuals.
1.1.1.2.1.3	Undetected broken switch components	Erroneous status control	Derail-ment	Catastrophic	Frequent	1	Intolerable	Supervise Safety Related Inputs.	T	M	M	M	M	M	5.3.5	5.3.1.2	Safety function This function is intended to supervise the detection of hazardous situations by external sensors.
		Incorrect maintenance of switch	Derail-ment					Regular inspection and maintenance	M						NA	NA	Non functional requirement. Maintenance manuals.
1.1.1.2.2	Insufficient safety distance to moving switch																
1.1.1.2.2.1	Insufficient worst case safety distance																
1.1.1.2.2.1.1	Wrong worst case safety distance registered (on train)																
1.1.1.2.2.1.1.1	Failed or incorrect communication of worst case safety distance (stop point / speed limit)	Data communication failure	Derail-ment	Catastrophic	Frequent	1	Intolerable	Provide Communication with Staff	T	M	M	M	M	M	5.9.2	Ref. Missing $ $	Safety function This function is intended to inform staff about availability of functions concerning operation and status of data communication equipment.

1 Hazard Identification

Hazard Identification			
Hazard Numbering (up to 10 level)	Hazard	Hazard Cause	Type of Accident (primary)
1.1.1.1.1.1	**Wrong position registered**	Odometer failure	Derail-ment
1.1.1.1.1.2	**Wrong speed registered**		
1.1.1.1.1.2.1	**Speed measurement failure**	Wheelspin	Derail-ment
1.1.1.1.1.2.2	**On-board speed processing failure**	On-Board ATP equipment design failure	Derail-ment
		Incorrect maintenance of On-Board ATP equipment	Derail-ment

2 Estimation of initial risk

Estimation of initial risk			
Severity of Consequences	Assumed Probability	Risk reduction	Risk
Catastrophic	Frequent	1	Intolerable
Catastrophic	Frequent	1	Intolerable
Catastrophic	Frequent	1	Intolerable

3 Safety Measures

Safety Measures									
Generic Safety Measures	Category of Safety Measure (T, P, M)	GOA					Ref. Modurban D80	Ref. IEC 62290-2	Remarks
		1a	1b	2	3	4			
Determine Train Location	T	NA	M	M	M	M	5.4.1.2	5.1.2.2.3	Safety function
Respond to Train Location Failure	T	NA	M	M	M	M	5.7.2	NA	Safety function
	T								
Calculate Train Speed - This function determines train speed.	T	O	M	M	M	M	5.4.1.7	5.1.5.1	Safety function
Supervise Actual Speed - This function supervises the operation of trains to ensure that trains remain within the dynamic speed profile.	T	O	M	M	M	M	5.4.3.4	5.1.5.2	Safety function
Calculate Train Speed - This function determines train speed.	T	O	M	M	M	M	5.4.1.7	5.1.5.1	Safety function

Summary

- Each hazard within the scope of this analysis has been assigned a corresponding safety function from MODURBAN D80 where possible.
- Category of Safety Measures has been assigned to all hazards.
- GOA assigned to all hazards.