INTEGRATION
ENGINEERING SAFETY MANAGEMENT

Technical Note on the use of Project Wide Hazard Review (PHWR) in Engineering Safety Management (ESM)

Document Number: CRL1-XRL-O8-GPS-CR001-50024

Current Document History:

Revision:	Effective Date:	Author(s) ('Owner' in eB *)	Reviewed by: ('Checked by' in eB *)	Approved by:	Reason for Issue:
1.0	18/05/2016	Stephen James	Chi Wong	Jeremy Bates	First Issue

Revision Changes:

Revision	Status / Description of Changes
1.0	First revision.

Contents

1 Introduction

1.1 Technical Note on the Use of the PWHR in the ESM Process

This document shall be used as a technical note for Project Wide Hazard Review (PWHR) in accordance with the Engineering Safety Hazard Management Procedure (Ref 1).

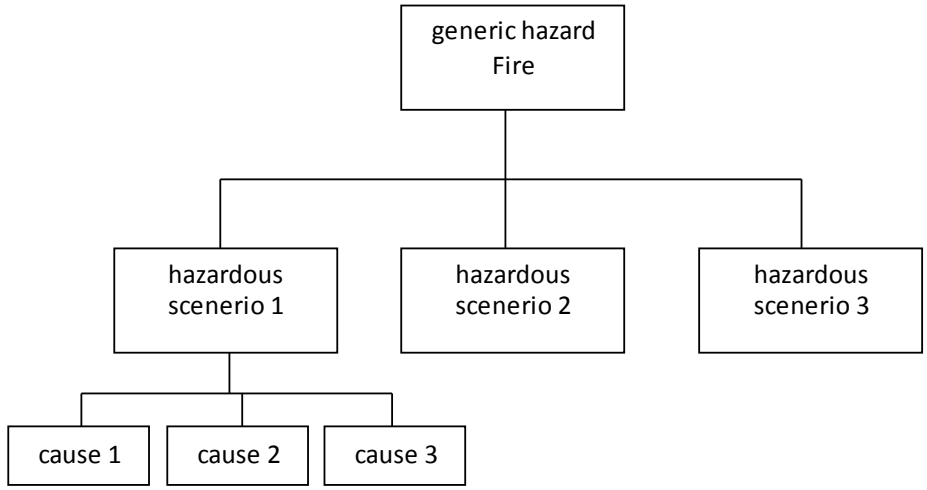
The Technical Note is not a complete set of instructions for PWHR use but represent a response to observations of some current PWHR practice. They form a part elaboration on some particular aspects of the current guidance.

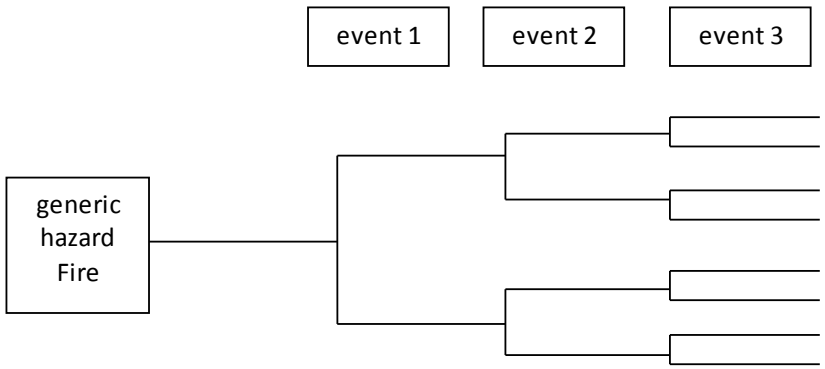
2 Scope

In what follows, the word 'system' generally refers to a station, shaft or portal.

2.1 Generic Hazard Codes

The hazards identified in the PWHR are grouped into a number of 'Generic Hazard Codes.' Associated with these are particular hazardous scenarios (states of the system) and causes and consequences. The relationship between these is shown graphically by a Fault Tree and Event Tree as follows:





It is clear that a particular hazardous scenario leads to a particular Top Event, e.g. the hazardous scenario 'Loss of cooling to plant room equipment' can lead to Fire (Fir1). The control measures and residual risk should refer to this causes identified for this hazardous scenario.

A consequence, in this example, might be evacuation and there is therefore a tendency amongst ESMs to identify this as an additional top event (generic hazard). **This is incorrect.**

Evacuation would be a consequence and should be identified in the relevant PWHR column. Control measures and risk evaluation are for the Fire top event. The consequence column can state that the control measures for 'Failure to Evacuate' are addressed under its own generic hazard code Oth2, successful evacuation itself not being a hazard.

This approach focuses the identification of control measures on the specified causes leading to the 'top event'.

It is current practice across the PWHRs to identify multiple generic hazards for a single hazard explanation and cause.

There are some hazardous scenarios that have byzantine consequences, an obvious example being EMC. These have to be treated on a case by case basis.

2.2 Hazardous Scenarios

Hazards can be identified at a very high level or at a very detailed almost FMEA level. Clearly the choice will determine the number of total hazards and the depth of control required. A risk based approach is the sensible level of hazard identification.

At too high a level the hazard is unwieldy and fails to focus the causal logic, e.g. 'loss of all fire detection and protection'. There are clear lines along which this should be split. Furthermore, a specific problem with this type of hazard description is that is combines what are likely to be two independent events. This is to be avoided unless it is the common cause failure that is being addressed.

At too low a level, many hazardous scenarios would result in the same control measures with low risk. This again is contrary to the CSM philosophy.

Further to the comment above about failures of independent systems, this is essentially beyond the design basis of the system, e.g. 'loss of all power, grid and ups'. The design is for an independent back up of power and an acceptance of risk of the residual very low frequency event. There is no further mitigation necessary. The failures of the two systems are addressed independently; loss of normal power leading to evacuation, loss of UPS on demand (leading to evacuation failure), loss of UPS under normal operation (no immediate consequence).

2.3 Beyond design basis hazards do not belong in the hazard log.

Similarly, some hazards refer to the failure of other processes, e.g. these include:

- systematic failure in the design;
- lack of a Congestion Control and Evacuation Plan (CCEP);
- lack of a fire strategy.

These are not hazards, they do not refer to an unwanted specific system state and it would be impossible to determine risk.

The PWHR is currently populated with 'non-hazards' as described above.

2.4 All Reasonably Foreseeable Hazards

The PWHR should encapsulate all of the reasonably foreseeable hazards within the definition of the system boundary and also those at the boundary of the system, i.e. the interface hazards. This is a fundamental requirement of System Safety Engineering; it's a CRL requirement, a CSM requirement and consequently an AsBo requirement.

2.5 PWHR Completeness

A systematic approach to hazard identification is fundamental to ensuring that a PWHR can claim completeness. Completeness cannot be gleaned by simply reviewing the PWHR.

Indeed, it is a necessary statement in a DESJ that 'all reasonably foreseeable hazards have been identified'. The evidence supporting this claim cannot be a reference to the PWHR. It is the systematic process that has been employed that gives confidence that necessary and sufficient System Safety Engineering acumen has been employed. The DESJ currently does not make this clear.

It is intuitive that in the application of a sound systematic approach similar systems should result in similar risks, i.e. similar hazardous scenario coverage. This might not mean the same number of hazards for each system for at least two reasons:

- There are system specific hazards;
- The lower level at which hazards are identified increases the number of hazards but does not change the output in terms of risk and safety requirements.

In view of the last paragraph, one should expect a large correlation between different systems but this is currently not the case.

In aiming to achieve completeness the following should be noted. The identification of hazards and population of the PWHR should be independent of other assurance processes or documents that form part of the overall Engineering Safety Management System. For example, hazards that are addressed by components of the Fire Strategy are nonetheless hazards with a residual risk and these should be included in the PWHR. **Without them, the PWHR is incomplete, these hazards are not managed and the residual system safety risk is not known.**

2.6 Systematic Approach To Completeness

In order for Crossrail to begin to understand the necessary coverage of the PWHR causal logic diagrams have been generated for each generic hazard code, where appropriate. The diagrams breakdown the top event into failure branches that a complete DESJ would be expected to address. Each branch should correlate to a hazard in the PWHR, to another assurance process to manage the hazard or to an argument for exclusion.

It is emphasized that the contents of the PWHR have been used to guide these drawings since a return to the HAZID stage is not desired. They are essentially a graphical way of demonstrating the hierarchical connection between:

- what is in the PWHRs;
- what is necessary for a claim of completeness;
- what is necessary for the formulation of a safety argument.

In the knowledge of their own specific system an ESM might find it necessary to make additions to these diagrams. All constructive criticism is welcome.

It is clear that the application of a single systematic approach will establish consistency across all systems with regard to completeness.

2.7 A claim for PWHR completeness is a claim that all of these branches have been considered and explicitly addressed in the DESJ.

Causal diagrams are presented below for the following generic codes:

- Fire Fir1;
- Smoke Fir2
- Fall From Height Stf1;
- Evacuation Oth2;
- Congestion Oth3.

All other Generic Hazards have a very simple causal structure, effectively the top event with a range of hazardous scenarios. These can be read from the spread sheets:

- Slips & Trips Stf2;
- Flood Oth1;
- All other 'Other' codes OthX;
- Derailment DerX;
- Collisions ColX;
- Impacts ImpX;
- Entrapment EntX;
- Electrocution EleX.

The black columns on the left contain the breakdown.

3 Reference Documents

Ref:	Document Title	Document Number:
1.	Engineering Safety Hazard Management Procedure	CRL1-XRL-O8-GPD-CR001-50002
2.	CRL Technical Directorate - Engineering Safety Management – System Safety Plan	CRL1-XRL-O7-GST-CR001-00001
3.	CRL Technical Directorate - Engineering Safety Management - System Safety Plan Implementation Strategy	CRL1-XRL-O8-STP-CR001-50007
4.	CRL Technical Directorate - Engineering Safety Management - Hazard Management Procedure	CRL1-XRL-O8-GPD-CR001-50002
5.	CRL Technical Directorate - Crossrail Delivery Contracts Standard Engineering Safety Management Requirements Specification	CRL1-XRL-O8-GPD-CRG03-50001
6.	Project Works Information Volume 2B, Part 32, Contractors Engineering Safety Management Requirements (Systemwide)	CRL1-XRL-O8-XWI-CRG03-50002 (Appendix 1 to CRL1-XRL-O8-GPD-CRG03-50001)
7.	Contractors Engineering Safety Management Requirements (Stations, Shafts and Portals)	CRL1-XRL-O8-XWI-CRG03-50005 (Appendix 2 to CRL1-XRL-O8-GPD-CRG03-50001)
8.	Project Wide Hazard Record Process	CRL1-XRL-O8-GPS-CR001-50013
9.	Guidelines and Etiquette for Undertaking HAZID and HAZOP Workshops	CRL1-XRL-O8-GPS-CR001-50010
10.	Crossrail Process and Format for Product Breakdown Structures for Systems	CRL1-XRL-O8-GPS-CR001-50002
11.	Crossrail Common Safety Methods Hazard Assessment Process	CRL1-XRL-O8-GPS-CR001-50003
12.	Crossrail Format and Process for Engineering Safety Justifications for Systems	CRL1-XRL-O8-GPS-CR001-50004
13.	Crossrail FDC Assurance Stage Gate Engineering Safety Management Review Process	CRL1-XRL-O8-GPS-CR001-50005
14.	Crossrail Hazard Review Panel Terms of Reference	CRL1-XRL-O8-GPS-CR001-50009

Ref:	Document Title	Document Number:
15.	Crossrail Safety Issues File (SIF) and Action Tracker Report	CRL1-XRL-O8-LLG-CR001-50001
16.	Crossrail Process and Format for Comparative Risk Assessments	CRL1-XRL-O8-GPS-CR001-50007
17.	Crossrail Process and Format for Overall Safety Justifications	CRL1-XRL-O8-GPS-CR001-50012
18.	Design & Build Contract Assurance Stage Gate Engineering Safety Management Review Process	CRL1-XRL-O8-GPS-CR001-50014
19.	Crossrail Review and Approval of Contract Engineering Safety Management Deliverables	CRL1-XRL-O8-GPS-CR001-50015

4 Appendices

Appendix A - Fire Risk FR1

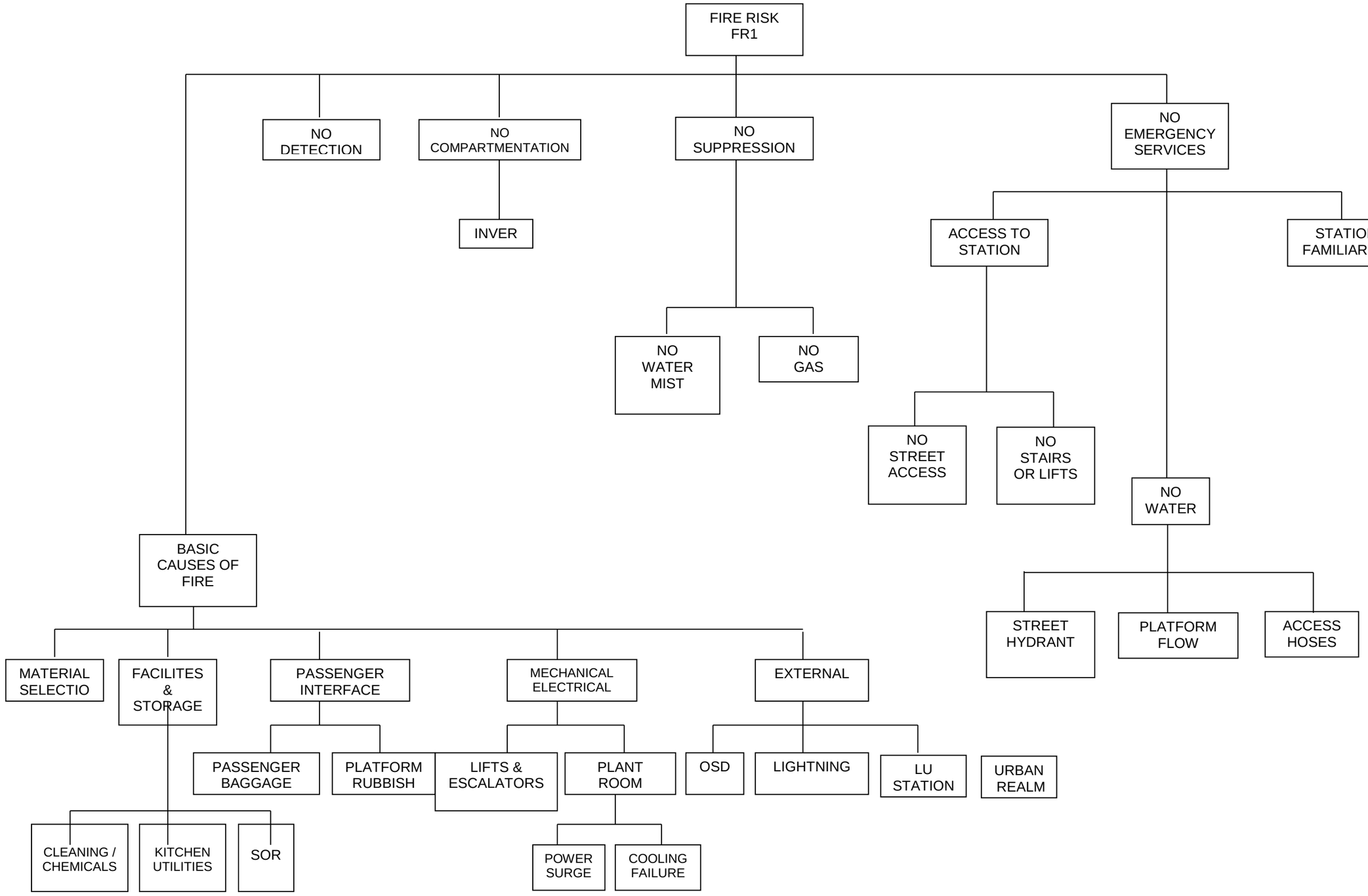
Appendix B - Smoke Risk FR2

Appendix C - Fall From Height Stf1

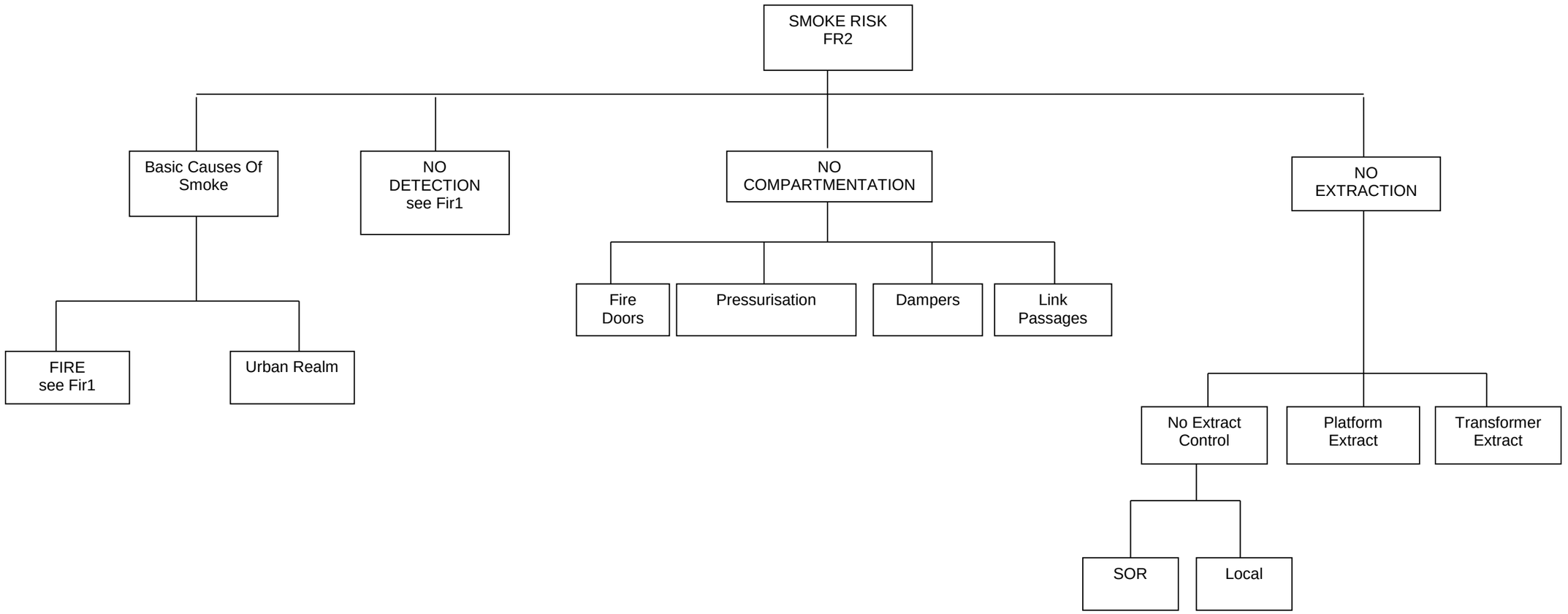
Appendix D - Evacuation Oth2

Appendix E - Congestion Risk Oth3

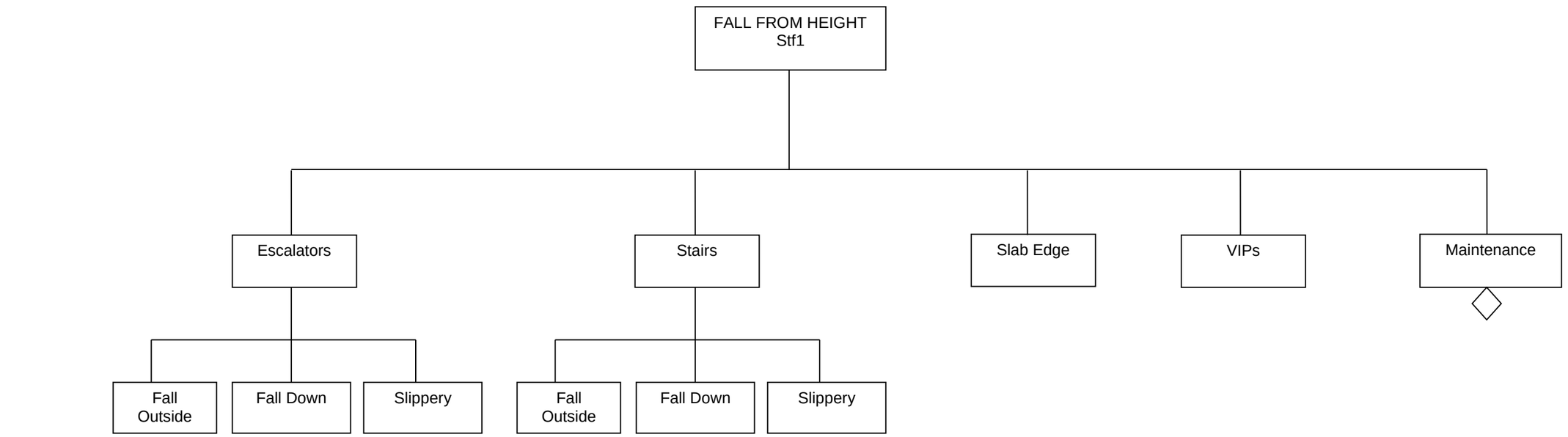
Appendix A - Fire Risk FR1



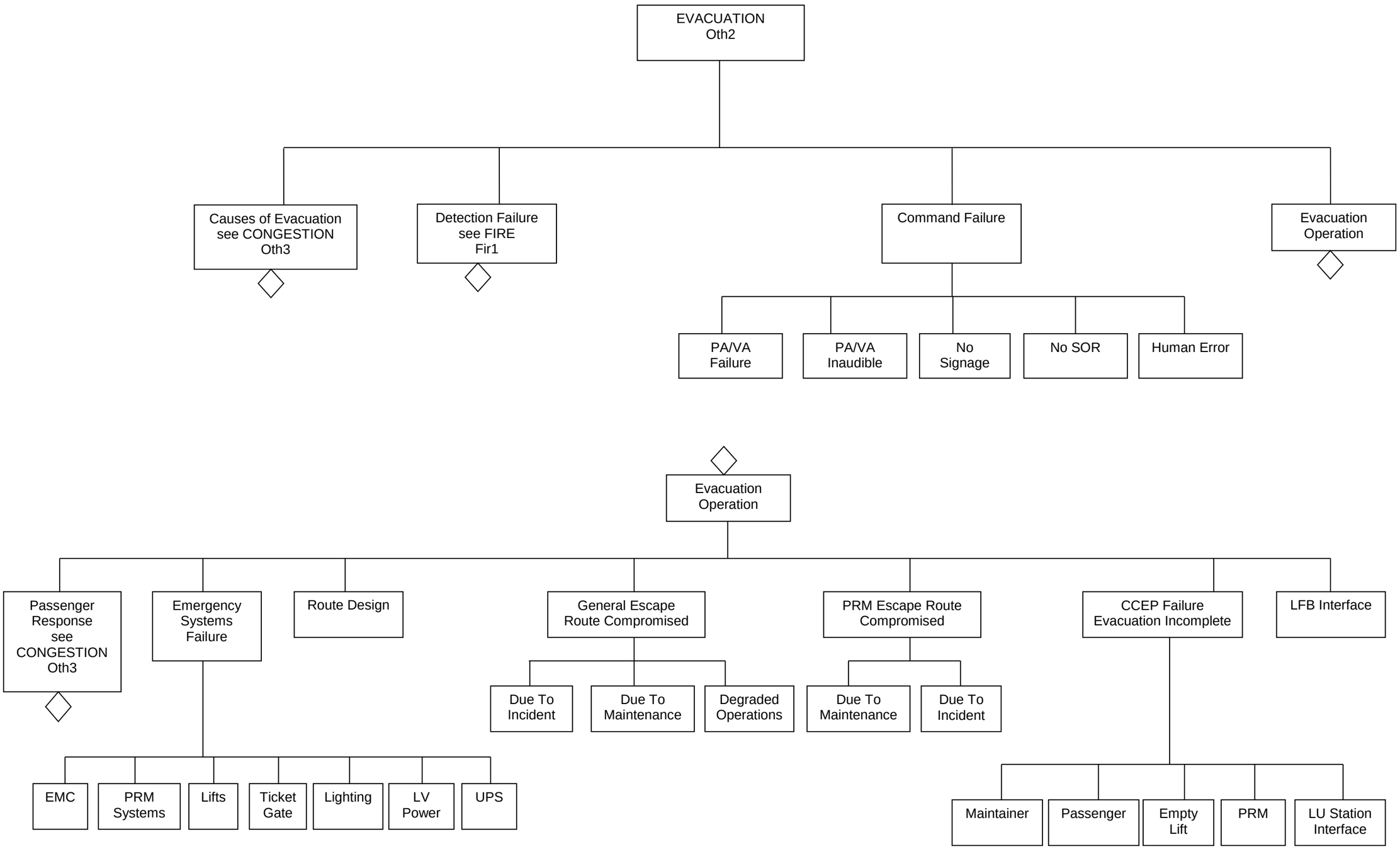
Appendix B - Smoke Risk FR2



Appendix C - Fall From Height Stf1



Appendix D - Evacuation Oth2



CRL RESTRICTED

Appendix E - Congestion Risk Oth3