Transit System Hazard Analyses – A Post Mortem

David Anderson, P.Eng

CH2M Hill, Senior Safety & Reliability Engineer

New York, New York

Topics

- Introduction
- Misapplication of Analyses
- Unclear Hazards
- Poor Risk Assessment
- Confusing hazards with mitigations
- Incorrect usage of Reliability Analysis
- Unrealistic/misunderstood numbers

Introduction

"Post Mortem" refers to an examination of the hazard analysis process and a presentation of how it met its demise.

We shall try to breathe some life into it.

Misapplication of Analyses

PHL – List of Hazards

PHA – General hazards/OHS

SSHA – Subcontractor's hazards

SHA – Integration of hazards

O&SHA – Hazards related to incorrect procedures

Misapplication of Analyses (cont'd)

Title	Performed by	Integrated by
Preliminary Hazard List	Contractor	Contractor
Preliminary Hazard Analysis	Contractor	Contractor
Subsystem Hazard Analysis	Sub-Contractor	Contractor
System Hazard Analysis	Contractor	Contractor
Operating & Support Hazard Analysis	Sub-Contractor	Contractor

Unclear Hazards

Most Hazards expressed in two fields; recommend using four.

Link to PHL and severity definitions.

Unclear Hazards (Cont'd)

Description	Condition/Cause	Mishap	Effect
Fewer fire extinguishers on board	Minimize vandalized or stolen equipment		Insufficient fire extinguishing capacity.
Fire	Floor heater operating temperature	Floor heaters ignite papers.	Death
Contact with live electrical components	Exposed high voltage		Possible electrocution
Electrocution	Maintenance on live electrical equipment.	Maintainer contacts live electrical equipment	Death

Poor Risk Assessment

Initial Risk		Hazard	Effect	Final Risk	
I	D	Doors cannot be opened.	Egress not possible, injuries / fatality.	IV	E
I	D	Equipment causes fire	Possible fire (injury or asphyxiation).	III	E
I	C	Passengers trapped in vehicle in emergency	Passengers injured/die.	III	E

Severity should not change.
Multiple effects undesirable.
Effect should match severity.

Confusing hazards with mitigations

Cause	Mitigation
Maintenance procedures not followed. Lack of personnel training.	Appropriate personnel training. Follow maintenance procedure .
Incorrect design of equipment EMI filtering.	Electronics designed and tested in accordance to standards.
Inappropriate design, missing warning, maintenance procedures not followed.	Maintenance procedures will document the correct methods to remove and replace equipment items and will provide warnings where applicable.

Maintenance, design and training are mitigations.
Non-existence or incorrect does not make them a hazard.
Results in circular logic.

Incorrect Usage of Reliability Analyses

FMECA is not a hazard analysis.

Examines one failure at a time, the occurrence of a single failure seldom results in a hazard.

FTA requires detailed knowledge of the system and quantitative data.

Combination is difficult, but beneficial.

Unrealistic or Misunderstood Data

- Frequency targets often expressed as Probability – 10^{-9}.
- Data sometimes does not exist or is not revealing.
- The meaning behind numbers must be understood.

What Numbers Mean

n	X^{-n}	Hours	Time/yrs
0	1	1	
1	0.1	10	
2	0.01	100	4 days
3	0.001	1000	1.5 months
4	0.0001	10000	1.14
5	0.00001	100000	11.4
6	0.000001	1000000	114
7	0.0000001	10000000	1,140
8	1E-08	100000000	11,400
9	***1E-09***	***1E+09***	***114,000***
10	1.00E-10	1.00E+10	1,140,000
11	1.00E-11	1.00E+11	11,400,000
12	1.00E-12	1.00E+12	114,000,000
13	1.00E-13	1.00E+13	1.14E+09
14	1.00E-14	1.00E+14	**1.14E+10**

What Numbers Mean (Cont'd)

Examples from a Fault Tree Analysis.

Event	Probability	Time in Years
Both headlights failed	1^{-16}	A long time
Operator doesn't honk horn	1^{-12}	100 Million
Worn out flooring	1^{-8}	11,000
Wiper blade failed	1^{-6}	30

Conclusion

- Hazards form the basis of the safety case.
- Main issues include application and clarity.
- General understanding of probability is required.
- Thank you.

Questions

?