

Engineering Disasters and Learning from Failure

Presentation

Karl Ray

Colorado Springs, Colorado

© July 2010

Overview

- Notable failures
- Learning from failure
- Failure definitions
- Applicability
- Causes of failures
- Failure analysis process
- Conclusion
- Resources

Notable Failures



- Challenger
- Columbia
- Chelyabinsk (Mayak atomic weapons complex)
- Three Mile Island
- Chernobyl
- Tacoma Narrows Bridge
- Hyatt Regency Skywalk

Learning from Failures

"People don't surrender their mental models easily. They may puzzle over contradictory evidence, but usually succeed in pushing it aside--until they come across a piece of evidence too fascinating to ignore, too clear to misperceive, too painful to deny, which makes vivid still other signals they do not want to see, forcing them to alter and surrender the world-view they have so meticulously constructed."

Vaughan, D., *The Challenger Launch Decision*, ISBN 978-0226851754

Learning from Failures - 2

"Thus the colossal disasters that do occur are ultimately failures of design, but the lessons learned from those disasters can do more to advance engineering knowledge than all the successful machines and structures in the world."

Source: Petroski, H., *To Engineer Is Human, The Role of Failure in Successful Design*, ISBN 0-679-73416-3

Why Analyze Failures?

- Increase knowledge
- Improve development processes
- Reduce maintenance costs
 - chronic failures are responsible for 80% of maintenance budgets
 - one RCFA analysis in Kalinaukas' Union Camp paper mill, saved the company \$1,021,000 in production losses
- Improve reliability of future developments

Source: LePree, J., *Root Cause Failure Analysis*, retrieved from:

<http://www.maintenanceresources.com/ReferenceLibrary/FailureAnalysis/RCFA2article.htm>

Failure Mode Definitions

- Category I—Catastrophic—A failure that may cause injury or death.
- Category II—Critical—A failure which may cause severe injury, major property damage, or major system damage that will result in major downtime or production loss.
- Category III—Marginal—A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of system availability or degradation.
- Category IV—Minor—A failure not serious enough to cause injury, property damage or system damage, but will result in unscheduled maintenance or repair.

Applicability

- Failure analysis is applicable to all engineering disciplines!
 - Aircraft/Aerospace
 - Mechanical
 - Electrical
 - Civil
 - Software

Causes of Failures

- Human factors (ethical failures and accidents)
- Design flaws (often caused by ethical failures)
- Materials failures
- Extreme conditions or environments
- Combinations of these reasons

Causes of Failures Attributable to Engineering

From an analysis of 800 structural failures conducted by the Swiss Federal Institute of Technology. When engineers were at fault, causes of failures were:

- Insufficient knowledge 36%
- Underestimation of influence 16%
- Ignorance, carelessness, negligence 14%
- Forgetfulness, error 13%
- Relying upon others without sufficient control . 9%
- Objectively unknown situation 7%
- Unprecise definition of responsibilities 1%
- Sicherheitsprobleme bei Bauwerken (Braschiert), ISBN: 978-3764308582. 1%

Source: Matousek, M. and Schneider, J., *Untersuchungen zur Struktur des*

Root Cause Failure Analysis

- Describe the failure event
- Describe the failure modes
- Hypothesize
- Verify the hypotheses
- Determine physical roots & verify
- Determine latent roots & verify

Forensic Engineering Process

- Background investigation
- Sample and evidence collection
- Field investigation
- Laboratory and computer analysis
- Report generation
- Presentation of findings

Conclusion

- Performing failure analysis is important for all engineering disciplines
- Lessons learned from failure analysis can be:
 - Used to prevent similar failures in similar articles
 - Used to improve development processes
 - Further engineering knowledge
 - Used to reduce ongoing maintenance costs

Resources

- University of Plymouth, Interactive Tutorials on "Learning from Failure"
http://www.tech.plym.ac.uk/sme/Interactive_Resources
- Plant Engineering, Maintenance, and Reliability Reference Library
<http://www.maintenanceresources.com/ReferenceLibra>
- Carvey, H., Windows Forensics and Incident Recovery, ISBN 0-321-20098-5
- The Journal of Engineering Failure Analysis,
http://www.elsevier.com/wps/find/journaldescription.cws_home/30190/description