LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

e-maintenance vulnerability and other maintenance risk aspects

Per Anders Akersten
Adjunct Professor
Risk & Reliability Management

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Division of Operation and Maintenance Engineering

Luleå Railway Research Center

Center for Dependability and Maintenance (Center for Maintenance and Industrial Services)

Outline of talk

- ***Maintenance and risks***
- ***Risk and vulnerability concepts***
- ***The e-maintenance concept***
- ***General threats***
- ***An analysis approach***

Are there any maintenance-related risks?

The lack of maintenance can lead to a hazardous degrading production system. The chemical release and fire at the Associated Octel Company Limited, Ellesmere Port, Cheshire in 1994 was most likely caused by overseen preventive maintenance actions which led to the failure of a corroded securing flange between the fixed pipeline and the discharge port of a pump that circulates highly flammable liquids (HSE).

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Are there any maintenance-related risks?

A major disaster occurred at the end of October 1989 at Philips petrochemical plant in Pasadena, Texas. A heavy explosion of two iso-butane tanks resulted in the death of 23 employees and another 130 employees were injured. Maintenance work was performed incorrectly on a pipe section. The isolation valve, which is used to seal off the flammable liquid, was not used properly. Because of the similarity of the air connections, the maintenance personnel mixed up the air connections and opened the valve fully instead of closing it before the maintenance actions were conducted, which led to a major gas leakage. The accident was caused by human-error of the maintenance personnel due to improper system design (Khan & Abbasi, 1999).

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Are there any maintenance-related risks?

An example of insufficient maintenance followed by a conscious rule violation by the production personnel is the Siberian accident which occurred in 1989 near Nizhnevartovsk. The pipeline pressure dropped, due to a leakage in the pipeline system. The Engineers did not investigate the trouble; instead they increased the pumping rate to maintain the system pressure. The leakage caused a huge cloud of highly flammable liquefied gas. ***(continued..)***

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Are there any maintenance-related risks?

The smell of gas was reported by the valley settlements in the area, but still no actions were taken to investigate the problem. Two trams were passing by the gas filled area and it was probably the brakes of one of the train that ignited the cloud of gas. 462 persons were killed in the accident and another 796 were hospitalised with grave burn wounds (Khan & Abbasi, 1999).

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Are there any maintenance-related risks?

The effect of maintenance actions are not necessarily detected during the maintenance phase, in some cases the effect of the impropriate actions taken to ensure safety and reliability of the system can appear in the start up phase of the equipment. The Piper Alpha accident in 1988 was caused by maintenance actions and the plant failed dangerously at start up which resulted in the death of 165 peoples and substantial economical losses (Hale et. al, 1998).

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

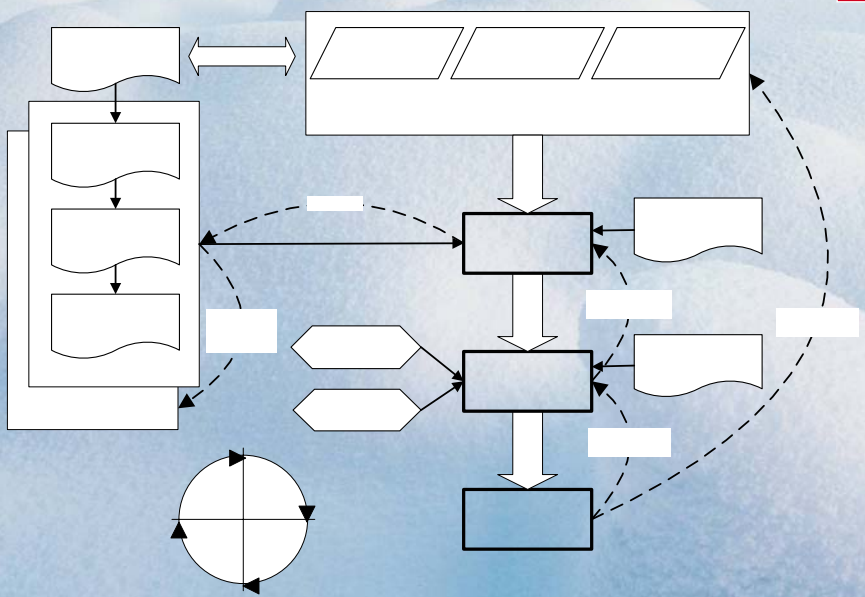
Maintenance-related risks do exist

- *in the maintenance planning phase*
- *in the maintenance execution phase*
- *in the functional testing phase*
- *in the use of data, information & knowledge*

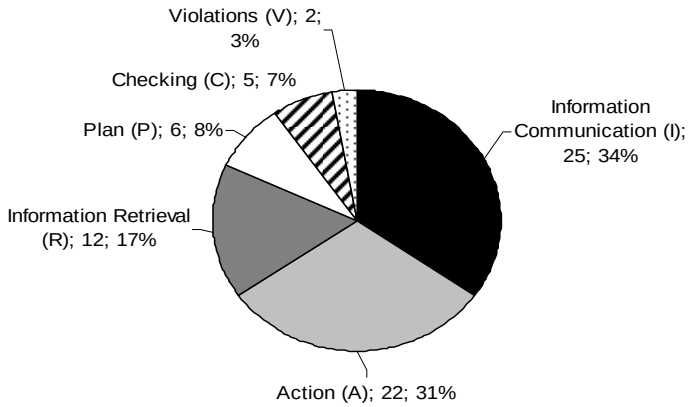
Moreover:

- *during maintenance, the system under study is more vulnerable*
- *human errors, unintentional as well as intentional, do occur*

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering



Classification of Human Failures



Classification of human failures causing maintenance-related incidents and accidents within Swedish railway 1988 - 2000.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Risk components

A) Source

- ***Hazards***
- ***Opportunities***
- ***Uncertainties***

B) Object of harm

- ***Vulnerabilities***
- ***Possible consequences***
- ***Uncertainties***

Dependability attributes

- availability, i.e. readiness for service
- reliability, i.e. continuity of service
- safety, i.e. absence of adverse consequences
- integrity, i.e. absence of improper system alterations
- maintainability, i.e. ability to perform repairs/modification

The vulnerability concept

"susceptibility to injury or attack"
(no standard definition available yet)

A characterization a system's lack of resilience with respect to different threats that may cause loss of availability, integrity or confidentiality.

Threats, examples

- *natural disaster or other phenomenon*
- *failure of a system element*
- *faulty system state*
- *unintentional act by an individual*
- *malicious act by an individual or a group*

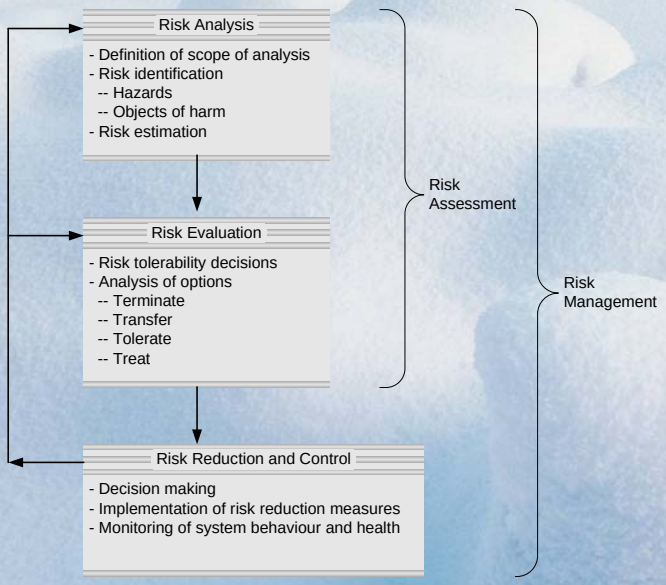
Attack

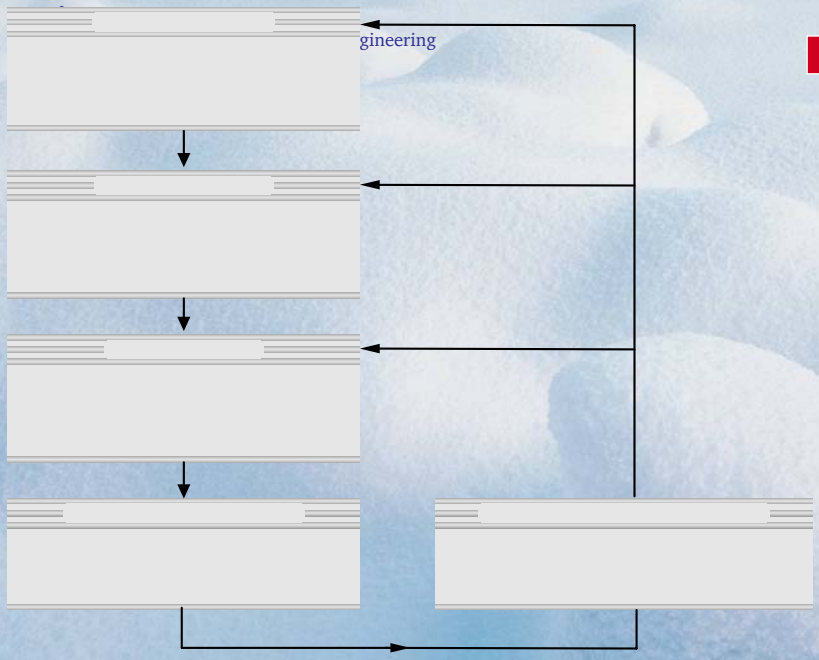
The presence of a threat, attempting to exploit vulnerability

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Risk/attack components

A) Source	*B) Object of harm*
Hazards	*Vulnerabilities*
Threats	*Possible consequences*
Opportunities	*Uncertainties*
Uncertainties	


Risk Analysis
- Definition of scope of analysis
- Risk identification
-- Hazards
-- Objects of harm
- Risk estimation
Risk Evaluation
- Risk tolerability decisions
- Analysis of options
-- Terminate
-- Transfer
-- Tolerate
-- Treat
Risk Reduction and Control
- Decision making
- Implementation of risk reduction measures
- Monitoring of system behaviour and health
Risk Assessment
Risk Management



Inductive/Deductive Methods

Inductive methods, e.g. Failure Mode and Effects Analysis (FMEA), determine what system states are possible.

Deductive methods, e.g. Fault Tree Analysis (FTA), determine how a given system state can occur.

Inductive risk analysis methods ...

... go from fault or failure mode, through system failure, to effects w.r.t. safety, environment and property

... consider primarily only one fault or failure mode at a time

... are straightforward, fairly simple to apply

Deductive risk analysis methods ...

- *... go from specified failure effects, through fault or failure modes, to failure mechanisms*
- *... consider primarily only one specified failure effect at a time*
- *... use logical reasoning and pose high demands on the analyst*

From RM to e-

e-service

teleservice

telematics

e-manufacturing

e-maintenance

e-health

e-medicine

telemedicine

...

e-maintenance definition (Koc & Lee, 2005)

"Intelligent Maintenance System (IMS) is an internet-based and web-enabled predictive maintenance technology which consists of intelligent machine degradation assessment, e-prognostics, and e-diagnostics .....

Remote and real time assessment of machine's performance information requires an integration of many different technologies including sensory devices, reasoning agents, wireless communication, virtual integration and interface platforms."

Some related activites at Luleå University

- Systems Science
  - sensor system development
  - web-enabled services
  - human health monitoring applications
  - ”Future Wireless Mine”
- Operation & Maintenance Engineering
  - requirements management
  - product support, including
    - support to client
    - support to physical product
  - information extraction from large datasets
  - aerospace applications

e-maintenance system functions

- real-time monitoring of machine behaviour and health
- fault diagnostics
- machine performance degradation assessment and prognostics
- data collection
- information sharing
- exchange of information
- extraction of information, data mining
- decision support
- ...

CC-PKB general threats

[Common Criteria (ISO 15408) Profiling Knowledge Base]

1. Administrative errors of commission
2. Administrative errors of omission
3. Hostile administrator modification of user or system data
4. Administrator violates user privacy policy
5. A critical system component fails
6. Software containing security-related flaws
7. Failure of a distributed system component
8. Hacker undetected system access
9. Hacker attempts resource denial of service
10. Hacker eavesdrops on user data communications
11. Cryptanalysis for theft of information
12. Hacker masquerading as a legitimate user or as system process
13. Message content modification
14. Exploitation of vulnerabilities in the physical environment of the system
15. Social engineering
16. Malicious code exploitation
17. Unexpected disruption of system or component power
18. Recipient denies receiving information
19. Sender denies receiving information
20. A participent denies receiving information
21. Legitimate system services are spoofed
22. Hostile user acts cause confidentiality breaches
23. User abuses authorization to collect data
24. User errors cause confidentiality breaches
25. User error makes data inaccessible
26. User errors cause integrity breaches
27. User errors undermine the system's security features
28. User's misuse causes denial of service
29. User abuses authorization to modify data
30. User abuses authorization to send data

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

CC-PKB general threats 1-9

1. Administrative errors of commission
2. Administrative errors of omission
3. Hostile administrator modification of user or system data
4. Administrator violates user privacy policy
5. A critical system component fails
6. Software containing security-related flaws
7. Failure of a distributed system component
8. Hacker undetected system access
9. Hacker attempts resource denial of service

CC-PKB general threats 10-16

10. Hacker eavesdrops on user data communications
11. Cryptanalysis for theft of information
12. Hacker masquerading as a legitimate user or as system process
13. Message content modification
14. Exploitation of vulnerabilities in the physical environment of the system
15. Social engineering
16. Malicious code exploitation

CC-PKB general threats 17-25

17. Unexpected disruption of system or component power
18. Recipient denies receiving information
19. Sender denies receiving information
20. A participent denies receiving information
21. Legitimate system services are spoofed
22. Hostile user acts cause confidentiality breaches
23. User abuses authorization to collect data
24. User errors cause confidentiality breaches
25. User error makes data inaccessible

CC-PKB general threats 26-30

26. User errors cause integrity breaches
27. User errors undermine the system's security features
28. User's misuse causes denial of service
29. User abuses authorization to modify data
30. User abuses authorization to send data

e-maintenance system functions

- real-time monitoring of machine behaviour and health
- fault diagnostics
- machine performance degradation assessment and prognostics
- data collection
- information sharing
- exchange of information
- extraction of information, data mining
- decision support
- …

CC-PKB general threats

1. Administrative errors of commission
2. Administrative errors of omission
3. Hostile administrator modification of user or system data
4. Administrator violates user privacy policy
5. A critical system component fails
6. Software containing security-related flaws
7. Failure of a distributed system component
8. Hacker undetected system access
9. Hacker attempts resource denial of service
10. Hacker eavesdrops on user data communications
11. Cryptanalysis for theft of information
12. Hacker masquerading as a legitimate user or as system process
13. Message content modification
14. Exploitation of vulnerabilities in the physical environment of the system
15. Social engineering
16. Malicious code exploitation
17. Unexpected disruption of system or component power
18. Recipient denies receiving information
19. Sender denies receiving information
20. A participent denies receiving information
21. Legitimate system services are spoofed
22. Hostile user acts cause confidentiality breaches
23. User abuses authorization to collect data
24. User errors cause confidentiality breaches
25. User error makes data inaccessible
26. User errors cause integrity breaches
27. User errors undermine the system's security features
28. User's misuse causes denial of service
29. User abuses authorization to modify data
30. User abuses authorization to send data

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

Analysis components

Causes	There are many threats that can directly affect the system or system element under study.
Barriers (probability reduction)	Some threats may attack the barriers, safeguards or safety functions, intended to reduce the probability of an incident.
Incidents	The incident is any event, resulting from an attack.
Barriers (mitigation)	In order to mitigate the impacts of an incident, barriers, safeguards or safety functions are often introduced. They, too, may be subject to threats.
Impacts	An attack may have impact directly on the system under study, on the persons involved and on the physical and business environments.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

The importance of barriers

The risk analysis must include the identification of barriers and possible threats to the barrier functions.

System functions and related barriers may be affected by common cause failures or attacks, not only malicious attacks, performed by a well-informed agent.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	**Threat / deviation**	**Barrier to incident**	**Threat to barrier**	**Incident**	**Barrier to impact**	**Threat to barrier**	**Resulting impact**

The starting point is a compilation of identified system or system element requirements, primarily functional requirements.

Using the guide-words or list of general threats, deviations from or threats to the requirement under study are identified.

Barriers or safety functions, reducing the probability of the threat or deviation leading to an incident, are identified.

Threats that can jeopardize the function of the barrier are identified.

Identification of incidents, resulting from the threat. An incident is defined as an adverse event or state, causing damage to health, safety, availability, or physical/business environment.

Barriers or safety functions, mitigating the impacts of the incident, are identifed.

Threats that can jeopardize the function of the barrier are identified.

Resulting impacts on health, safety, availability or physical/business environment, are identified.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	**Threat / deviation**	**Barrier to incident**	**Threat to barrier**	**Incident**	**Barrier to impact**	**Threat to barrier**	**Resulting impact**

The starting point is a compilation of identified system or system element requirements, primarily functional requirements.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Using the guide-words or list of general threats, deviations from or threats to the requirement under study are identified.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Barriers or safety functions, reducing the probability of the threat or deviation leading to an incident, are identified.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Threats that can jeopardize the function of the barrier are identified.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Identification of possible incidents, resulting from the threat. An incident is defined as an adverse event or state, causing damage to health, safety, availability, or physical/ business environment.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Barriers or safety functions, mitigating the impacts of the incident, are identifed.

LULEÅ UNIVERSITY OF TECHNOLOGY
Division of Operation and Maintenance Engineering

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Threats that can jeopardize the function of the barrier are identified.

A simple analysis approach

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

Resulting impacts on health, safety, availability or physical/business environment, are identified and evaluated.

Tools used

FMEA-sheet		Object:					
Function / requirement	Threat / deviation	Barrier to incident	Threat to barrier	Incident	Barrier to impact	Threat to barrier	Resulting impact

- ***FMEA-sheet, providing a structure***
- ***Requirements and functions elicitation***
- ***Threat categories list/Guidewords***
- ***Barrier analysis***
- ***Event trees/attack trees, describing possible attacks, active barrier functions and resulting impacts***

Conclusions

Risks and vulnerabilities related to the utilization of e-services have been identified as an important area for research. In this presentation the concepts of risk and vulnerability in relation to e-maintenance have been briefly described. Some well-known methodologies and tools for the management of vulnerability are combined into a proposed simple analysis methodology.

The paper represents the view of a risk analyst and reliability engineer, not directly involved in the development of e-maintenance systems or tools.

References

- Avizienis, A., Laprie, J.-C., Randell, B. & Landwehr, C. (2002). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11-33
- Hale, A.R, et al. (1998). Evaluating safety in the management of maintenance activities in the chemical process industry. Safety Science, 28, 21-44.
- HSE (Health and Safety Executive) (1989). Dangerous Maintenance. London: HMSQ.
- Khan, F. & Abbasi, S.A. (1999). Major accidents in process industries and an analysis of causes and consequences. Journal of Loss Prevention in the Process Industries, 12, 361-378.
- Koç, M., Ni, J., Lee, J., & Bandyopadhyay, P. (2005). Introduction to e-Manufacturing. In: R. Zurawski (Ed.) *Industrial Information Technology Handbook*, Boca Raton: CRC Press, Chapter 97.
- Lee, J. (1998). Teleservice engineering in manufacturing: challenges and opportunities. *International Journal of Machine Tools & Manufacture*, 38, 901-910.
- Stamatis, D.H. (1995). *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. Milwaukee: ASQ.
- Stephenson, P. (2004). Applying impact and vulnerability analysis to risk management. *Computer Fraud and Security*, Issue 2, 16-20.