

Comparison of Hazard Analysis Methods Using a Data Center Example

Muhammad Fahadullah Muhammad Farhan Khan
Email: {muhfa044,muhkh108}@student.liu.se
Supervisor: Almut Herzog, {almhe@ida.liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

Data centers contain the most valuable assets for any organization for its IT operations; especially where the business relies on the information systems and the business continuity is associated with IT. Since data centers occupy large spaces, there exist various risks which concerns information security. Therefore a secure environment is required to reduce the chances of a security breach. Furthermore, any sort of failure within the system effects business operation which leads to loss of revenue.

We have identified fifteen possible case scenarios as hazards and select one of them for analyzing through two methods of hazard analysis: Hazard and Operability Analysis (HAZOP) and Fault Tree Analysis (FTA). Comparison is done for the results of both the methods and our findings are then described. We chose HAZOP because with this method we can check the safety of a design, decide whether and where to build, develop a list of questions to ask a supplier, check operating/safety procedures, improve the safety of an existing facility, and verify that safety instrumentation is reacting to best parameters. Above all, HAZOP can be used practically at any stage. HAZOP methodology is so widely used that almost any process hazard analysis (PHA) is referred to as a HAZOP [1]. We select the other method as FTA because it can be used to help identify root causes of trouble and to design remedies and countermeasures.

1. Introduction

A facility or room dedicated to accommodate mission critical computer systems and core IT infrastructure for companies and organization is known as data center. These components are typically telecommunications and storage systems, redundant or backup power supplies, data communications connections and high security appliances, environmental controls (e.g. air-conditioning, fire suppression) etc.

A data center is the heartbeat of any organization, especially when the business is IT driven. To effectively create, collaborate, and interact, the data center is the main resource on which the employees, partners, and customers rely on. With the rise of internet and web-based technologies over the last decade with improving productivity, accelerating, and enhancing business process, data centers have become the strategic focus of IT efforts to protect, optimize, and grow the business. Regardless of how many computing devices are dispersed into the organization, a centralized data center is always a need for large corporate organizations [2].

Identifying possible risks and hazards is essential to remain aware of the lacking features which could lead to disastrous situations and resulting in huge losses to the business. With hazard analysis and the comparison with its different methods, we have come up with better security measures for the system, and as well as better method to adopt.

In this report, we identify some physical security risks which could harm valuable data center assets leading ultimately to huge losses to the business. This analysis also helps to determine typical environmental services required to maintain suitable operating conditions for the data center systems.



Figure 1 – A typical data center

2. The System

HAZOP can be performed only on systems, not for organizations. Therefore, the system we choose for the project is a data center of The Resource Group (www.trgcustomersolutions.com). TRG is a US based organization with its business aimed in off-shoring its operations around the world and it has the largest business process outsourcing (BPO) operations in Pakistan, Senegal, and Philippines. The main offshore facility at Karachi is a major call center running 24/7. Therefore, the IT backbone needs to be up all the time to keep the business running.

The data center is a medium sized structure consisting of six total racks, two for network devices, two for system servers, one for voice-over-IP servers, and one for data storage devices. The network racks contain several routers, primary and secondary PIX firewalls, core switch, Ethernet switches, and satellite receivers. Systems server racks contain primary and secondary mail servers, primary and secondary DNS, web server and FTP. The voice-over-IP servers consist of Asterisk being used as primarily and Zultys exchange as secondary. The storage rack contains backup media servers and devices.

Other than the typical racks, the data center is equipped with air-conditioning system to maintain a certain temperature. There are 3-4 AC units installed to be working alternatively in different time spans. An electronic temperature gauge monitors the room temperature and maintains a log. Smoke detector senses any kind of smoke and sends signal to alarm system in case of any fire. A fire extinguisher is present for initial treatment. Network cables are passing through some paths and all the cables all together going in/out through a single channel. The electric power supply is coming through a UPS system which is outside the data center room. Access control is done by a magnetic card reader connected to an automatic lock installed at the only entrance to the room, which allows entering only authorized personnel.

Below are 15 of the most common signs that the data center is at a security risk [3]:

- i. Out-of-date physical wiring diagrams
- ii. Out-of-date logical equipment configuration diagrams and schematics
- iii. Infrequent testing of UPS
- iv. Failure to recharge UPS batteries
- v. Failure to test generator and fuel levels
- vi. Lack of preventive maintenance on air conditioning equipment
- vii. Annunciator system not tested

- viii. Fire suppression system not recharged
- ix. Emergency power-off system not tested
- x. Emergency power-off system not documented
- xi. Infrequent testing of backup generator system
- xii. Equipment not properly anchored
- xiii. Evacuation procedures not clearly documented
- xiv. Circumvention of physical security procedures
- xv. Lack of effective training for appropriate personnel

3. Hazard Analysis

A Hazard is a potential or existing condition that may cause harm to people or damage to property or the environment [4].

The hazards associated with any facility that produces or uses chemicals can be quite numerous, perhaps in the hundreds or thousands for larger facilities. These hazards are the result of the physical properties of the materials, the operating conditions, the procedures, or the design, to name a few. Most of the hazards are continually present in a facility [9].

Without proper control of hazards, a sequence of events (scenario) occurs that results in an accident. A hazard is defined as anything that could result in an accident, i.e. an unplanned sequence of events which results in injury or loss of life, damage to the environment, loss of capital equipment, or loss of production or inventory [9].

Risk consists of two components: the probability of the accident and the consequence. It is not possible to completely characterize risk without both of these components. Thus, a hazard could have low probability of accident but high consequence or vice versa. The result for both cases may be moderate risk. The purpose of hazard analysis and risk assessment in the chemical process industry is to (1) characterize the hazards associated with a chemical facility; (2) determine how these hazards can result in an accident, and (3) determine the risk, i.e. the probability and the consequence of these hazards. The complete procedure is shown in Figure 2 [9].

There are several methods available for performing the hazard analysis. The most common types are Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). The hazard and operability analysis (HAZOP) procedure is popular because of its ease of use, the ability to organize and structure the information, reduced dependence on the experience of the analysts, and the high level of results [5].

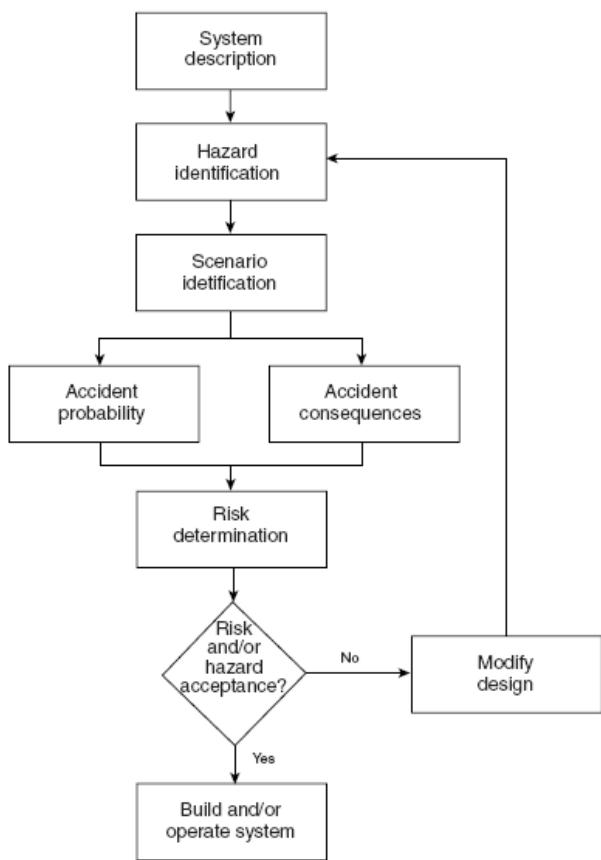


Figure 2 – Flowchart representing the complete hazard analysis and risk assessment procedure [9].

3.1 HAZOP

A Hazard and Operability (HAZOP) study is a structured and systematic examination of a planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment, or prevent efficient operation. The HAZOP technique was initially developed to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems. A HAZOP is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team (HAZOP team) during a set of meetings [6].

The HAZOP study should preferably be carried out as early in the design phase as possible - to have influence on the design. On the other hand; to carry out a HAZOP we need a rather complete design. As a compromise, the HAZOP is usually carried out as a final check when the detailed design has been completed. A HAZOP study may also be conducted on an existing facility to identify

modifications that should be implemented to reduce risk and operability problems [6].

HAZOP studies may also be used more extensively, including [6]:

- At the initial concept stage when design drawings are available
- When the final piping and instrumentation diagrams (P&ID) are available
- During construction and installation to ensure that recommendations are implemented
- During commissioning
- During operation to ensure that plant emergency and operating procedures are regularly reviewed and updated as required

The results of the HAZOP analysis are the team's recommendations, which include identification of hazards and the recommendations for changes in design, procedures, etc. to improve the safety of the system. Deviations during normal, startup, shutdown, and maintenance operations are discussed by the team and are included in the HAZOP. A block flow diagram of the HAZOP process is shown below in figure 3.

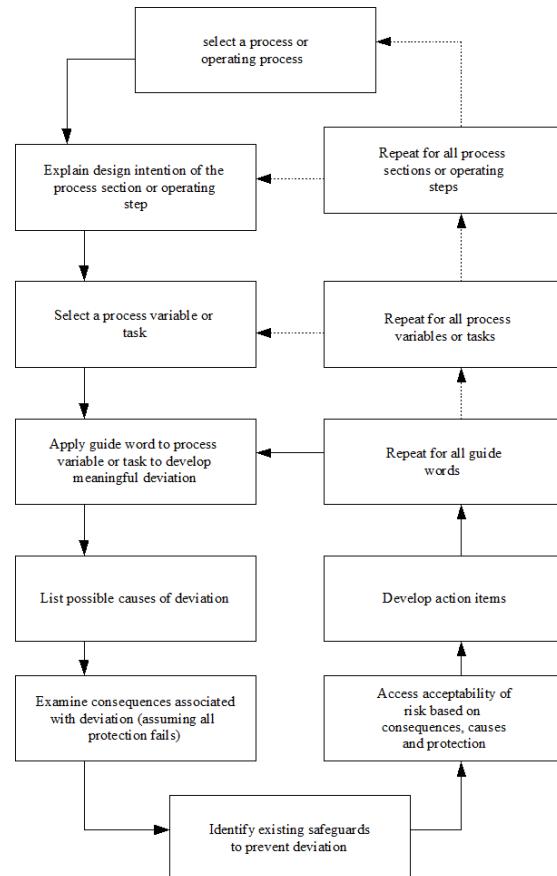


Figure 3 – HAZOP flow diagram [7].

3.2 Fault Tree Analysis

Fault tree analysis is a graphical representation of the major faults or critical failures associated with a product, the causes for the faults, and potential countermeasures. The tool helps identify areas of concern for new product design or for improvement of existing products. It also helps identify corrective actions to correct or mitigate problems [8].

Fault tree analysis is useful both in designing new products/services and in dealing with identified problems in existing products/services. In the quality planning process, the analysis can be used to optimize process features and goals and to design for critical factors and human error. As part of process improvement, it can be used to help identify root causes of trouble and to design remedies and countermeasures [8].

Following is the FTA procedure [8]:

- Select a component for analysis: Draw a box at the top of the diagram and list the component inside.
- Identify critical failures or “faults” related to the component: Using Failure Mode and Effect Analysis is a good way to identify faults during quality planning. For quality improvement, faults may be identified through Brainstorming or as the output of Cause and Effect Analysis.
- Identify causes for each fault: List all applicable causes for faults in ovals below the fault. Connect the ovals to the appropriate fault box.
- Work toward a root cause: Continue identifying causes for each fault until you reach a root or controllable cause.
- Identify countermeasures for each root cause: Use Brainstorming or a modified version of Force Field Analysis to develop actions to counteract the root cause of each critical failure. Create boxes for each countermeasure, draw the boxes below the appropriate root cause, and link the countermeasure and cause.

4. Analysis

The analysis using both the selected methods is as follows.

4.1 HAZOP Analysis for air-conditioning system failure

Following is the HAZOP analysis for some situations for our data center as shown in figure 1 (appendix). The selected risk is “Air-Conditioning failure” for all causes. We have selected this use-case because in order to keep the room cool and control humidity, air-conditioning system must be fully functional. Keeping the equipment at the board level within the temperature/humidity range specified by the manufacturer is the primary goal of the air-conditioning system. The electronic equipment will tend to malfunction if it is placed in a confined space generating excess amount of heat.

There are four deviation levels we have selected for the analysis: critical, high, medium, and low. There exist three guided words for temperature: “More” for high temperatures, “Part of” and “Less” for low temperatures depending on how critical the problem is. In our case the temperature is high due to air-conditioning failure, therefore we will consider “More” as the guide word for “high temperature” as the deviation, “Part of” for “irregular temperature”, and “Less” for situation when “temperature starts rising up”. But it is differentiated in terms of critical, high, medium, and low. Since in our case, we are considering problem with the air-condition unit, so the temperature are assumed to go higher and there is no existence for the “Less” deviation.

We start with the critical levels. In the first scenario, the core router is shut down due to high humidity and temperature. It is treated as the most critical condition because it will cause loss of connectivity to external networks as a consequence. The safeguard and immediate action is described as watching the temperature log frequently and incase of the incident restore the normal operating temperature. The next critical level is with the operation of the core switch. If the core switch goes down due to abnormal temperature conditions, the internal connectivity is affected. The same procedure is then followed for safeguard and action as with the core router. The third critical level is taken as a problem with the Asterisk server which will disrupt all the telephony within the organization causing every employee to be unable to communicate over the phone. As a safeguard it is first made sure that the server is well placed nearby to the cooling system and proper ventilation is provided. An internal alert system within the server which generates error logs in case of any errors or unexpected shut downs is also required. As a secondary voip server (Zultys Exchange) is available so therefore automatic switching mechanism needs to be developed. Action to couple up with the issue is to restore the normal operating temperature and afterwards starting over the server,

running the diagnosing tools to ensure all services working correctly before the server goes live again.

The next deviation level is named as ‘High Level’. The first scenario is examined with the satellite receiver device which is sensing high temperature and buzzing alarm to alert before it shuts down. In this case it is recommended to make an immediate switch over to the secondary link which might be a bit slower than primary but it will keep the operations running. In the meantime, operating temperature must be restored to normal conditions and make a switch back to primary receiver. The second example for high level deviation is taken as shutting down of storage media server. It will disconnect all network shared drives for everyone having his data on the server. The safeguard would be having the data replicated with the backup storage server more frequently. With the switch over to the secondary server, the users should also be informed about the failure. Restoring back the primary server, a complete diagnosis is to be done to make sure no data is lost during the failure. Inform back the users when the network shared drives are up.

We have taken the example of PIX firewall on the medium level of deviation. It is a Cisco PIX firewall which starts malfunctioning, in fact it stops giving response when the operating temperature is not normal. This will block the allowed traffic as well and also may cause some network services to stop, for example VPN connections, internet traffic, hosted web services, email etc. A necessary safeguard is to have a secondary firewall installed. The immediate action for this case is to reboot the device and call up the electric department to check out the air-conditioning system.

When the temperature starts rising up, the internal fans of heavy devices starts running fast making noise. This example has been selected as low level in which we hear fan noise from core switch and router. The safeguard would be keep close eye on the sys logs and watch out for any possible break ups. The immediate action would be opening up all the doors allowing the air to pass through and check out the temperature gauge carefully.

4.2 Fault Tree Analysis for air-conditioning system failure

In FTA we selected the same case as main event: Air-Conditioning Failure; and then further divided it to root cause the case. There could be two reasons either no current to the air-conditioners or air-conditioner’s wiring fault as the wiring cable was not up to the load of air conditioning units.

Air-conditioners wiring fault is an undeveloped event. For no current to the air-conditioners we subdivided into two events either power supply no. 01 fails off or no continuity in high voltage circuit. We then subdivided no continuity in high voltage circuit into two events like fuse fails open in which we made two basic events; fuse no. 01 fails open or fuse no. 02 fails open. With these we made relay opens event and further divided it into basic event of relay fails open and no current to the relay. Then no current to the relay subdivided into power supply no. 2 fails off and no continuity in low voltage circuit.

At the last stage we subdivided no continuity in low voltage circuit into switch fails open basic event and crew member open the switch undeveloped event. The FTA chart is shown in figure 2 (appendix).

5. Comparison

FTA is basically a root causing analysis in which we do the risk and design assessment, making it a decision making method. The strengths of FTA are structured, graphical, quantitative and easy to model complex systems; it covers hardware, software, humans, procedures, timing. The user must know when, why and how to use it correctly. It evaluates safety for hazardous and catastrophic events; reliability for system unavailability; and performance for unintended functions. But, lack of proper fault tree planning and design can result in problems like restructure of entire tree, renaming all events in the tree, rework resulting in more cost and time. It must be planned ahead by leaving room for future tree expansion; allow for possible future changes in the tree without repercussion; Structure tree carefully, later changes can impact entire tree. Large fault trees require more design foresight by developing organized plan when several analyst work on same fault tree.

In our example of the selected system, our findings with FTA are the causes that lead to occurrence of the failure. We simply track down the possible reasons in the FTA flow diagram. But the diagram does not provide any of the safety measures, suggestions, consequences, and recommendations to overcome the risk. Furthermore, putting the tree in a wrong way can cause further failures for the system.

The HAZOP uses a team approach having pooled expertise. It is acceptable to major hazards in process industries, and also it is a systematic process. It is easy to learn and it can be easily adapted to almost all the operations that are carried out within process industries. No special level of academic qualification is required.

One does not need to be a university graduate to participate in a study.

With HAZOP, we select different deviations with respect to the nature of issue occurring within the data center. In the HAZOP chart, we can document the causes, consequences, safeguards, and appropriate actions for each deviation. Unlike FTA, the HAZOP chart provide complete details for the selected use case and the data center engineers or technicians can use this as a guideline. Thus, the HAZOP study we have done in the selected example can become an operation manual for the data center for the selected use case

6. Conclusion

By selecting air-conditioning failure as the use case for a data center system, the main objective is to perform two hazard analysis methods and make a comparison. With performing fault tree analysis first, we are able to accomplish what could be the possible reasons which lead to cause the air-conditioning system to fail. With FTA, we only achieve the root causes for the incident. The FTA diagram does not depict the safety precautions and safeguards for the use case.

Then we perform HAZOP method for the same use case. With HAZOP, we find out a complete comprehensive solution for the entire use case. A complete possible list of risks is identified with its respective disasters, techniques to avoid or minimize such risks, and provides guideline to follow in case of occurrence of these incidents.

As a result, HAZOP provides optimum solution for our selected example; therefore we find HAZOP a better method for industry-wide risk analysis.

7. References

- [1] Dyadem International Ltd, HAZOP – Hazard and Operability Analysis, 2008, http://www.dyadem.com/engineering/risk_management/facilitation_services/hazop/, accessed on April 21, 2008
- [2] Cisco Systems Inc, Cisco Data Center Network Architecture and Solutions Overview, 2006, http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns377/net_brochure0900aecd802c9a4f.pdf, accessed on April 23, 2008
- [3] Change Tech Solutions Inc, Manage your data center's risk exposures and efficiencies, Oct 30, 2002, <http://articles.techrepublic.com.com/5100-10878-1054496.html>, accessed on April 10, 2008
- [4] Chapter four, Hazard Analysis, <http://www.ema.gov.au/agd/ema/rwpattach.nsf/viewattachmentPersonal/BCE29B04E48926E6CA256C8>

A000A60E8/\$file/HAZARD_ANALYSIS.PDF,
April 25, 2008

- [5] Critech Research, Hazard Analysis, January 2002, <http://www.critech.com/hazard.htm>, accessed on April 10, 2008
- [6] Marvin Rausand, HAZOP Hazard and Operability Study, October 7, 2005, <http://www.ntnu.no/ross/srt/slides/hazop.pdf>, accessed on March 23, 2008
- [7] http://www.sms-ink.com/images/hazop_flow.gif, April 10, 2008
- [8] Concordia University, Office of Quality Programs 1999, <http://web2.concordia.ca/Quality/tools/15fta.pdf>, accessed on March 10, 2008
- [9] Daniel A. Crowl, Kirk-Othmer Encyclopedia of Chemical Technology, Hazard Analysis and Risk Assessment (Vol.13), John Wiley and Sons Inc, 1999-2008, <http://mrw.interscience.wiley.com/emrw/978047123896/kirk/article/hazacrow.a01/current/pdf>, accessed on March 10, 2008

Appendix

Figure1 – HAZOP Analysis for data center air-conditioning failure.

Guide Word	DEVIATION	CAUSE	CONSEQUENCE	SAFEGUARDS	ACTION
More	High temperature (Critical Level)	No current to air-conditioners. All Air-conditioning units turned off.	Core router went down. All network connectivity to other remote sites is lost. Internet connectivity to the whole facility is down.	Check out the temperature log on the temperature gauge. Make sure of human presence to watch out alerts generated by temperature gauge.	Open all the doors of the room for ventilation and turn on all the air-conditioning systems. Turn on the core router after gaining back to normal operating temperature. Make sure the internal temperature of the device is back to normal. Send the downtime report to the networks manager.
More	High temperature (Critical Level)	No current to air-conditioners. All Air-conditioning units turned off.	Core switch went down. Nodes lost network connectivity to most of the resources. Nodes are connected to the network but can only access the devices connected to its primary switch. Internet is also down.	Monitor the temperature log and follow the same process mentioned above.	Unplug the core switch immediately, both the primary and secondary power supplies to the device. Restore the room temperature with the same procedure as above. Turn the device back on. Once the device is back to operation, send the downtime report to the networks manager.
More	High temperature (Critical Level)	No current to air-conditioners. All Air-conditioning units turned off.	Asterisk server went down. All telephony services are out of order. Can not dial or receive phone calls. Whole office facility out of contact both with internal and the rest of the world.	Make sure the server is placed in an open area and its internal cooling system is functioning properly. Build an alert system generated by the server as well for any system failures. Develop a mechanism for automatic switch over to the secondary server (Zultys exchange).	Start over the server again. Run diagnostic tools on the server to make sure everything is good. Follow the same procedure for restoring the normal operating temperature as defined above.

More	High temperature (High Level)	No current to air-conditioners. All Air-conditioning units turned off.	Satellite receiver beeping alarm and generating warning alerts. If the temperature is not restored then the receiver will go down and internet connectivity will be lost.	Make sure the secondary link is available all the time and smooth and fast switch over is possible.	Switch to the secondary link. Restore the room temperature. Switch back to the primary link when operating temperature is restored.
More	High temperature (High Level)	No current to air-conditioners. All Air-conditioning units turned off.	Storage server went down. Employees are unable to access their data from their personal and shared drives.	Make sure the backup (secondary) storage server is replicated more frequently.	Switch to the secondary server. Roll out an email to all the users informing them about the failure. Switch on the primary server and run diagnostic tools, make sure the system is fine. Make sure no data is lost. Switch back the storage drives to the primary server.
PART OF	Irregular temperature (Medium level)	Unstable power supply. Air-conditioning units malfunctioning, not maintaining the operating temperature.	PIX firewall is malfunctioning Some of the internet services will not work, for example VPN connections and some specific remote connections are lost.	Procure a secondary firewall and configure it in a way that in case of primary failure, a switchover to secondary firewall will keep the system running.	Shutdown the PIX firewall. Disconnect the power cables. Wait for some time to get it cool down, and then start it back on. Check all of its connectivity and then verify its functionality from different nodes.
PART OF	Irregular temperature Temperature starts rising higher. (Low Level)	One or some of the air-conditioning units tripped off from the safety switch in the electric circuitry.	Cooling fans of core switch and core router starts running at high speed making big sounds. This is just one step before the alarms. When the devices sense high temperature, they speeds up their own fans to control internal temperature.	Keep an eye on the sys log for routers and switches and watch out the alerts generated.	Do not wait for the alarms. Check out the air-conditioning systems once you hear the fan sounds.

Figure 2 – Fault Tree Analysis Flowchart.

