Model Based Approach to Zonal Safety Analysis

Rachael Henderson[1], Ghulam Hussain[2], and Jacek Stecki[3]

[1,2]*Department of Mechanical Engineering, The University of Melbourne, Parkville - 3010, VIC, Australia*
hrn@student.unimelb.edu.au
ghussain@student.unimelb.edu.au

[3]*Chief Technology Officer, PHM Technology P/L*
jstecki@phmtechnology.com

ABSTRACT

Zonal Safety Analysis (ZSA) is an analysis technique for assessing the safety of complex systems however current tools limit its repeatability, thoroughness and time efficiency. The model based method proposed in this paper remedies these limitations.

Zonal Safety Analysis is widely used in the aerospace industry with similar analysis techniques also seen in the design of offshore oil & gas systems, mining equipment, defence platforms and other high-risk systems. The importance of ZSA comes from its ability to allow the designer to analyse the spread of hazards through the system from a physical standpoint. This is done by dividing the system into zones and understanding how hazardous forms of energy or material (e.g. fire or oil) could spread between these zones. This paper suggests a method for tracking the spread of hazards using a model of the system that can automatically generate the potential propagation of the hazards. To give the designer a better understanding of the source of the hazard, and greater flexibility in preventing it from occurring, the causes of these hazards are also defined in the model. Using a model based approach allows the analysis process to be efficiently repeated for a design variant at any stage in the product lifecycle by updating the structure (i.e. different components/configuration) or parameters (i.e. hazard causes, criticality) of the system model.

1. INTRODUCTION

Zonal analysis is a safety analysis technique commonly used in the aerospace industry. It is used to ensure the safety of the people operating and in the vicinity of the system, the nearby environment and the system itself. This is done by tracking the spread of hazards through the system from a physical standpoint. The current processes involve dividing the system into zones, finding the potential hazards originating from these zones and the impact these hazards could have on adjacent zones (SAE International, 1996). While hazard identification and mitigation in systems and plants has been widely discussed ((Dharmavaram & Klein, 2012), (de Bruin & Swuste, 2008), (Löwe & Kariuki, 2007)), it is the process of breaking the system into zones and tracking the physical spread of hazards that makes zonal analysis unique.

While widely used, the two most popular standards, SAE ARP4761 (SAE International, 1996) and ATA MSG-3 (Air Transport Association of America, Inc, 2003) fall short in terms of repeatability, thoroughness and time efficiency. This is because these two methods do not have rigorous, specific processes for identifying the potential hazards and how these my spread. This affects the repeatability of this process and makes it significantly more difficult to automate, negatively affecting time efficiency. The model based method presented in this paper is a more thorough and repeatable process. The value of this modelling technique comes from it relying less on the user's judgement than currently used standards as well as that a model based process is more able to be converted to a software system. This provides greater time efficiency due to the automation of many previously manual processes and the ability to quickly update the model based on design changes and re-run the analysis. Hence, such analysis can be run more often and can have applications in a wider range of industries, not just aerospace, allowing the user to identify issues earlier in the design process and prior to the first prototype.

The technical justification for using this method is its similarity to the pre-existing standards. The overall process of this method is very similar to that of ARP4761, except that where the method in the standard relies on a user's judgement, the model-based method presented in this paper performs a rigorous analysis that should capture all possibilities, not just those that would be captured by an individual or even group of users. This method will also capture how hazards may evolve from many contributing

factors – something else the method in ARP4761 or ATA MSG-3 may not catch.

2. PROPOSED MODEL BASED APPROACH

The workflow for the overall zonal analysis process that will be presented in the remainder of this document is in Figure 1.

2.1. System Model Generation

The system models required for this process include a functional block diagram and hazard diagrams for each component in the system. In the example in section 3 these are generated in MADe (Maintenance Aware Design environment), a software package developed by PHM Technology (PHM Technology, 2015). A *functional block diagram* is a model of the system where the constituent parts of the system are represented by blocks and the functional or physical connections between these components are represented by connections between the respective blocks. A *hazard diagram* describes the sequence of events and circumstances required for a hazard to eventuate.

2.2. Zone and Barrier Modelling

Once these models have been generated, zones are defined by the engineer carrying out this analysis. *Zones* are mutually exclusive collections of components that are in physical contact or proximity to one another. Between these zones barriers are modelled. A *barrier* is anything which either: prevents any activity which can cause hazard, or protects system and people from the consequences of that hazard. A barrier is used to prevent or obstruct energy flow in a system (Hollnagel, 1999) and since a hazard is a release of energy, barriers can protect against hazards. For each hazard or cause of hazard the barrier protects against, it is assigned a SIL (Safety Integrity Level) based on the probability of that hazard or cause of hazard being stopped. The SIL of a barrier must be defined for each hazard or cause of hazard in the system and is unique to that hazard/cause of hazard. The mapping between SIL and probability of halting hazard and causes of hazards is given in Table 1. Throughout this paper, for calculations, the worst case (higher failure rate) will be used.

Table 1 Relationship between SIL number and the probability of an SIS functioning for a low-demand system (Gruhn & Cheddie, 2006)

Safety Integrity Level (SIL)	Probability of not stopping hazard or cause of hazard
4	$10^{-4} – 10^{-5}$
3	$10^{-3} – 10^{-4}$
2	$10^{-2} – 10^{-3}$
1	$10^{-1} – 10^{-2}$

2.3. Finding causes of hazard

Once the model of the system – including zones and barriers – has been established, the potential causes of hazard that can occur in each zone are ascertained. Figure 3 shows the general process of how these causes of hazard become full hazards. There are three different types of cause of hazard that must be considered: environmental causes, human causes and failure causes where failure causes of hazard come from a failure in one of the parts of the system. The first two have predefined taxonomies and will have their probability of occurrence ascertained by the engineer performing the analysis using experience and previously collected data. Causes of hazard originating from failure of failure in a component of the system are discovered through failure analysis. Failure analysis will also give the expected rate of occurrence of the cause of hazard.

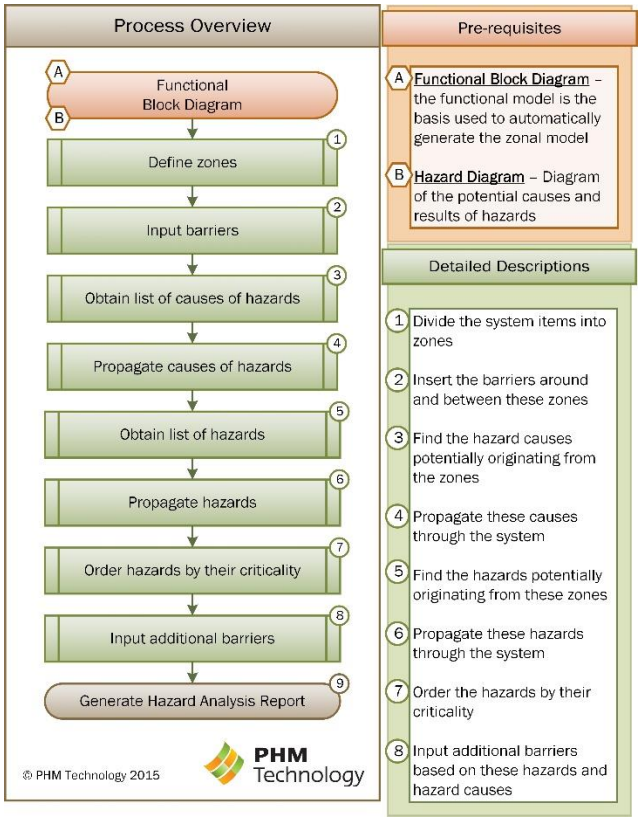


Figure 1 Workflow of proposed analysis procedure

2.4. Propagating the causes of hazard

Only causes of hazard resulting from the failure of components is propagated throughout the model. Environmental and human factors cannot spread as they are unique to the zone. In order to understand to which zones and with what probability causes of hazard may spread, one by one, these causes are propagated throughout the model. This propagation involves finding all paths a cause of hazard can take and using the probability of the initial component

failure occurring and the probability of the barriers on that path stopping the cause of hazard. This is used to find the probability of the cause of hazard reaching that zone.

An example of this calculation for a small system is given in the example in section 3 of this paper. This propagation will assume total independence of all barriers, i.e. the failure of one barrier has no impact in the success or failure of another.

2.5. Finding resultant hazards

A hazard may occur when more than one cause of hazard is present in the same zone. Once the probability of all causes of hazard occurring in each zone – both from originating from that zone and spreading there – has been calculated, the hazard diagrams associated with each zone can be used to calculate the probability of hazards occurring in the zones. With this information, the engineer performing the analysis can decide if this calculated probability is acceptable. Similarly, the probability of the hazard or contributing causes of hazard being detected at any point where the barriers would then indicate the probability of detecting hazards and causes of hazard rather than stopping them.

2.6. Hazard Criticality Number

Once the probability of occurrence and detection of a hazard has been established, these numbers can be converted to a 1-10 rating and, with a 1-10 rating of the severity of the hazard, the three values can be used in a similar manner to a Risk Priority Number (RPN) so as to allow the engineer a more intuitive understanding of the danger posed by a certain hazard. The 1-10 rating for probability of occurrence, detection and severity are henceforth referred to as the O, S and D values respectively. The multiplication of these values form the Hazard Criticality Number (HCN).

O, S and D are ranked between 1 and 10 to provide the user more intuitive measure with which to assess relative risk and such that the HCN can provide equal weight to all three values.

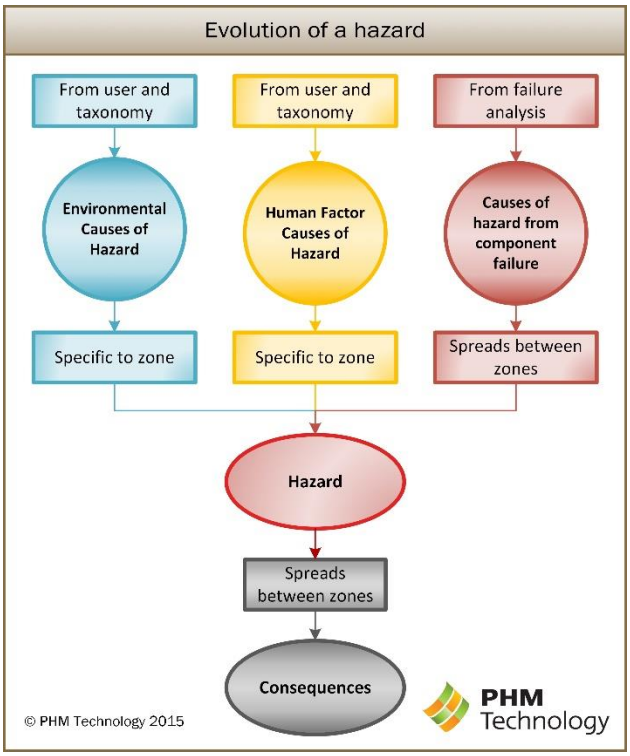


Figure 3 Image showing the differences between the different types of cause of hazard

Occurrence Number

Equation 1 will be used for the calculation of the O value where λ_o is the average number of occurrences per hour. The range given for this mapping is loosely based around average failure rates of components and should be wide enough to accommodate all hazards of concern.

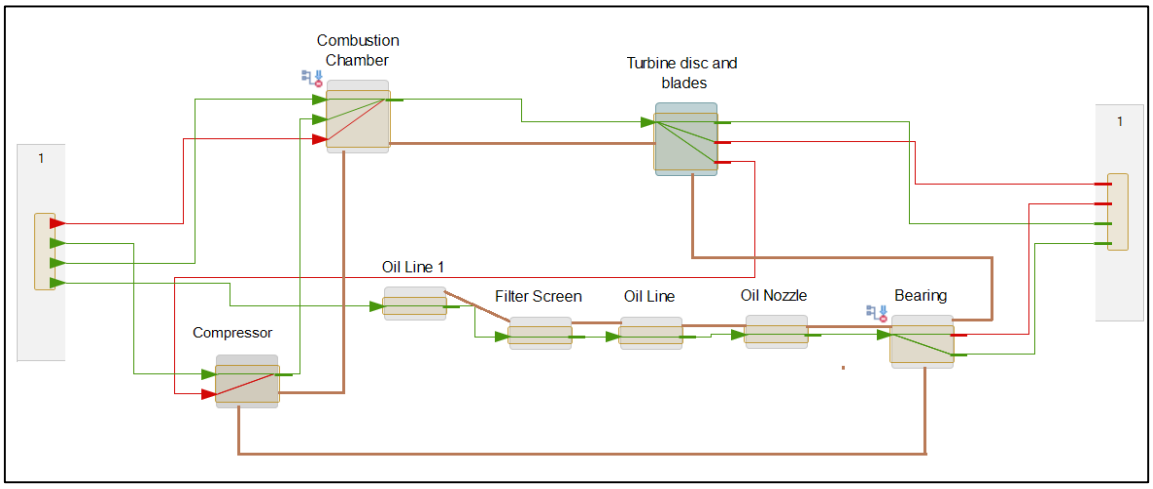


Figure 2 Functional Block Diagram of the system

$$O = \begin{cases} 1, & if\ \lambda_o \geq 10^{-2} \\ 12 + \log_{10} \lambda_o\,, & if\ 10^{-12} < \lambda_o < 10^{-2} \\ 10, & else \end{cases} \quad (1)$$

Severity Number

For each zone and hazard combination a severity number is user defined. This will be defined by the user and indicates the danger to the system, people and environment if the hazard were to occur in this zone.

Detection Number

The equation for D is similar to O. Here p_d represents the probability of the hazard not being detected throughout the entire path. As with the equation for O, the range should be small enough to easily differentiate the relative detectability of hazards as well as accommodating all hazards where detectability would be difficult enough to be of concern.

$$D = \begin{cases} 1, & if\ p_d \leq 10^{-10} \\ 10 + \log_{10} p_d\,, & if\ 10^{-10} < p_d < 1 \\ 10, & else \end{cases} \quad (2)$$

3. EXAMPLE

3.1. Background

To illustrate the process presented in this paper an example based on a real-life in-flight uncontained engine failure will be used. In this example, the failure of a stub pipe carrying lubricating oil resulted in the release of oil in the engine. The oil was ignited resulting in uncontained failure of the engine (Australian Transport Safety Bureau, 2013). While nobody was injured, the debris from the engine failure caused multiple systems to fail or be damaged and if it were not for the actions of the flight crew, the outcome might have been different.

3.2. Zonal Analysis Example

To illustrate the process defined earlier in this paper, a highly simplified model of the system described in section 3.1 will be used (see Figure 2). Additionally, the numeric values associated with the system as well as specified safety limits are created purely for the purpose of the example and may or may not align with the reality of the situation.

3.2.1. Initial Model

The input to the zonal anlaysis process described in this report is a functional block diagram of the system created in the software package MADe (see Figure 2). The green and red connection represent functional connections between components and are not important to this analysis. The physical paths between components (thick and brown) can also be seen and it is these paths that allow hazards and causes of hazard to spread between zones.

3.2.2. Creation of Zone

The system is divided into zones. The components or subsystems that are in physical proximity or physically connected to the others, are to be defined in one zone by the user.

For example the lubrication system that provides lubrication to the bearings of the turbine and compressor can be defined in one zone called “Lubrication Zone”. These zones can be seen in Figure 4.

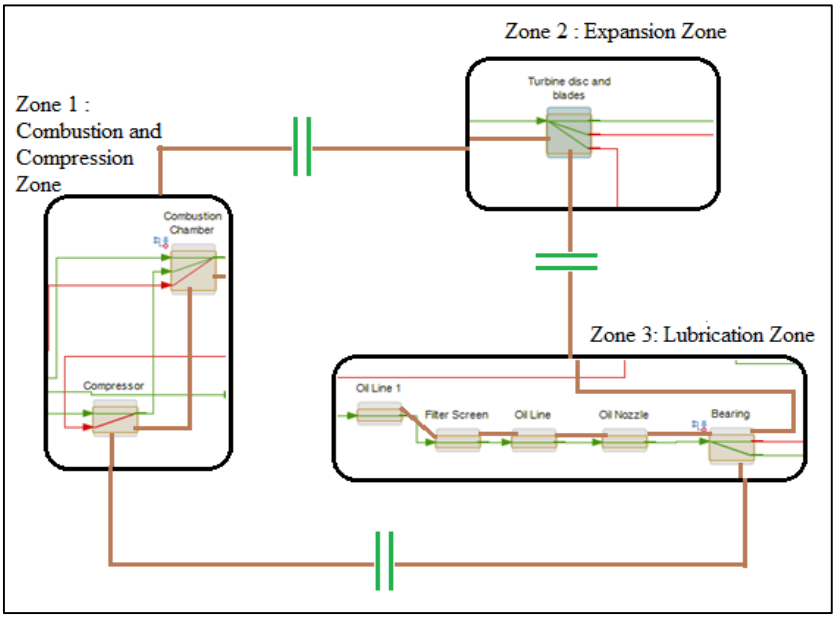


Figure 4 Sytem model with zonal divisions and barriers

Table 2. Table illustrating numeric zone designations

Zone Number	Zone Name
1	Combustion and Compression Zone
2	Expansion Zone
3	Lubrication Zone

3.3. Assumptions

The following data would be input by the user based on the design of the system and known data about the components.

3.3.1. Causes of hazard

For the purposes of this example, the rate of leakage of the oil from the pipe in the lubrication zone is assumed to be 8.072×10^{-6} per hour. In a practical application, this would come from an empirical failure rate of the component and analysis of failure diagrams for the component, such as that given in Figure 5.

3.3.2. Barrier Effectiveness

The SIL of the barriers between the zones for the cause of hazard – oil and the hazard – fire are given in Table 3 and Table 5. The probability of oil or fire being detected between these zones is given in Table 4 and Table 6 respectively. Throughout this example, the worst-case probabilities will be used, meaning the larger numbers for the probability of failure of barrier or probability of non-detection. In a practical setting, this data would come from analysis of the design and be user entered.

Table 3. Safety Integrity Level (SIL) of the different barriers between the zones to reduce the frequency of the leakage cause of hazard

Zone Links	SIL	Probability of failure of barrier
1 to 2	2	10^{-2}
1 to 3	1	10^{-1}
2 to 3	1	10^{-1}

Table 4. Effectiveness of the barriers between the different zones designed to detect the leakage cause of hazard

Zone Links	Probability of non-detection of oil
1 to 2	10^{-1}
1 to 3	10^{-1}
2 to 3	10^{-3}

Table 5. Safety Integrity Level (SIL) of the different barriers between the zones to reduce the frequency of fire

Zone Links	SIL	Probability of failure of barrier
1 to 2	1	10^{-1}
1 to 3	2	10^{-2}
2 to 3	1	10^{-1}

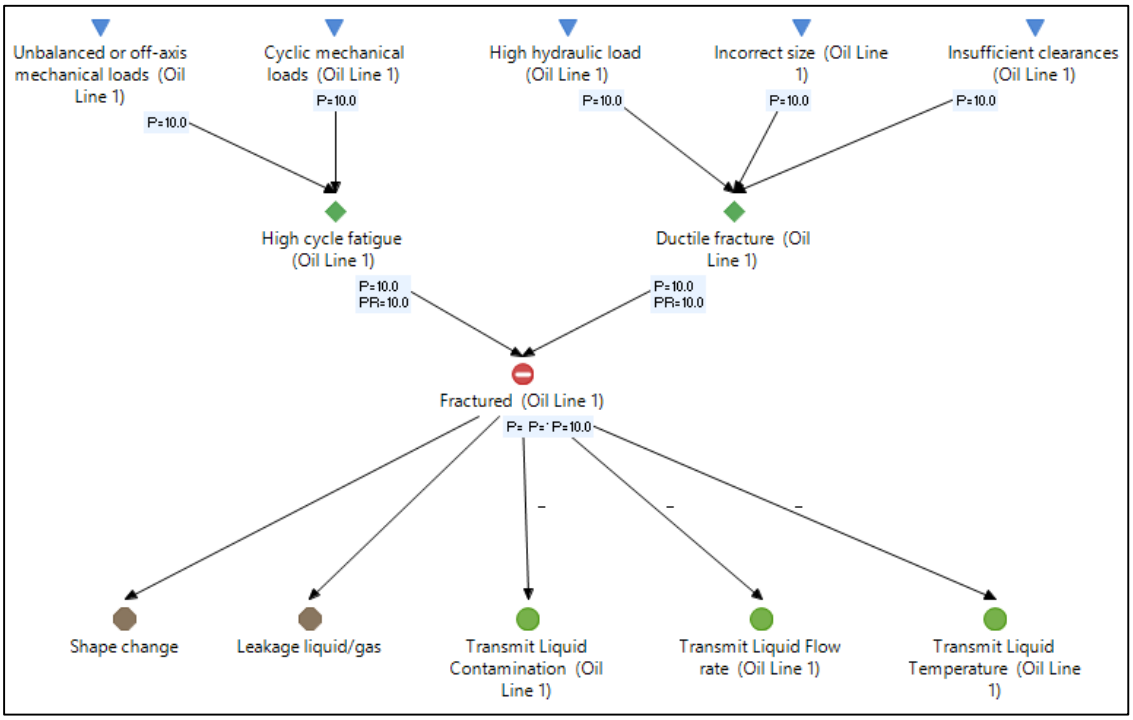


Figure 5 Example of a failure diagram for a component

Table 6. Barrier effectiveness for detecting fire hazard

Zone Links	Probability of non-detection of fire
1 to 2	10^{-2}
1 to 3	10^{-1}
2 to 3	10^{-1}

3.3.3. Hazard diagram

In order to obtain the frequency of the fire from the frequency of the oil leak, we need to know how other factors contribute to ignition and how frequent these other factors will occur. The evolution of a hazard from the causes is understood by using a hazard diagram (Figure 6), where the causes of hazard coming from component failure are given in red, the causes given by environmental factors in blue and the human factors in yellow. This is the hazard diagram that will be assumed for zone 2.

This hazard diagram assumes that either a leakage of oil (given by the red circle on the right) and high temperature (given by the blue circle on the left) or a leakage of oil and improper wire maintenance (the centre yellow circle) will give the hazard of fire (red diamond). These required combinations are indicated by the two small 'AND' gates above the fire hazard where one has lines from the blue circle and red circle and the other lines from the yellow circle and red circle. The potential consequence of death is indicated by the black square.

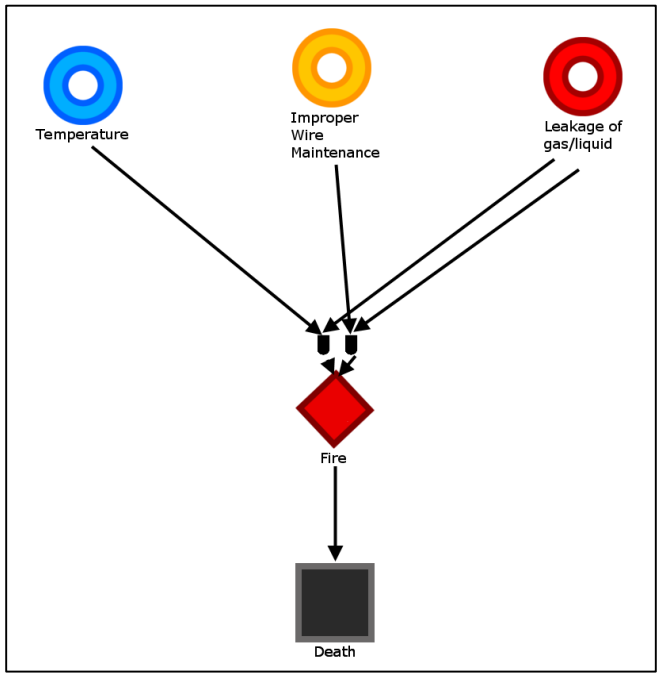


Figure 6 Hazard Diagram for the expansion zone

Table 7. Data available for calculating the probability of fire occurring

Probability of high temperature	Probability of improper wire maintenance
9×10^{-1}	2×10^{-2}

3.3.4. HCN Limit

The user will be required to place a limit on the maximum allowable HCN. For the purposes of this example, it is assumed to be 350.

3.4. Hazard Analysis

3.4.1. Propagation of Causes of Hazards

The causes of hazard identified in 3.3.1 are propagated to all the adjacent zones. In Figure 4 it can be seen that there are two paths between the lubrication and expansion zone; one directly between the two, and one through the combustion and compression zone. The probabilities of the cause of hazard reaching the other zones can be calculated using the SIL of the barriers between all zones and the known initial probability of leakage occurring (sections 3.3.2 and 3.3.1 respectively).

To illustrate the calculations required, below is a set of calculations identifying the probability of the leakage cause of hazard reaching the expansion zone (zone 2) from the lubrication zone (zone 3). All paths from the source zone (zone 3) to the target zone (zone 2) are identified. The identified paths are $3 \rightarrow 2$ and $3 \rightarrow 1 \rightarrow 2$.

The probability of the cause of hazard (uncontained oil) moving through each path is now identified. Assuming the probability of the cause of hazard occurring in zone 3 is 100%, we can see that:

- The probability of the leakage reaching zone 3 through the path $3 \rightarrow 2$ is $1 \times 0.1 = 0.1$ as there is a maximum probability of the barrier between zone 3 and 4 failing of 10% of the time
- The probability of the leakage reaching zone 3 through the path $3 \rightarrow 1 \rightarrow 2$ is $1 \times 0.1 \times 0.01 = 10^{-3}$ as there is a maximum probability of the barrier between zone 1 and 3 failing of 10% and a maximum probability of the barrier between zone 1 and 2 failing of 1%

Once we have identified the probabilities of each path we then find the probability that the cause hazard will not take any path. For the example this will mean:

$$1 - P_{reach} = (1 - 0.1) \times (1 - 10^{-3}) = 0.8991 \qquad (3)$$

Therefore the probability of the cause of hazard reaching zone 2 through either path is $1 - 0.8991 = 0.1009 = 10.09\%$. This is then multiplied by the average number of oil leakages per hour in the source zone to get the average number of times leaked oil will reach the target zone.

Table 8. Probability data for the propagation of the hazard cause

Zone	Probability of oil reaching zone given leakage	Average rate of leaked oil reaching zone per hour	Probability of cause not being detected
3 to 1	1.009×10^{-1}	8.14×10^{-7}	1.0009×10^{-1}
3 to 2	1.009×10^{-1}	8.14×10^{-7}	1.099×10^{-2}
3 to 3	1	8.07×10^{-6}	1

This process is automated and repeated for all target and source zones. The process for determining if the cause is not detected is nearly identical. We only have one target zone in our example but all non-source zones are also potential target zones. Table 8 shows these values and Figure 7 shows the paths of the cause of hazard.

3.4.2. Obtain List of Hazards

Equation 4 is used to obtain the expected frequency of fire (P_f) in zone 2. This is done by using the pre-calculated frequency of the leaked oil reaching zone 2 (given in Table 8 and designated as $Leakage\ rate$ in equation 4), the required combination of causes for fire to occur in zone 2 (given in Figure 6 with an explanation in section 0) and the expected probability of these other causes occurring at the same time as the oil (given in Table 7 with P_{Temp} representing the probability of high temperature and P_{Wire} the probability of poor wire maintenance).

$$P_f = Leakage\ rate \times (P_{Temp} + P_{Wire}) \quad (4)$$
$$= 8.14 \times 10^{-7} \times (0.9 + 0.02) = 7.5 \times 10^{-7}$$

The probability of detection of the hazard is equal to that of the contributing failure cause of hazard (leakage).

3.4.3. Propagate Hazards

In this step, the hazard (fire) is spread to adjacent zones and the probability of it reaching other zones is calculated. As this process is identical to hazard cause propagation, we again need to define the SIL of barriers against the fire hazard for each zone connection. Again this will be user entered and Table 5 shows the data we will be using for this example and Figure 7 shows the paths of the hazards.

Putting these SIL values of fire barriers between each zone into the same algorithm used for the causes the following probabilities for each zone are obtained.

Table 9. Probabilities of the fire hazard reaching the zones

Zone Number	Probability fire reaches zone if started in zone 2	Average number of fires per hour in zone
1	1.009×10^{-1}	7.6×10^{-8}
2	1	7.5×10^{-7}
3	1.009×10^{-1}	7.6×10^{-8}

Table 10. Probability of the fire or the entire hazard path (including causes) being detected

Zone Number	Probability of fire not being detected after reaching zone	Probability of leakage and fire not being detected
1	1.99×10^{-2}	2.87×10^{-4}
2	1	1.009×10^{-2}
3	1.009×10^{-1}	1.11×10^{-3}

3.4.4. Defining Hazard Criticality – HCN Values

We are using the HCN as defined in section 2.6 to prioritize the hazards and zones that are of the most importance. Using the equations outlined in section 2.6 for D and O and values of S created solely for the purpose of example, Table 11, Table 12 and Table 13 are generated. Multiplying O, S and D as per the process outlined in section 2.6 Table 14 is obtained.

Table 11. Occurrence numbers for the fire hazard for zones

Zone Number	Average number of fires per hour	O
1	7.6×10^{-8}	5
2	7.5×10^{-7}	6
3	7.6×10^{-8}	5

Table 12. Severity numbers for zones for the fire hazard

Zone Number	Zone Name	S
1	Combustion and Compression Zone	8
2	Expansion Zone	8
3	Lubrication Zone	9

Table 13. Detection number for the fire hazard zones

Zone Number	Probability of entire fire path remaining undetected	D
1	2.187×10^{-4}	6
2	1.099×10^{-2}	8
3	1.11×10^{-3}	7

Table 14. HCN for all zones for the fire hazard

Zone Number	O	S	D	HCN
1	5	8	6	240
2	6	8	8	384
3	5	9	7	315

3.5. Updating design

As stated in section 3.3.4, the maximum allowable HCN is 350, it can be seen that the hazardousness in zone 2 needs to be reduced. As the hazard is created in zone 2 and does not spread there, the design must be updated such that the hazard causes are more easily detected or occur less often in zone 2. In this example we will alter the design to reduce the occurrence.

3.5.1. Updating Barriers

The optimal location for the barrier upgrade so as to reduce the rate of fire in zone 3 can be found.

The two paths identified between the source of the leak and zone 2 where it can become fire are $3 \rightarrow 2$ and $3 \rightarrow 1 \rightarrow 2$. The probabilities of the oil following either of these paths are given in Table 15. The data in Table 15 comes from multiplying the probability of all the barriers along the path failing. The probabilities of the barriers failing obtained from Table 3.

Table 15. Table showing the probabilities the paths are responsible for

	$3 \rightarrow 2$	$3 \rightarrow 1 \rightarrow 2$
Probability	10^{-1}	10^{-3}

It can be seen that barrier $3 \rightarrow 2$ is responsible for the highest rate of fire in the target zone. This means we recommend an increase of the SIL of the barrier between zones 3 and 2 – between the lubrication and expansion zones.

3.5.2. Barriers to Reduce the Occurrence of Hazard

Upgrading the barriers in the location identified in 3.5.1, the SIL of the barriers for the cause of hazard were updated with the values given in Table 16.

Table 16. Proposed SIL for the cause of hazard

Zone Links	SIL	Probability of failure of barrier
1 to 2	2	$10^{-2} - 10^{-3}$
1 to 3	1	$10^{-1} - 10^{-2}$
2 to 3	3	$10^{-3} - 10^{-4}$

Using the SILs, the probabilities and rates of occurrence of the cause of hazard can be identified.

Table 17. Probabilities and rates of cause of hazard for the upgraded barrier

Zone Links	Probability of leakage reaching zone	Average number of leakages per hour
3 to 1	1.00009×10^{-1}	8.1×10^{-7}
3 to 2	1.999×10^{-3}	1.6×10^{-8}
3 to 3	1	8.1×10^{-6}

Using an identical procedure to that shown previously, the new average number of occurrences of fire per hour in the source zone can be found. Using the known rate that the leaked oil will appear in zone 2 of 1.6×10^{-8} (designated

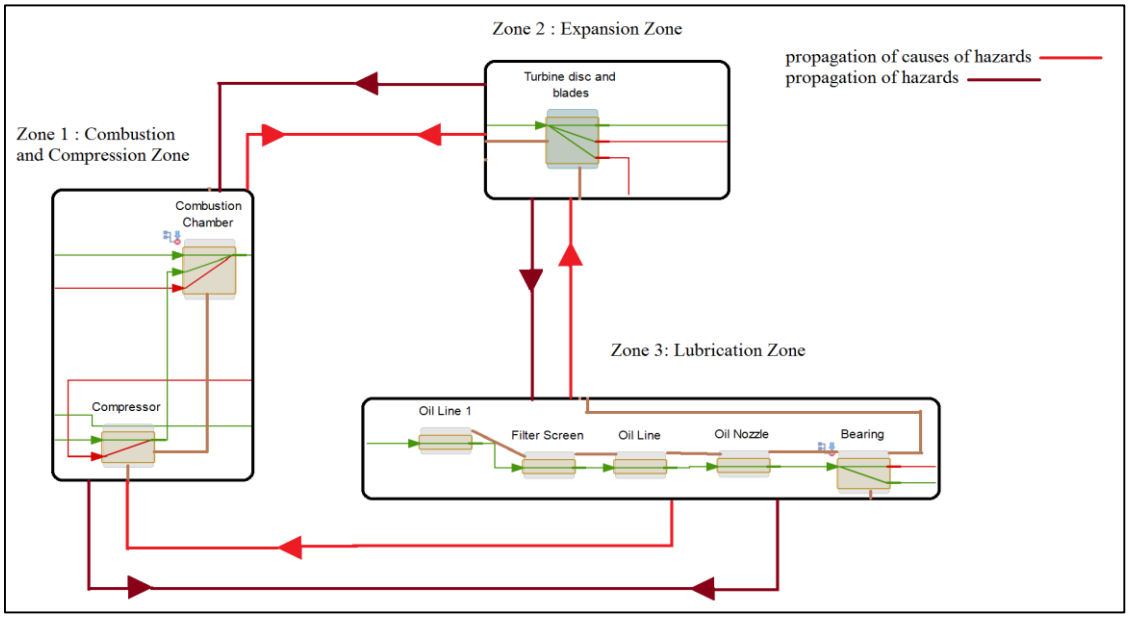


Figure 7 Image showing the propagation paths of the cause of hazard and hazard

Leakage Rate in equation 5) we can calculate the expected rate of fire in zone 2. This uses the probabilities of high temperature and poor wire maintenance given in section 0.

$$P_f = Leakage\ rate \times (P_{Temp} + P_{Wire}) \quad (5)$$
$$= 1.6 \times 10^{-8} \times (0.9 + 0.02)$$
$$= 1.47 \times 10^{-8} \text{ per hour}$$

Propagating the hazards in the same way as shown previously, the below values are found.

Table 18. Probabilities and Rates of Hazard Propagation in each zone and their respective Occurrence number

Zone Number	Propagation fire reaches zone	Average number of fires per hour	O
1	1.009×10^{-1}	1.5×10^{-9}	3
2	1	1.5×10^{-8}	4
3	1.009×10^{-1}	1.5×10^{-9}	3

As the only number that will change will be O, we can use the previously defined S and D values. Using this, we can see in Table 19 that the upgraded barrier has improved the HCN value for zone 3.

Table 19. Comparison between HCN of old and new design

Zone	Current Design				Updated Design			
	O	S	D	HCN	O	S	D	HCN
1	5	8	6	240	3	8	7	144
2	6	8	8	384	4	8	7	256
3	5	9	7	315	3	9	8	189

It can be seen that the updated design delivers the required HCN and the system now meets safety requirements that it did not in the previous design. Through the use of the algorithm proposed in this document the hazards have been successfully identified, their level of risk (HCN) identified and then methods have been suggested to reduce this risk to acceptable levels.

4. CONCLUSION

In this paper, a new method for performing zonal analysis using a model of the system and hazards/causes of hazards was presented. Modelling this system like a connected graph were the zones are the nodes and the strength of the connection represents the ability of the barrier between two zones to protect against a specific hazard or cause of hazard allows greater automation of the process as well as increased repeatability. This makes it superior to current manual processes such as those contained in MSG-3 and ARP4761. A potential method of implementing this process was presented in the example.

Potential areas for future investigation include using fuzzy logic instead of crisp data for the O, S, D and HCN values to account for numerical inaccuracies in the initial model, the inclusion of functional failures rather than only physical (e.g. pressure loss as opposed the material leakage analysed in the example) and the automatic generation of recommendations for zonal divisions based on the relative distances between objects, with that information coming from a CAD file. This latter process would allow even greater automation and allow new designs to be evaluated even more quickly.

ACKNOWLEDGEMENTS

The authors wish to express their sincere thanks to Chris Stecki as well as everyone at PHM Technology for their assistance and support during this project. The authors would also like to thank Dr Jimmy Philip for his guidance throughout the project.

REFERENCES

Air Transport Association of America, Inc. (2003). *ATA MSG-3*. Air Transport Association of American, Inc. Washington, DC: Air Transport Association of American, Inc. Retrieved March 28, 2015

Australian Transport Safety Bureau. (2013, June 27). *Investigation: AO-2010-089 - In-flight uncontained engine failure Airbus A380-842, VH-OQA, overhead Batam Island, Indonesia, 4 November 2010*. Retrieved March 15, 2015, from Australian Transport Safety Bureau: http://www.atsb.gov.au/publications/investigation_reports/2010/aair/ao-2010-089.aspx

de Bruin, M., & Swuste, P. (2008, February). Analysis of hazard scenarios for a research environment in an oil and gas exploration and production company. *Safety Science, 46*(2), 261-271.

Dharmavaram, S., & Klein, J. A. (2012, September). An introduction to assessing process hazards. *Process Safety Progress, 31*(1), 266-270. doi:10.1002/prs.11495

Gruhn, P. E., & Cheddie, H. (2006). *Safety Instrumented Systems - Design, Analysis, and Justification* (2nd ed.). ISA. Retrieved April 22, 2015

Hollnagel, E. (1999). Accidents and barriers. *Proceedings of Lex Valenciennes, 28*, pp. 175-182. Retrieved July 5, 2015

Löwe, K., & Kariuki, S. G. (2007, December). Integrating human factors into process hazard analysis. *Reliability Engineering & System Safety, 92*(12), 1764-1773.

PHM Technology. (2015). MADe.

SAE International. (1996, December 1). ARP4761. SAE International. Retrieved February 13, 2015

BIOGRAPHIES

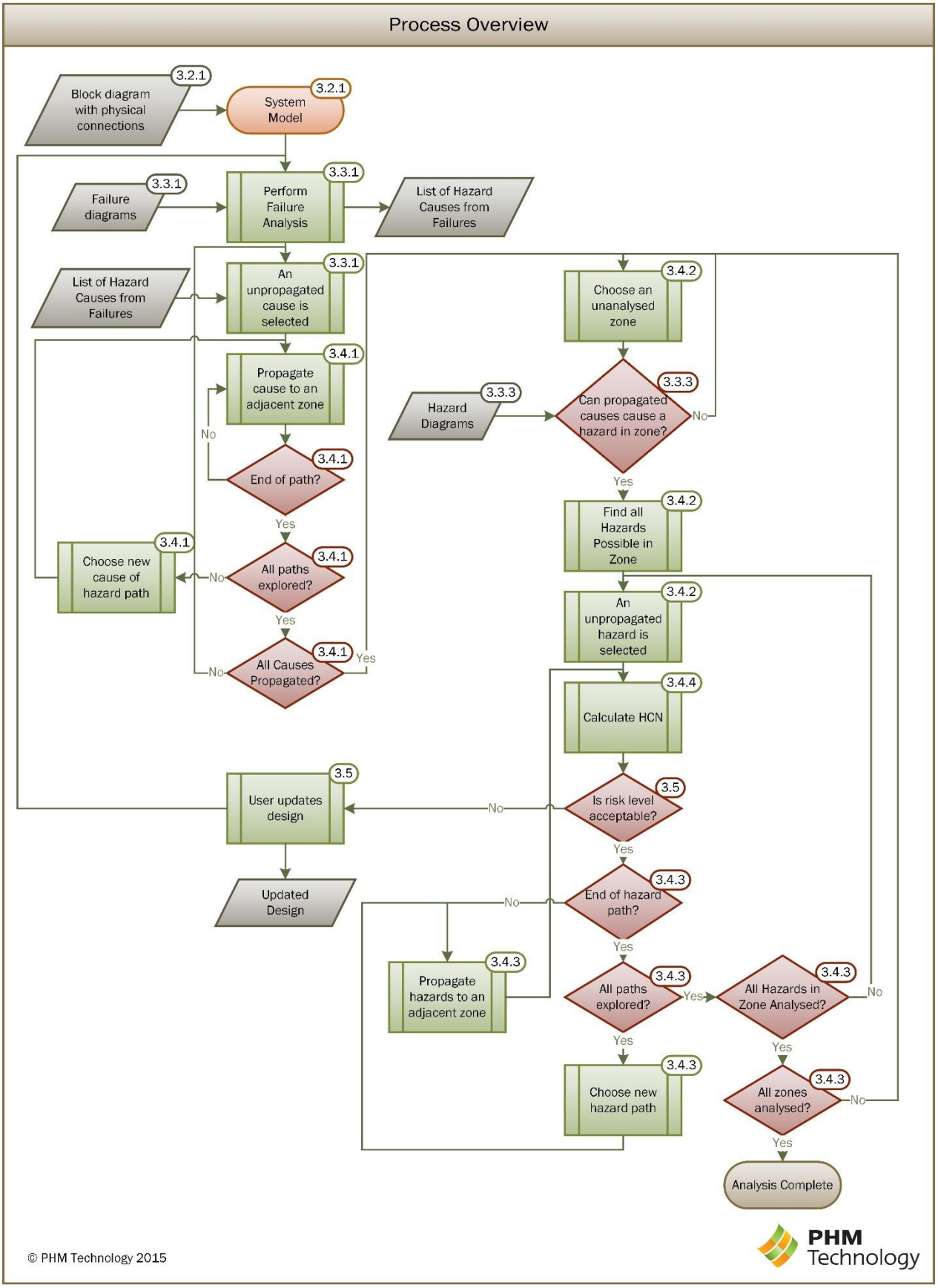
Rachael Henderson completed a Bachelor of Science majoring in electrical systems in 2014 and a Master of Engineering majoring in mechatronics in 2016 at the University of Melbourne. She is currently a design engineer at Supacat and was previously an intern at PHM technology.

Ghulam Hussain has completed his Master of Engineering degree majoring in Mechanical Engineering, at the University of Melbourne, in December 2015. He has completed his Bachelor of Mechanical Engineering at the University of Engineering and Technology, Lahore, in September 2013. During his academic career, he worked on different projects including the design of a gamma type low temperature differential solar sterling engine, the design and manufacture of a prototype water tube boiler and the design and fabrication of a prototype gear box for an industrial application. Previously he was an intern at Descon Engineering Limited, Lahore, in the Project Management Department.

Dr. Jacek S. Stecki Chief Technical Officer, PHM Technology P/L - Risk Assessment, Prognostic and Health Management R&D company. Former Associate Professor and Director of Centre for Machine Condition Monitoring at Monash University, Melbourne, Australia. Consultant in the field of subsea engineering, simulation, prognostics and health management (PHM), subsea engineering (oil and gas) and hybrid vehicles. Over 40 years experience in research and consulting on fluid power, condition monitoring subsea engineering and simulation. The author of over 150 technical and scientific papers on the subject of fluid power, simulation, condition monitoring and subsea engineering. Currently involved in Prognostic and Health Management programs in Minining, Petrochemical and Aerospace industries.

APPENDIX

Overleaf is a flowchart displaying the entire proposed process with numbering corresponding to the sections and subsections of this document where a more detailed description of the process or illustration though an example can be found.


Process Overview
Block diagram with physical connections
3.2.1
System Model
3.2.1
Failure diagrams
3.3.1
Perform Failure Analysis
3.3.1
List of Hazard Causes from Failures
List of Hazard Causes from Failures
An unpropagated cause is selected
3.3.1
Propagate cause to an adjacent zone
3.4.1
End of path?
3.4.1
No
Yes
All paths explored?
3.4.1
Choose new cause of hazard path
3.4.1
No
Yes
All Causes Propagated?
3.4.1
No
Yes
Choose an unanalysed zone
3.4.2
Hazard Diagrams
3.3.3
Can propagated causes cause a hazard in zone?
3.3.3
No
Yes
Find all Hazards Possible in Zone
3.4.2
An unpropagated hazard is selected
3.4.2
Calculate HCN
3.4.4
Is risk level acceptable?
3.5
No
Yes
User updates design
3.5
Updated Design
End of hazard path?
3.4.3
No
Yes
Propagate hazards to an adjacent zone
3.4.3
All paths explored?
3.4.3
Yes
All Hazards in Zone Analysed?
3.4.3
No
Yes
Choose new hazard path
3.4.3
All zones analysed?
3.4.3
No
Yes
Analysis Complete
© PHM Technology 2015
PHM Technology