

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800

Open access books available

122,000

International authors and editors

135M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Developing Risk Models for Aviation Inspection and Maintenance Tasks

Lee T. Ostrom and Cheryl A. Wilhelmsen
University of Idaho
USA

1. Introduction

Risk assessment has been used to analyze a wide range of industries to determine vulnerabilities with the ultimate purpose of eliminating the sources of risk or reducing them to a reasonable level. The purpose of this chapter is to show how risk assessment tools can be used to develop risk models of aviation maintenance tasks. Two tools will be discussed in this chapter, though many other methods exist. The tools discussed in this chapter are:

- Failure Mode and Effect Analysis (FMEA)
- Event and Fault Tree Analysis

Ostrom and Wilhelmsen (2011) discuss a wide range of risk assessment tools and this book provides many examples of how these tools are used to analyze various industries.

2. Failure mode and effect analysis

An FMEA is a detailed document that identifies ways in which a process or product can fail to meet critical requirements. It is a living document that lists all the possible causes of failure from which a list of items can be generated to determine types of controls or where changes in the procedures should be made to reduce or mitigate risk. The FMEA also allows procedure developers to prioritize and track procedure changes (Mil Std 882B, C, 1984 and 1993). The process is effective because it provides a very systematic process for evaluating a system or a procedure, in this instance. It provides a means for identifying and documenting:

1. Potential areas of failure in process, system, component, or procedure.
2. Potential effects of the process, system, component, or procedure failing.
3. Potential failure causes.
4. Methods of reducing the probability of failure.
5. Methods of improving the means of detecting the causes of failure.
6. Risk ranking of failures, allowing risk informed decisions by those responsible.
7. A starting point from which the control plan can be created.

FMEA can be used to analyze:

1. Process: Documents and addresses failure modes associated with the manufacturing and assembly process.
2. Procedure: Documents and addresses failure points and modes in procedures.

3. Software: Documents and addresses failure modes associated with software functions.
4. Design: Documents and addresses failure modes of products and components long before they are manufactured and should always be completed well in advance of prototype build.
5. System: Documents and addresses failure modes for system and subsystem level functions early in the product concept stage.
6. Project: Documents and addresses failures that could happen during a major program.

A procedure analysis will be used to demonstrate how an FMEA can be conducted. An FMEA is conducted on a step-by-step basis. Table 1 shows an example of an FMEA table. The following constitutes the steps of an FMEA. These steps will be illustrated by use of an example.

Item	Potential Failure Mode	Cause of Failure	Possible Effects	Probability	Criticality (Optional)	Prevention
Step in procedure, part, or component	How it can fail:					
	-pump not working	What caused the failure:	Outcome of the failures:	How possible is it:	How bad are the results:	What can be done to prevent either failures or results of the failures?
	-stuck valve	Broken part	Nothing	Can use numeric values:	Can use dollar value:	
	-no money in a checking account	Electrical failure	System crash	0.1, 0.01, or	\$10., \$1,000., or \$1,000,000	
	-broken wire	Human error	Explosion	1E-5	Can use a qualitative measure:	
	-software error	Explosion	Fire	Can use a qualitative measure:	Can use a qualitative measure:	
	-system down	Bug in software	Accident	Negligible, low probability, high probability.	Nil, Minimal problems, major problems.	
-reactor melting down		Environmental release				

Table 1. Example FMEA Table

The first step is to create a flow diagram of the procedure. This is a relatively simple process in which a table or block diagram is constructed that shows the steps in the procedure. Table 2 shows the simple steps checking an engine chip detector. Note that this is a simple example and not an exhaustive analysis. Table 3 lists the major, credible failures associated with each step in the process. Table 4 shows the effect of the potential failures. Table 5 shows the complete FMEA for the task.

Inspecting Chip Detector	
Step Number	Process Steps
1	Cut and Remove Lock Wire from Oil Drain Plug
2	Remove Oil Drain Plug
3	Drain Oil
4	Cut and Remove Lock Wire from Chip Detector
5	Remove Chip Detector
6	Examine Chip Detector
7	Clean Chip Detector
8	Replace Chip Detector
9	Lock Wire Chip Detector
10	Replace Oil Drain Plug
11	Lock Wire Oil Drain Plug
12	Replace Oil

Table 2. Process Steps for checking a chip detector

FMEA is a relatively simple, but powerful tool and has a wide range of applicability for analyzing aircraft maintenance tasks.

3. Event tree and fault tree analysis

An event tree is a graphical representation of a series of possible events in an accident sequence (Vesely, William; et. al., 2002). Using this approach assumes that as each event occurs there are only two outcomes, failure or success. A success ends the accident sequence and the postulated outcome is either that the accident sequence terminated successfully or was mitigated successfully. For instance, a fire starts in an engine. This is the initiating event. Then the automated system closes fuel feed. If the lack of fuel does not extinguish the fire, the next step is that the fire suppression system is challenged. If the system actuates the fire suppression system the fire is suppressed and the event sequence ends. If the fire suppression system fails the fire is not suppressed then the accident sequence progresses. Table 6 shows this postulated accident sequence. Figure 1 shows this accident sequence in an event tree.

As in most of the risk assessment techniques, probabilities can be assigned to the events and combined using the appropriate Boolean Logic to develop an overall probability for the various paths in the event. Using our example from above, we will now add probabilities to the events and show how the probabilities combine for each path. Figure 2 shows the addition of path probability to the event tree.

Inspecting Chip Detector	
Process Steps	Major Failures
Cut and Remove Lock Wire from Oil Drain Plug	No major failures that affect process outcome
Remove Oil Drain Plug	No major failures that affect process outcome
Drain Oil	No major failures that affect process outcome
Cut and Remove Lock Wire from Chip Detector	No major failures that affect process outcome
Remove Chip Detector	Improper removal can remove debris from chip detector and cause false reading. Chip detector can be damaged if improperly removed.
Examine Chip Detector	Aircraft Maintenance Technician (AMT) fails to notice debris on chip detector.
Clean Chip Detector	AMT fails to properly clean chip detector
Replace Chip Detector	AMT fails to properly install chip detector
Lock Wire Chip Detector	AMT fails to properly lock wire chip detector
Replace Oil Drain Plug	AMT fails to properly install oil drain plug
Lock Wire Oil Drain Plug	AMT fails to properly lock oil drain plug
Replace Oil	AMT fails to properly replace oil

Table 3. Failures Associated with Each Step

Inspecting Chip Detector		
Process Steps	Potential Failure Modes	Potential Failure Effects
Remove Chip Detector	Improper removal can remove debris from chip detector and cause false reading. Chip detector can be damaged if improperly removed.	Engine could fail if chips are not properly detected. Added cost to replace damaged chip detector.
Examine Chip Detector	Aircraft Maintenance Technician (AMT) fails to notice debris on chip detector.	Engine could fail if chips are not properly detected.
Clean Chip Detector	AMT fails to properly clean chip detector	Debris could be placed back into engine.
Replace Chip Detector	AMT fails to properly install chip detector	Oil could leak past chip detector. Threads of chip detector could be damaged.
Lock Wire Chip Detector	AMT fails to properly lock wire chip detector	Chip detector could become loose and fall out, leading to loss of engine oil.
Replace Oil Drain Plug	AMT fails to properly install oil drain plug	Engine oil could leak out. Oil drain plug could become damaged.
Lock Wire Oil Drain Plug	AMT fails to properly lock oil drain plug	Oil drain plug could become loose and fall out. Oil drain plug could become damaged.
Replace Oil	AMT fails to properly replace oil	Engine could fail.

Table 4. Effect of Potential Failures

Procedure Step	Potential Failure Mode	Cause of Failure	Possible Effects	Probability	Criticality	Prevention
Cut and Remove Lock Wire from Oil Drain Plug	No major failures that affect process outcome	AMT Fails to Perform Task	Delay in performing task.	Very Low	Not Critical	Ensure AMTs follow work schedule
Remove Oil Drain Plug	No major failures that affect process outcome	AMT Fails to Perform Task	Delay in performing task.	Very Low	Not Critical	Ensure AMTs follow work schedule
Drain Oil	No major failures that affect process outcome	AMT Fails to Perform Task	Delay in performing task.	Very Low	Not Critical	Ensure AMTs follow work schedule
Cut and Remove Lock Wire from Chip Detector	No major failures that affect process outcome	AMT Fails to Perform Task	Delay in performing task.	Very Low	Not Critical	Ensure AMTs follow work schedule
Examine Chip Detector	AMT fails to notice debris on chip detector.	AMT Fails to Properly Perform Task	Engine could fail if chips are not properly detected. Added cost to replace damaged chip detector.	Moderate	Critical	Training, procedures, and inspection oversight
Clean Chip Detector	AMT fails to properly clean chip detector	AMT Fails to Properly Perform Task	Engine could fail if chips are not properly detected.	Moderate	Critical	Training, procedures, and inspection oversight
Replace Chip Detector	AMT fails to properly install chip detector	AMT Fails to Properly Perform Task	Debris could be placed back into engine.	Moderate	Critical	Training, procedures, and inspection oversight
Lock Wire Chip Detector	AMT fails to properly lock wire chip detector	AMT Fails to Properly Perform Task	Oil could leak past chip detector. Threads of chip detector could be damaged.	Moderate	Critical	Training, procedures, and inspection oversight
Replace Oil Drain Plug	AMT fails to properly install oil drain plug	AMT Fails to Properly Perform Task	Chip detector could become loose and fall out, leading to loss of engine oil.	Moderate	Critical	Training, procedures, and inspection oversight
Lock Wire Oil Drain Plug	AMT fails to properly lock oil drain plug	AMT Fails to Properly Perform Task	Engine oil could leak out. Oil drain plug could become damaged.	Moderate	Critical	Training, procedures, and inspection oversight
Replace Oil	AMT fails to properly replace oil	AMT Fails to Properly Perform Task	Oil drain plug could become loose and fall out. Oil drain plug could become damaged.	Low	Critical	Training, procedures, and inspection oversight
			Engine could fail.			

Table 5. Complete FMEA for Chip Detector Task

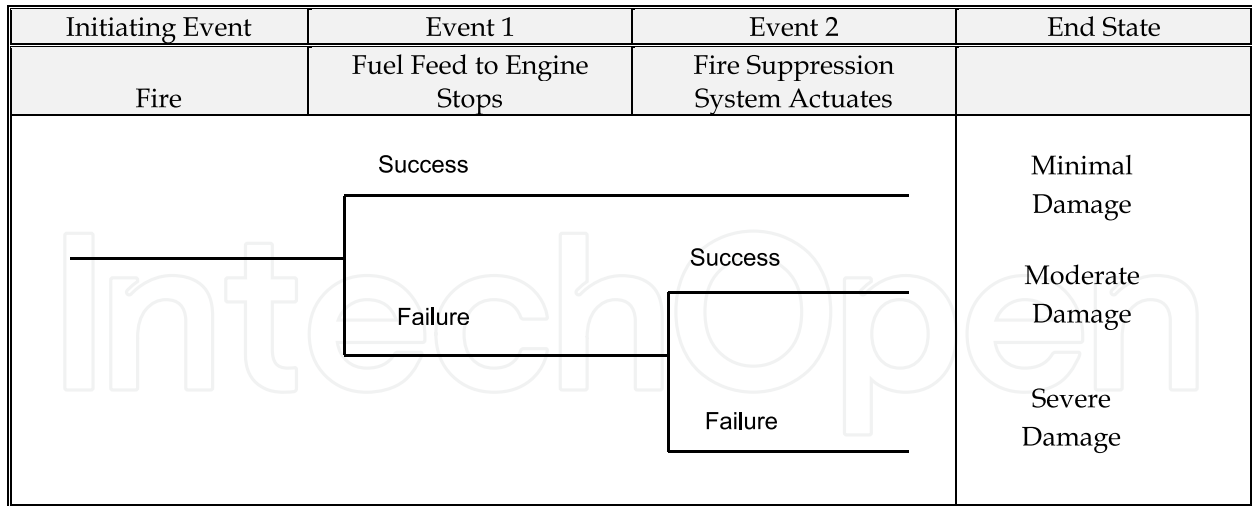


Fig. 1. Event Tree

Event	Description	Possible Outcomes
Fire	This is the initiating event.	
Fuel feed is stopped	The lack of fuel causes the fire to stop.	Success - the fire stops Failure - the fire continues
Fire suppression system actuates	The fire suppression system detects the fire and it actuates.	Success - system actuates and controls the fire Failure - fire destroys the engine

Table 6. Accident Sequence

Event	Description	Possible Outcomes	Probability
Fire	This is the initiating event.		0.001
Fuel feed stops	The automatic controls stops fuel flow to the engine	Success - stopping fuel flow stops fire Failure - fire continues	0.999 0.001
Fire suppression system actuates	The fire suppression system detects the fire and it actuates.	Success - system actuates and controls the fire Failure - system fails to control the fire	0.99 0.01

Table 7. Event Sequence with Probabilities

This result of this analysis tells us that the probability derived for a fire in which the fuel feed system stops fuel supply to engine actuates and the consequence in minimal damage is approximately 1/1000 or 1×10^{-3} . The probability derived for a fire in which the fuel feed system fails to actuate, but the fire suppression system successfully extinguishes the fire and there is only moderate damage is 1×10^{-6} or 1×10^{-6} . Finally, the probability that a fire occurs and both the fuel feed system fails and fire suppression system fails and severe damage occurs is 1×10^{-8} or 5×10^{-8} .

Initiating Event	Event 1	Event 2	End State	Path Probability
Fire	The automatic controls stops fuel flow to the engine	Fire Suppression System Actuates		
Success			Minimal Damage	$0.001 \times 0.999 = 0.00099$ or 0.001
Failure		Success	Moderate Damage	$0.001 \times 0.001 \times 0.99 = 1 \times 10^{-6}$
Failure		Failure	Severe Damage	$0.001 \times 0.001 \times 0.01 = 1 \times 10^{-8}$

Fig. 2. Event Tree with Path Probabilities

This approach is considered inductive in nature. Meaning the system uses forward logic. A fault tree, discussed below, is considered deductive because usually the analyst starts at the top event and works down to the initiating event. In complex risk analyses event trees are used to describe the major events in the accident sequence and each event can then be further analyzed using a technique most likely being a fault tree (Modarres, M., 2006).

As indicated, the fault tree begins at the end, so to speak. This top-down approach starts by supposing that an accident takes place (Vesely, William; et. al., 2002). It then considers the possible direct causes that could lead to this accident. Next it looks for the origins of these causes. Finally it looks for ways to avoid these origins and causes. The resulting diagram resembles a tree, thus the name.

Fault trees can also be used to model success paths as well. In this regard they are modeled with the success at the top and the basic events are the entry level success that put the system on the path to success.

The goal of fault tree construction is to model the system conditions that can result in the undesired event. Before construction of a fault tree, the analyst must acquire a thorough understanding of the system. A system description should be part of the analysis. The analysis must be bounded, both spatially and temporally, in order to define a beginning and

endpoint for the analysis. The fault tree is a model that graphically and logically represents the various combinations of possible events, both fault and normal, occurring in a system leading to the top event. The term “event” denotes a dynamic change of state that occurs to a system element. System elements include hardware, software, human, and environmental factors (Vesely, William; et. al. 2002).

Table 8 shows the most common fault tree symbols. These symbols represent specific types of fault and normal events in fault tree analysis. In many simple trees only the Basic Event, Undeveloped Event and Output Event are used.

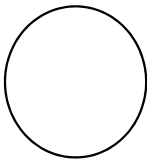
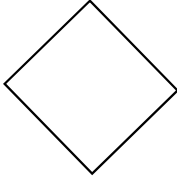

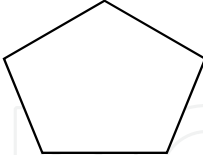
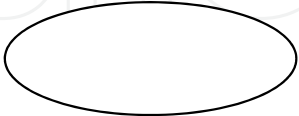
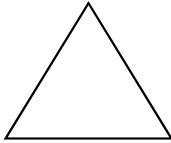
Symbol Name	Symbol	Description
Basic Event		A basic initiating fault (or failure event).
Undeveloped Event		An event which is no further developed. It is a basic event that does not need further resolution.
Output Event		An event that is dependent on the logic of the input events.
External Event (House Event)		An event that is normally expected to occur. In general, these events can be set to occur or not occur,
Conditioning Event		A specific condition or restriction that can apply to any gate.
Transfer		Indicates a transfer to a sub tree or continuation to another location.

Table 8. Common Fault Tree Symbols

Events representing failures of equipment or humans (components) can be divided into failures and faults. A component failure is a malfunction that requires the component to be repaired before it can successfully function again. For example, when a turbine blade in an engine breaks, it is classified as a component failure. A component fault is a malfunction that will “heal” itself once the condition causing the malfunction is corrected. An example of a component fault is a switch whose contacts fail to operate because they are wet. Once they are dried, they will operate properly.

Output events include the top event, or ultimate outcome, and intermediate events, usually groupings of events. Basic events are used at the ends of branches since they are events that cannot be further analyzed. A basic event cannot be broken down without losing its identity. The undeveloped event is also used only at the ends of event branches. The undeveloped event represents an event that is not further analyzed either because there is insufficient data to analyze or because it has no importance to the analysis.

Logic gates are used to connect events. The two fundamental gates are the “AND” and “OR” gates. Table 9 describes the gate functions and also provides insight to their applicability.

There are four steps to performing a Fault Tree Analysis:

1. Defining the problem
2. Constructing the fault tree
3. Analyzing the fault tree qualitatively
4. Documenting the results

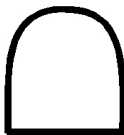

Description	Symbol
AND Gate. The AND gate indicates that the output occurs if and only if all of the input events occur.	
OR Gate. The OR gate indicates that the output occurs if and only if at least one of the input events occur.	

Table 9. Logic Gates

A top event and boundary conditions must be determined when defining the problem. Boundary conditions include:

- System physical boundaries
- Level of resolution
- Initial Conditions
- Not allowed events
- Existing Conditions
- Other Assumptions

Top events should be precisely defined for the system being evaluated. A poorly defined top event can lead to an inefficient analysis.

Construction begins at the top event and continues, level by level, until all fault events have been broken into their basic events. Several basic rules have been developed to promote consistency and completeness in the fault tree construction process. These rules, as listed in Table 10, are used to ensure systematic fault tree construction (American Institute of Chemical Engineers, 1992).

Item	Description
Fault Tree Statements	Write the statements that are entered in the event boxes and circles as malfunctions. State precisely a description of the component and the failure mode of the component. The “where” and “what” portions specify the equipment and its relevant failed state. The “why” condition describes the state of the system with respect to the equipment, thus telling why the equipment state is considered a fault.
Fault Event Evaluation	When evaluating a fault event, ask the question “Can this fault consist of an equipment failure?” If the answer is yes, classify the fault event as a “state-of-equipment” fault. If the answer is no, classify the fault event as a “state-of-system” fault. This classification aids in the continued development of the fault event.
No Miracles	If the normal functioning of equipment propagates a fault sequence, assume that the equipment functions normally. Never assume that the miraculous and totally unexpected failure of some equipment interrupts or prevents an accident from occurring.
Complete Each Gate	All inputs to a particular gate should be completely defined before further analysis of any other gate. For simple models, the fault tree should be completed in levels, and each level should be completed before beginning the next level. This rule may be unwieldy when constructing a large fault tree.
No Gate-to-Gate	Gate inputs should be properly defined fault events; that is, gates should not be directly connected to other gates. Shortcutting the fault tree development leads to confusion because the outputs of the gate are not specified.

Table 10. Rules for Constructing Fault Trees

Many times it is difficult to identify all of the possible combinations of failures that may lead to an accident by directly looking at the fault tree. One method for determining these failure paths is the development of “minimal cut sets.” Minimal cut sets are all of the combinations of failures that can result in the top event. The cut sets are useful for ranking the ways the accident may occur and are useful for quantifying the events, if the data is available. Large fault trees require computer analysis to derive the minimal cut sets, but some basic steps can be applied for simpler fault trees:

1. Uniquely identify all gates and events in the fault tree.

2. If a basic event appears more than once, it must be labeled with the same identifier each time. Resolve all gates into basic events.
3. Gates are resolved by placing them in a matrix with their events.
4. Remove duplicate events within each set of basic events identified.
5. Delete all supersets that appear in the sets of basic events.

By evaluating the minimal cut sets, an analyst may efficiently evaluate areas for improved system safety. The analyst should provide a description of the system analyzed, as well as a discussion of the problem definition, a list of the assumptions, the fault tree model(s), lists of minimal cut sets, and an evaluation of the significance of the minimal cut sets. Any recommendations should also be presented. An example fault tree for the engine fire example is shown in Figure 3.

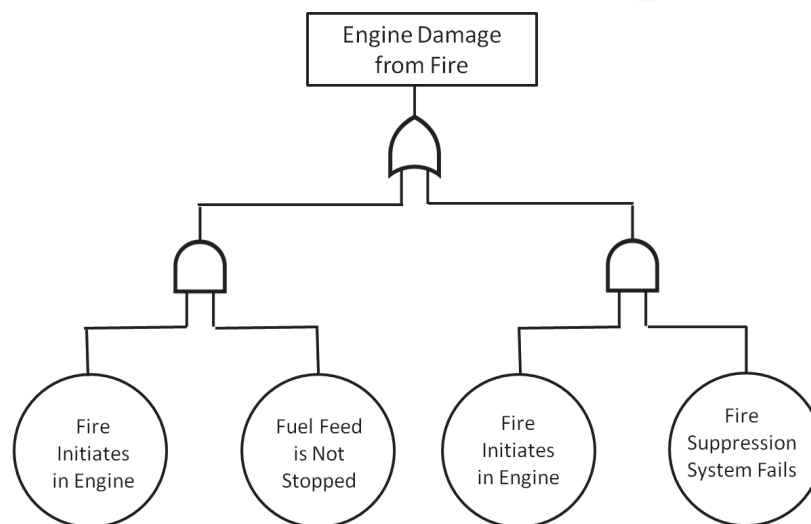


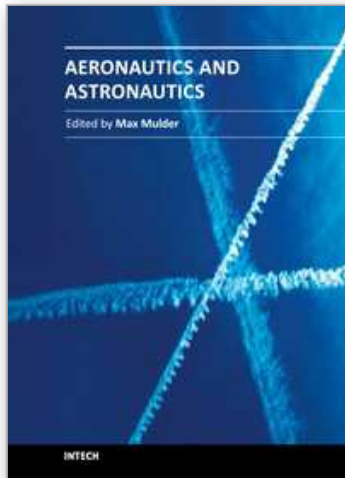
Fig. 3. Example Fault Tree

4. Summary

This chapter discussed how common risk assessment techniques could be used to perform risk assessments of aviation related activities. As discussed in the very beginning paragraph of this chapter, Ostrom and Wilhelmsen (2011) discuss in depth how to use risk assessment techniques to analyze a wide variety of systems, tasks, and activities.

5. References

- American Institute of Chemical Engineers., (1992) *Guidelines for Hazard Evaluation Procedures*, New York.
- Mil Std 882B, C (1984, 1993)
- Modarres, M., (2006) *Risk Analysis in Engineering: Techniques, Tools, and Trends*, CRC Press; 1 edition, ISBN: 1574447947
- Ostrom, L. & Wilhelmsen, C., (Summer 2011) *Risk Assessment Tools and techniques and Their Application, in Process*.
- Vesely, William; et. al. (2002) (pdf). *Fault Tree Handbook with Aerospace Applications*. National Aeronautics and Space Administration.
<http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf>. Retrieved 2010-01-17.



Aeronautics and Astronautics

Edited by Prof. Max Mulder

ISBN 978-953-307-473-3

Hard cover, 610 pages

Publisher InTech

Published online 12, September, 2011

Published in print edition September, 2011

In its first centennial, aerospace has matured from a pioneering activity to an indispensable enabler of our daily life activities. In the next twenty to thirty years, aerospace will face a tremendous challenge - the development of flying objects that do not depend on fossil fuels. The twenty-three chapters in this book capture some of the new technologies and methods that are currently being developed to enable sustainable air transport and space flight. It clearly illustrates the multi-disciplinary character of aerospace engineering, and the fact that the challenges of air transportation and space missions continue to call for the most innovative solutions and daring concepts.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Lee T. Ostrom and Cheryl A. Wilhelmsen (2011). Developing Risk Models for Aviation Inspection and Maintenance Tasks, *Aeronautics and Astronautics*, Prof. Max Mulder (Ed.), ISBN: 978-953-307-473-3, InTech, Available from: <http://www.intechopen.com/books/aeronautics-and-astronautics/developing-risk-models-for-aviation-inspection-and-maintenance-tasks>

INTECH
open science | open minds

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License](https://creativecommons.org/licenses/by-nc-sa/3.0/), which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.

IntechOpen

IntechOpen