Université d'Ottawa | University of Ottawa

GNG1103 – Engineering Design
GNG1503 – Génie de la conception

Failures and Iterative Testing

Presented by: Emmanuel Bouendeu

https://www.apicasystem.com/wp-content/uploads/2015/08/failurepoints.png

Université d'Ottawa | University of Ottawa

Agenda

- Quiz 3
- Reminders
- **Review Questions**
- **Failures et Criticality**
  - Detection, prediction et prevention
- **Testing with Prototypes**
  - Strategies of iterative testing
- **Uncertainty and Risk**
  - Design Margin
  - FMEA

Université d'Ottawa | University of Ottawa

Reminders

- **Lab 8**: Electronic Soldering + Laser Cutting: This week
- **Project Plan** (Week 4,6,**8**,10): Weekly review & update
- **Presentation for Client Meet 3** (Submission March 02) : March 04
- **Deliverable G** (Prototype 2 & Customer Feedback): March 08
- **Deliverable H** (Prototype 3 & Customer Feedback): March 22
- What is your summary of **Lecture 13**?
  - Modeling and importance
  - Modeling techniques & when to apply them
  - Elements to understand when modeling
  - Attributes of a good modeling
  - FEA principle

Université d'Ottawa | University of Ottawa

Review Questions

1. **Handling failures** takes into account three or four **considerations**. List these considerations.
2. Calculate the **probability of failure and operation** of a system composed of two subsystems A and B in series with failure probabilities 0.1 and 0.2 respectively.
3. What are the two ways of **handling failure uncertainty and risk** when failures cannot be eliminated by prototype testing?
4. In the table below, indicate whether the statements are true or false.

#	Statement	True/False
1	The level severity, occurrence and detection defines the **RPN**.	
2	**FMEA** is a technique to manage projects and risks.	
3	Component failure can always occur with certain probability.	
4	Building and testing prototypes can help predict failures.	
5	With a RPN value of 130, a corrective action is required.	

genie.uOttawa.ca | engineering.uOttawa.ca

uOttawa

Université d'Ottawa | University of Ottawa

Failures and Criticality

- System **Failure is normal and expected**
  - Q: Are there certain types of system or design which must not fail?
  - Q: If so, **what** should be done differently when designing such products or services?
- **Failure***: Omission of occurrence or **performance**; a state of inability to perform a normal function; a fracturing or **giving way** under stress
- **Criticality** **: Turning point or specially important juncture; crucial, decisive; indispensable, vital

* https://www.merriam-webster.com/dictionary/failure
** https://www.merriam-webster.com/dictionary/critical

Image: www.austingunter.com/wp-content/uploads/2012/11/failure-poster.jpg

uOttawa

Université d'Ottawa | University of Ottawa

Handling Critical Failures

- **Detection**: Critical failures must be identified, if and when they occur, as having occurred
- **Prevention**: Using different strategies, failures are stopped from occurring …
  - Since we have accepted that this assumption is often **not** realistic, system **recovery** is an alternative, usually achieved by adding component **redundancy** to cope with those failures
  - Q: What kinds of failures do we need to "prevent"/ protect against?
- **Prediction**: If a failure cannot be detected or prevented, then some kind of warning of imminent failure is required, allowing recovery techniques to be used
  - Q: *How* can failures be predicted?

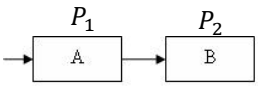
Image: https://en.wikipedia.org/wiki/Montparnasse_derailment

uOttawa

Université d'Ottawa | University of Ottawa

Protecting and Recovering Using Redundancy

Probability of operation and failure with components in series



*Components in **SERIES***

$$P_o = (1 - P_1)(1 - P_2$$

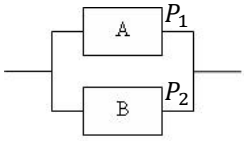
P_o: *Probability of operation*

$P_{1,2}$: *Probability of failure of A, B*

System operates provided **both** components do **not** fail. With independent component failures, this operation probability is: $(1\text{-}p)^2$ and the probability of system failure is therefore: $1 - (1\text{-}p)^2 = \mathbf{2p - p^2}$

A: Prob. (system failure) = $\mathbf{2p - p^2}$
= **0.19** (p=0.1)

Probability of operation and failure with components in parallel



*Components in **PARALLEL***

$$P_o = 1 - P_1 P_2$$

System failure occurs when both components fail, which has a probability of $\mathbf{p^2}$ (assuming independent component failures)

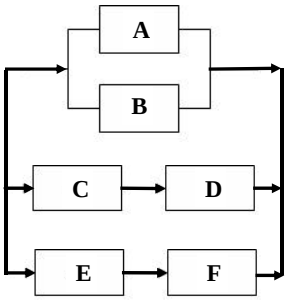
A: Prob. (system failure) = $\mathbf{p^2}$
= **0.01** (p=0.1)

Images: https://en.wikibooks.org/wiki/Computer_Systems_Engineering/Reliability_models

uOttawa

Université d'Ottawa | University of Ottawa

Exercise: Redundancy Calculations (5 minutes)



*Components in both **SERIES** and **PARALLEL***

Probability of ***independent*** events A and B **both** occurring is **P(A,B) = P(A) • P(B)**
Probability of ***mutually exclusive*** events A and B occurring (i.e. they can ***never*** *both* occur) is **P(A ⊕ B) = P(A) + P(B)**

Prob.(top arm fails) = p^2
Prob.(middle arm fails) = $2p - p^2$
Prob.(bottom arm fails) = $2p - p^2$

System fails if *all three* of these arms fail
Prob.(system failure) = $p^2 \cdot (2p - p^2) \cdot (2p - p^2)$
= $p^6 - 4p^5 + 4p^4$

A: Prob. (system failure) = $\mathbf{p^6 - 4p^5 + 4p^4}$
= **0.00036** (p=0.1)

Q: Assume that the probability of a single component failing is p=0.1 what is the probability of system failure?

Images: https://en.wikibooks.org/wiki/Computer_Systems_Engineering/Reliability_models

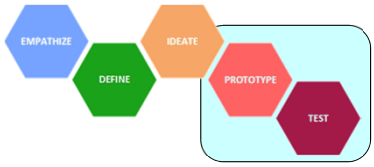
uOttawa

Predicting Failures

- To predict system failures, we can:
  - Model and measure component reliability
  - Analyze system structure and the interconnection dependencies for these components to determine the effects of component failures on the system
  - Analyze the root cause for failures that already happened
  - Build **prototypes** of part (*focussed*) or all (*comprehensive*) of the system in question

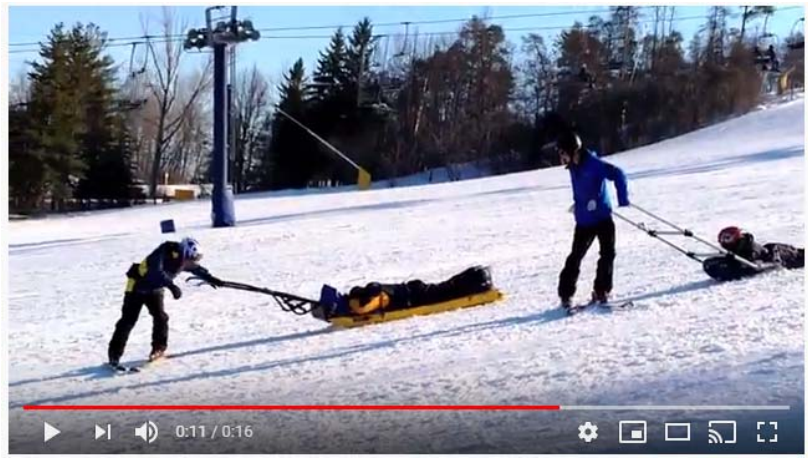
Q: How can we analyze or measure the reliability of less mechanical things like software designs or human operators of our designs?

Testing With Prototypes



- In previous lectures, we used prototypes to:
  - Gain understanding or insight about the design problem
  - Communicate with users
  - Generate Ideas
- Prototypes can *also* be used to test designs for the three defined kinds of potential failure:
  - Performance level failure (stopping distance)
  - Functional failure (brake of the rescue device)
  - Stress-induced failure (Brake at – 45ºC)

Case Study: Testing Stopping Distance



https://youtu.be/DxK-_wqgtjI

Testing Process: Performance Level Failures

- Determine the required and desired level of performance for the design (comprehensive) or portion of the design (focussed)
- Define a test to measure what level of performance the design can achieve (e.g. case study toboggan braking mechanism use of stopping distance)
  - It may only be necessary to determine whether the design can achieve the required level of performance or not, depending on the type of performance specification

Testing Process: Functional Failures

- Determine required performance attributes or features and desired functions to be verified
- Verify functionality
  - Verify that specific "critical" features can actually be realized at all (i.e. that success is actually achievable)
  - Measure the specific test conditions where correct functional operation stops. If these test conditions are *outside* of the required operating conditions, then functional failures may be acceptable
  - Verify specific functionality at the boundary cases or the extremes of the operating conditions. Highly-Accelerated Lifetime (HALT) tests use these conditions or even more severe ones to predict reliability and failure modes

Testing Process: Stress-Induced Failures

- Determine the specific extreme test conditions where failures occur
  - "Testing to failure" methods can be used, where the test condition parameters required for failure are recorded
  - Sometimes, historical data can be used to help determine the kinds of parameters to vary or else an understanding of failure mechanisms can help to determine the parameters to vary

Testing Steps With Prototypes (Planning)

Planning + Execution

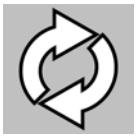
- Scientific method attempts to prove or disprove a hypothesis with some level of confidence
  1. Define the testing objectives and the type of prototype to be used (e.g. focussed or comprehensive, analytical or physical)
  2. Define the level of fidelity for the model or prototype
  3. Make the required assumptions and simplifications
  4. Define and plan the execution of the tests, making the required trade-offs between the usefulness of the results and the time and money required for the testing

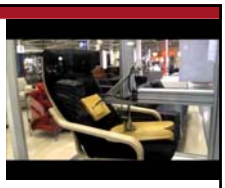
Testing Steps With Prototypes (Execution)

5. Execute the tests
   - Observe and record all results carefully
   - Watch out for systematic errors and experimenter bias!
   - Investigate all "surprise" results and determine the cause and whether this is a modeling artifact or not
6. Analyze and interpret all recorded results
   - Watch out for numerical round-off errors, faulty assumptions or improper extrapolation or interpolation
   - Consider the use of data analytics and determine if it is possible to access other sources of test data for comparison purposes

Université d'Ottawa | University of Ottawa

Iterative Prototype Testing





- When testing iteratively, the following can be varied:
  - Prototype (type, level of detail, etc.)
  - Tests (test cases, the number of test cases, …)
  - Test conditions (normal or extreme operating conditions, specific environmental conditions kept constant or varied systematically)
- Different combinations of variations are possible, such as:
  - Same prototype under different test conditions
  - Same prototype under same conditions multiple times (e.g. repetitive chair seating pressure test at IKEA)
  - Same conditions and same tests with different instances of the same prototype to measure or compare performance variation (e.g. "**A/B test mode**" used with two identical New Zealand boats)

Université d'Ottawa | University of Ottawa

Iterative Prototype Testing

- The following needs to be determined:
  - How many different prototypes are required? A sequence of prototypes could be used, each building on the results of previous ones or using increasing levels of detail or complexity
  - What different test cases are required? **Planning** ahead and **prioritizing** helps ensure that test cases are not missed or duplicated unnecessarily
  - How many instances of each prototype are required?
  - What test conditions are varied or kept constant with each iteration and how representative are these test conditions?

genie.uOttawa.ca | engineering.uOttawa.ca

Uncertainty and Risk

- Not all failures can be determined and not all failures are understood or are predictable
  - Initial prototypes or an initial prototype testing strategy can be redefined, adapted or evolved, but still may not cover all cases
- "*What if*" types of analysis can help cover cases when things do **not** turn out exactly as expected or when things are **not** understood well enough yet (i.e. users exist with different usability requirements)?
- We need a way to handle uncertainties and/or a way to quantify risks that we must take, if we can't reduce or eliminate risk by testing with prototypes

Image: http://www.riskmanagementmonitor.com/wp-content/uploads/2011/03/balancing-risk.jpgImage:

Adding Design Margin

- One solution is to improve the design significantly so that failures in the level of performance or failures in functionality or even stress-related failures are less likely
  - Design is changed so that it *more than meets* or goes well beyond the basic required performance levels
  - Such performance improvement usually comes at a cost and it is **not** possible to have enough design margin to eliminate **all** uncertainties and risks
  - A "thought experiment" analysis technique called Failure Mode and Effects Analysis (FMEA) is another way of managing risk and uncertainty of system failure.

Image: https://s-media-cache-ak0.pinimg.com/564x/b9/67/d4/b967d4b74cd38ef2637e4110fe69605d.jpg

Université d'Ottawa | University of Ottawa

Course Attendance: Registration

- Use your smartphone or laptop to **register/notify** your attendance in this lecture
- Allow **geo location** in the attendance site
- Accept **cookies** from third parties applications
- Log in using only your **Uottawa** account at the link below
  https://attendance.azarm.ca/attendancerecord/gng1103f
- Your attendance must be registered only **during the lecture** and at the **time specified by the professor**
- You can also use the **QR code** below, to register quickly

genie.uOttawa.ca | engineering.uOttawa.ca

uOttawa

Université d'Ottawa | University of Ottawa

FMEA Analysis

- For each design component:
  1. Identify failure modes
  2. Determine the possible effects or consequences of the failure
  3. Assess potential severity of the effect
  4. Identify failure causes (and take action!)
  5. Estimate probability of occurrence
  6. Assess likelihood of failure detection

Image: https://sciencenotes.files.wordpress.com/2008/06/car-bike-crash-mexico-crop.jpg

genie.uOttawa.ca | engineering.uOttawa.ca

uOttawa

Université d'Ottawa | University of Ottawa

FMEA Analysis: Identify Modes

- Q: "How could the component or system fail?"
  - List potential failure modes for the particular part or function
  - **Assume** the failure could occur, *however unlikely*

(5 mins) Exercise (Ski Hill Case Study):

- Do a Failure Mode Identification for the Ski Hill Rescue Toboggan handle

Université d'Ottawa | University of Ottawa

Ski Hill Case Study: Toboggan Handle Failure Modes

- Handle can:
  1. Break/fracture
  2. Bend
  3. *Freeze or remain seized in one position*
  4. Rust
  5. Become rough enough to damage gloves or winter clothing or ski lifts
  6. Be too cold for use without gloves (fine motor skills required?)
  7. Freeze itself or "get stuck" on ski patroller's mitts
  8. Pinch operators body or clothing during operation….

genie.uOttawa.ca | engineering.uOttawa.ca

Université d'Ottawa | University of Ottawa

FMEA Analysis: Effects

FM-1	Effect 1-1
	Effect 1-2
	Effect 1-3
FM-2	Effect 2-1
	Effect 2-2

- For each failure mode, identify the potential downstream consequences (the **Effects**)
- Brainstorm or use other methods to identify failure modes and effects

(5 mins) Exercise (Ski Hill Case Study):

- For ***one*** of the Ski Hill Rescue Toboggan handle failure modes, determine all of the potential effects

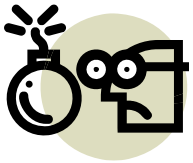
Université d'Ottawa | University of Ottawa

Ski Hill Case Study: Toboggan Handle Effects for "Stuck" Failure

- For "**3.** *Freeze or remain seized in one position*" failure mode, the potential downstream consequences are:
  - **3.1** Failure to stop or activate (e.g. frozen in the "off" position) causing injury to the user or injury to other ski-ers or injury to the ski patroller
  - **3.2** Failure to de-activate (e.g. frozen in the "on" position) making the device hard to move or transport and basically useless when a user needs to be carried down the hill
  - **3.3** Time wasted freeing up the mechanism, causing potential harm to the user because of unnecessary delays and preventing ski patrollers from serving other injured users
  - **3.4** The need to carry metal tools to free up the mechanism, which are potentially hazardous to the ski patroller

Université d'Ottawa | University of Ottawa

FMEA Analysis: Severity



- To analyze risk, first quantify the severity of the Effects
  - Assume that **all** Effects happen if the Failure Mode actually happens
  - Design and process changes can reduce these severity ratings

(3 mins) Exercise (Ski Hill Case Study):

- Quantify the severity of each of the effects listed in the previous slide using the severity table in the next slide

Université d'Ottawa | University of Ottawa

FMEA Analysis: Severity Table

Severity of Failure	Rank
Hazardous – No warning: Unsafe operation, without warning	10
Very high: Product inoperable; loss of primary function	8, 9
High: Product operable, but at a reduced level	6, 7
Low: Product operable; comfort or convenience items at reduced level	4, 5
Minor: Fit/finish, squeak/rattle don't conform; average customer notices	2, 3
No effect	1

Université d'Ottawa | University of Ottawa

Ski Hill Case Study: Toboggan Handle Effects Severity

Severity of Failure	Rank
Hazardous – No warning: Unsafe operation, without warning	10
Very high: Product inoperable; loss of primary function	8, 9
High: Product operable, but at a reduced level	6, 7
Low: Product operable; comfort or convenience items at reduced level	4, 5
Minor: Fit/finish, squeak/rattle don't conform; average customer notices	2, 3
No effect	1

- **3.1** Failure to stop or activate (frozen in "off" position)
  - **9:** depends on when and how the mechanism gets locked up
- **3.2** Failure to de-activate (frozen in the "on" position)
  - **7:** depends on whether toboggan can be moved or not
- **3.3** Time wasted freeing up the mechanism
  - **5:** Depends on frequency of occurrence
- **3.4** The need to carry metal tools to "free up" the mechanism
  - **4:** Depends on what tools are required to "free it up"

Université d'Ottawa | University of Ottawa

FMEA Analysis: Causes

- After Effects and Severity addressed, identify the **Causes** of the Failure Modes
- Causes of failure that result in a Failure Mode are **design deficiencies**

(5 mins) Exercise (Ski Hill Case Study):

- For the original failure mode, identify possible causes

Ski Hill Case Study: Toboggan Handle Causes for "Stuck" Failure

- For "**3.** *Freeze or remain seized in one position*" failure mode could be caused by:
  - Improper choice of material for mechanism
  - Too much friction
  - Poor design tolerances
  - Improper usage by ski patroller
  - Improper training of ski patrollers causing improper usage
  - Inadequate testing during the prototyping and test phase
  - *Unexpectedly harsh ice/snow conditions of some kind*
  - No rust protection or lubrication used or improper lubrication
  - Improper storage conditions
  - Poor maintenance practices (e.g. hosed down without drying)

FMEA Analysis: Occurrence

- Estimate failure occurrence factor (scale of 1-10)
  - Consider any fail-safe controls intended to prevent cause of failure
  - Consider the following two probabilities:
    1. probability that potential cause of failure will occur
    2. probability that once cause of failure occurs, it results in the indicated failure mode

(5 mins) Exercise (Ski Hill Case Study):

- Estimate the probability of the causes listed in the previous slide using the following ranking table

FMEA Analysis: Occurrence Factor Table

Occurrence Criteria	Rank
Very High – almost certain failure, in a major way	10
High – similar designs have failed in the past	7, 8, 9
Moderate – similar designs have occasional moderate failure rates	4, 5, 6
Low – similar designs have low failure rates	2,3
Remote - unreasonable to expect failure	1

Ski Hill Case Study: Occurrence Factor Table

Occurrence Criteria	Rank
Very High – almost certain failure, in a major way	10
High – similar designs have failed in the past	7, 8, 9
Moderate – similar designs have occasional moderate failure rates	4, 5, 6
Low – similar designs have low failure rates	2,3
Remote - unreasonable to expect failure	1

- "**3.** *Freeze or remain seized in one position*"
  - 3: Improper choice of material for mechanism
  - 8: Too much friction
  - 1: Poor design tolerances
  - 3: Improper usage by ski patroller
  - 2: Improper training of ski patrollers causing improper usage
  - 3: Inadequate testing during the prototyping and test phase
  - *6: Unexpectedly harsh ice/snow conditions of some kind*
  - 6: No rust protection or lubrication used or improper lubrication
  - 2: Improper storage conditions
  - 2: Poor maintenance practices (e.g. hosed down without drying)

Université d'Ottawa | University of Ottawa

FMEA Control Types

- FMEA method identifies three types of control, grouped according to purpose
  - **Type 1 Controls:** *prevent* Failure Mode from occurring, or reduce rate of occurrence (e.g. shear pin designed to fail to keep system from failing)
  - **Type 2 Controls:** *detect* Cause of Failure Mode and lead to corrective action(e.g. LED light to indicate when battery is low)
  - **Type 3 Controls:** *detect* Failure Mode *before* product reaches "customer" (e.g. 100% inspection)

Université d'Ottawa | University of Ottawa

FMEA Analysis: Detection

- Detection values associated with Control types
- Detection is a measure of:
  - Type 2 Controls to detect Causes of Failure
  - Type 3 Controls to detect subsequent Failure Modes
- High values indicate Lack of Detection
- Value of 1 does **not** imply 100% detection

(4 mins) Exercise (Ski Hill Case Study):

- Derive a type 2 control for one of the causes you have previously defined

genie.uOttawa.ca | engineering.uOttawa.ca

Université d'Ottawa | University of Ottawa

FMEA Analysis: Detection Table

Detection	Criteria: Likelihood of Detection	Rank
Absolute Uncertainty	Design Control does not detect, or there is no Design Control	10
Very Remote	Very remote chance Control will detect	9
Remote	Remote chance Control will detect	8
Very Low	Very low chance Control will detect	7
Low	Low chance Control will detect	6
Moderate	Moderate chance Control will detect	5
Moderately High	Mod. High chance Control will detect	4
High	High chance Control will detect	3
Very High	Very high chance Control will detect	2
Almost Certain	Control almost certain to detect	1

Université d'Ottawa | University of Ottawa

Ski Hill Case Study: Detection Table

Type 2 Controls: *detect* Cause of Failure Mode and lead to corrective action (e.g. LED light to indicate when battery is low)

Detection	Criteria: Likelihood of Detection	Rank
Absolute Uncertainty	Design Control does not detect, or there is no Design Control	10
Very Remote	Very remote chance Control will detect	9
Remote	Remote chance Control will detect	8
Very Low	Very low chance Control will detect	7
Low	Low chance Control will detect	6
Moderate	Moderate chance Control will detect	5
Moderately High	Mod. High chance Control will detect	4
High	High chance Control will detect	3
Very High	Very high chance Control will detect	2
Almost Certain	Control almost certain to detect	1

- "*Freeze or remain seized in one position*" - "*Unexpectedly harsh ice/snow conditions of some kind*"
  - Assume that a heater circuit is used to melt excess ice and snow if two electrodes are "connected" electrically through a resistive path formed by the excess ice and snow present on the handle
  - ⇨ The detection likelihood for this Type 2 control *depends on the conductivity of snow or ice*, which is OK if there are dissolved minerals in the mixture, but less so if the water is very pure
  - ⇨ "Moderate" or a detection likelihood of 5 seems about right!

genie.uOttawa.ca | engineering.uOttawa.ca

Université d'Ottawa | University of Ottawa

FMEA: Results

- **Risk Priority Number (RPN)**

$$RPN = S \times O \times D$$

S=Severity, **O**=(Probability of) Occurrence, **D**=Detection

- Once the RPN has been calculated for all failure modes, **take action** to reduce the RPN of the highest-risk item
  - Repeat the process until the *highest RPN value* is "satisfactory"

A corrective action is required when the value of RPN is higher than **130**

uOttawa

Université d'Ottawa | University of Ottawa

FMEA Document Template

	Failures			Cause		Detection		
Item	Potential Failure Mode	Effect	Severity	Casue	Occurance	Design control	Detection	RPN

uOttawa

Université d'Ottawa | University of Ottawa

FMEA Document Example

FMEA																
	Failure			Cause		Detection		Action			Action Results					
Item/ Function	Potential Failure Modes	Potential Effect of Failure	Severity	Potential Cause	Occurrence	Current Design Control	Detection	Risk Priority Number	Recommended Action	Responsibility	Action Taken	S	O	D	RPN
Deposit Ink	Too little Ink	No printing	7	Clogged Heads	4	None - instructions to user to regularly clean heads	3	**84**	design change to reduce chance of clogged heads	Ink head design team	More Robust Design	7	2	2	28
			7	Low Ink Levels	4	Ink Level light	1	**28**	None						
	Too much Ink	Can't read letters	8	Failure in Print head	2	Internal controls	3	**48**	Failure analysis	Ink head design team	Improved Control Algorithm	8	1	1	8

genie.uOttawa.ca | engineering.uOttawa.ca

uOttawa