



Aalto University  
School of Engineering

# Codes and Safety

*Prof. Kevin Otto  
Department of Mechanical Engineering*

*Kevin.Otto@aalto.fi*

# Pedagogy

**Lecture: Safety risks. Assessment. Reduce risks by design.**

**Team task: Complete a safety assessment of team product.**

- Making chart on risks related to the product, user and environment.
- Evaluate the severity of each risk.
- Team evaluates and comments another teams chart.

**Personal homework: Each student comes up with 3 ideas for reducing risks in your product. Describe with an annotated sketch.**

# Safety and Product Design

**Is your developed product safe?**

# EXERCISE

**Look at your product with your team.**

**What are ways a person can be harmed by your product?**

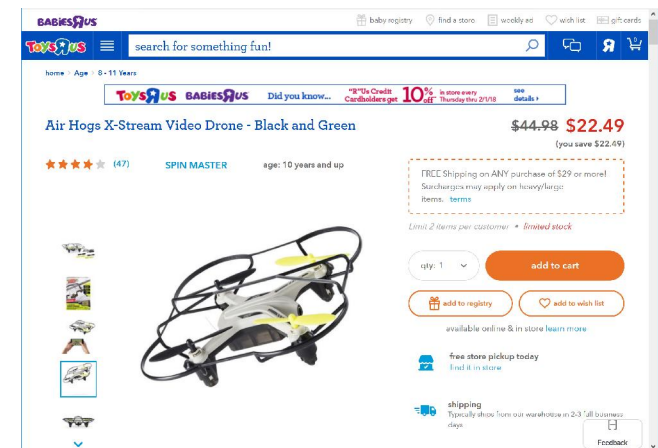
# Example – Toy Drone

Here is the PowerUp! drone.  
In 2013, it was a Kickstarter project.  
They raised \$1.2M  
They are now a company.  
\$49 on Amazon



# Example – Toy Drone

## AirHogz X-Stream Video Drone



# Example – Toy Drone



**Is this device safe?**

**Who is it intended for?**

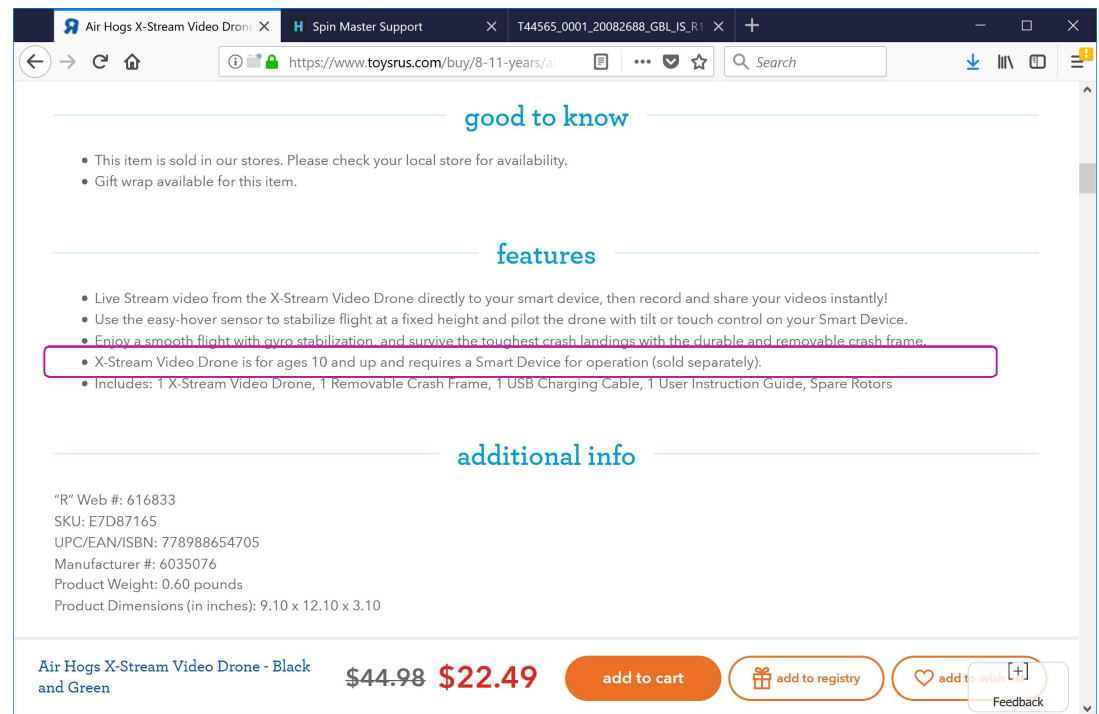
**How will they use it?**

**How can it be mis-used?**

**What should you provision into the design to prevent harm?**

# Example – Toy Drone

## AirHogz X-Stream Video Drone



good to know

- This item is sold in our stores. Please check your local store for availability.
- Gift wrap available for this item.

features

- Live Stream video from the X-Stream Video Drone directly to your smart device, then record and share your videos instantly!
- Use the easy-hover sensor to stabilize flight at a fixed height and pilot the drone with tilt or touch control on your Smart Device.
- Enjoy a smooth flight with gyro stabilization, and survive the toughest crash landings with the durable and removable crash frame.
- X-Stream Video Drone is for ages 10 and up and requires a Smart Device for operation (sold separately).
- Includes: 1 X-Stream Video Drone, 1 Removable Crash Frame, 1 USB Charging Cable, 1 User Instruction Guide, Spare Rotors

additional info

"R" Web #: 616833  
SKU: E7D87165  
UPC/EAN/ISBN: 778988654705  
Manufacturer #: 6035076  
Product Weight: 0.60 pounds  
Product Dimensions (in inches): 9.10 x 12.10 x 3.10

Air Hogs X-Stream Video Drone - Black and Green ~~\$44.98~~ **\$22.49** [add to cart](#) [add to registry](#) [add to wish list](#) [Feedback](#)



# Example – Drone

## PowerUp Drone



### Safety Information

Age Recommendation: Not for children under 14 years. This is not a toy. Keep these instructions for future reference - do not discard. Nevertheless, be sure to take the following precautions:

- Individuals with long hair should pull their hair back and fasten it with an elastic band. If hair becomes caught in the propeller, detach the propeller from the motor to release the hair.
- Never allow the propeller to get close to anyone's eyes.
- Before holding the airplane in your hand or making any adjustments to it, move the throttle slider in the smartphone app to minimum so that the propeller stops turning.

- Never hold propeller while throttle is raised. If propeller is jammed reduce throttle immediately. Resolve the reason before raising the throttle again.
- To avoid damaging the PowerUp Smart Module, always attach it to a paper airplane before activating the propeller.

### Charging Warnings

Read the following safety instructions and warnings before handling, charging or using the Li-ion battery.

**Caution:** All instructions and warnings must be followed exactly. Mishandling of Li-ion batteries can result in a fire, personal injury, and/or property damage.

- By handling, charging or using the included Li-ion battery, you assume all risks

associated with lithium batteries.

- If at any time the battery begins to balloon or swell, discontinue to use immediately. If charging or discharging, discontinue and disconnect. Continuing to use, charge or discharge a battery that is ballooning or swelling can result in fire.
- Always store the battery at room temperature in a dry area for best results.
- Always transport or temporarily store the battery in a temperature range of -20°C to 35°C. Do not store battery or aircraft in a car or direct sunlight. If stored in a hot car, the battery can be damaged or even catch fire.
- Always charge batteries away from flammable materials.
- Always inspect the battery before

charging and never charge damaged batteries.

- Always disconnect the battery after charging, and let the charger cool between charges.
- Always constantly monitor the temperature of the battery pack while charging.
- **Only use charger specifically designed to charge li-ion batteries.** Failure to charge the battery with a compatible charger may cause fire resulting in personal injury and/or property damage.
- Never cover warning labels with hook and loop strips.
- Never leave charging batteries unattended.

# Example – Toy Drone



**Is this device safe?**

Who is it intended for?

**How will a 10 year old use this?**

How can it be mis-used?

What should you provision into the design to prevent injury?

# Example – Toy Drone



# Example – Toy Drone

## AirHogz X-Stream Video Drone



Is this device safe?

How will a 10 year old use this?

**How can it be mis-used?**

What should you provision into the design to prevent injury?

# Example – Toy Drone



# Example – Toy Drone

**South China Morning Post** EDITION: INTERNATIONAL

## SOCIETY

### Drone 'flown by expat teen' hits Chinese toddler, causing facial injury


Police reported to be investigating a 14-year-old after the

**USA TODAY**

SPORTS LIFE MONEY TECH TRAVEL OPINION 14° CROSSWORDS WASHINGTON MORE

## What happens if a drone hits you in the head?

Doyle Rice, USA TODAY Published 4:37 p.m. ET April 28, 2017



What happens if a drone hits you in the head?

The Federal Aviation Administration (FAA) wants to know, so they conducted a study to understand and mitigate the risks of drones flying over people, and what happens if a drone loses connection to its pilot or just crashes to the ground.

**BBC** Sign in News Sport Weather Shop Earth Travel More Search

## NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts Health World News TV More

England Local News Regions Hereford & Worcester

### Toddler's eyeball sliced in half by drone propeller

© 26 November 2015



**LIVE Midlands Live: Breaking news and local stories**

9 minutes ago  
M42 fully reopens  
BBC News Travel

An 18-month-old boy has lost an eye after being hit by a drone family friend.


Oscar Webb's eye was sliced in half by a propeller after the operator lost control of the drone.

The toddler, from Stourport-on-Severn, Worcestershire, will need operations before he can have a prosthetic eye fitted.

It was the first drone injury Oscar's surgeon had seen, but she said "inevitable" there would be many more.

Mr Evans said: "It was up for about 60 seconds. As I brought it back just clipped the tree and span round."

"The next thing I know I've just heard my friend shriek and say 'Oscar' turned around and just saw blood and his baby on the floor crying."



### Mini Quadcopter Injury Nasty Deep Propeller cuts on Finger

16,538 views

118 24 SHARE

**alishanmao** Published on Jul 16, 2014

**SUBSCRIBE 251K**

Mini Quadcopters or all mutirotors are not toys. Please be very careful when flying and keep a safe distance. Make sure and double check to power off, or disarm motors when picking up or getting close to these little buggers. They bite hard and leave life long marks on your body.

SHOW MORE

A School of Engineering

# Example – Toy Drone



**Is this device safe?**

How will a 10 year old use this?

How can it be mis-used?

**What should you provision into the design to prevent injury?**

# Example – Toy Drone





# EXERCISE

**Who uses your product?**

**Make list and describe them.**

# Overview

Safety

Code of Ethics

Regulatory Compliance

Safety Assessment

Design for Safety



# Safety Assurance

**It is a designer's responsibility to ensure all products, services, processes or output of their work is safe.**

# Your Personal Code of Ethics

**When put in a professional situation,**

- What are you willing to develop? What not?
- What is your minimum safety factor before you refuse to let a design continue further?

# The ASME Code of Ethics



## The Fundamental Canons

1. Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties.
2. Engineers shall perform services only in the areas of their competence.
3. Engineers shall continue their professional development throughout their careers and shall provide opportunities for the professional and ethical development of those engineers under their supervision.
4. Engineers shall act in professional matters for each employer or client as faithful agents or trustees, and shall avoid conflicts of interest or the appearance of conflicts of interest.
5. Engineers shall build their professional reputation on the merit of their services and shall not compete unfairly with others.
6. Engineers shall associate only with reputable persons or organizations.
7. Engineers shall issue public statements only in an objective and truthful manner.
8. Engineers shall consider environmental impact in the performance of their professional duties.
9. Engineers shall consider sustainable development in the performance of their professional duties.

[https://www.asme.org/getmedia/9EB36017-FA98-477E-8A73-77B04B36D410/P157\\_Ethics.aspx](https://www.asme.org/getmedia/9EB36017-FA98-477E-8A73-77B04B36D410/P157_Ethics.aspx)

# The IEEE Code of Ethics



**We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:**

- 1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;**
- 2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;**
- 3. to be honest and realistic in stating claims or estimates based on available data;**
- 4. to reject bribery in all its forms;**
- 5. to improve understanding of technology; its appropriate application, & potential consequences;**
- 6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;**
- 7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;**
- 8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;**
- 9. to avoid injuring others, their property, reputation, or employment by false or malicious action;**
- 10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.**

<http://www.ieee.org/about/corporate/governance/p7-8.html>

# Safety Issues

**As a designer, it is your duty to yourself and to society that you fix any safety issue in your work.**

- Prevent harm
- Provide warnings about potential harm
- If there is newly found potential for harm, report it
- Fix it

# EXERCISE

**Recall who uses your product.**

**What are some features the designers put into the product to prevent harm?**



# Overview

Safety Assurance

Code of Ethics

**Regulatory Compliance**

**Safety Assessment**

**Design for Safety**



# Code Compliance

**Every region has government regulations and enforced codes which goods and services must comply**

- Failure to do so is illegal and breaking the law.

# How Much is the Designer's Responsibility?

Isn't any problem of safe use the user's fault?  
They bought it.

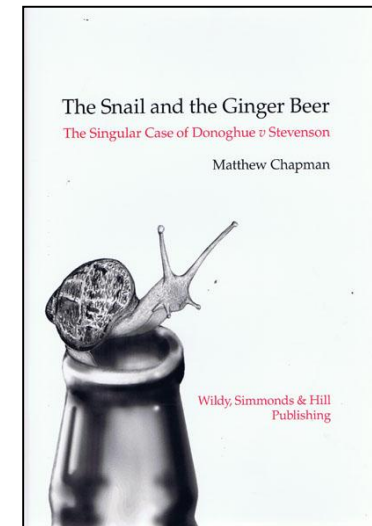


**Caveat Emptor.**

# The Law: Negligence

“Donoghue v Stevenson” defined the legal concept of *negligence*

- A product or service provider owes a *duty of care* against *reasonably foreseeable* product failures
- Not every possible scenario that one could imagine
- Instead, you owe a duty of care to ensure the product is safe over all reasonably foreseeable use cases



# The Law: Negligence

**“MacPherson v Buick Motors” expanded to define negligence of the manufacturer, not just the retailer, for defective products**

- A poorly designed and fabricated wooden spoke broke and the car collapsed.
- Buick was deemed liable, without sufficient due care in the design and manufacture



# Code Compliance

Every region has government regulations and enforced codes which goods and services must comply

- Failure to do so is illegal and breaking the law.
- Finland: TUKES



A screenshot of the TUKES website. The header includes the TUKES logo, a search bar, and navigation links for 'Text size', 'Sitemap', and language options ('Suomeksi', 'På svenska', 'Text version'). The main navigation menu includes 'Branches', 'For consumers', 'What's new', 'Information services', 'About Tukes', 'Contact details', and 'FINAS'. The 'Information releases' section lists several news items with dates and titles. A central banner features a blue background with diamond shapes and text about the Finnish Safety and Chemicals Agency (Tukes). To the right, there are sections for 'Dangerous products' (Tukes' Market Surveillance Register) and 'Chemical Products Surveillance' with a list of links. A 'Select branch' section at the bottom lists various product categories with arrows pointing to more information.

# Code Compliance

**Every region has government regulations and enforced codes which goods and services must comply**

- Failure to do so is illegal and breaking the law.



Use of hazardous substances in electrical equipment (Directive 2011/65/EU)  
Appliances burning gaseous fuels (Directive 2009/142/EC)  
Ecodesign requirements for energy-related products (Directive 2009/125/EC)  
Simple pressure vessels (Directive 2009/105/EC and Directive 2014/29/EU)  
Toys' safety (Directive 2009/48/EC)  
Electrical equipment voltage limits (Directive 2006/95/EC and 2014/35/EU)  
Machinery (Directive 2006/42/EC)  
Electromagnetic compatibility (Directive 2004/108/EC and 2014/30/EU)  
Measuring instruments (Directive 2004/22/EC and Directive 2014/32/EU)  
Cableway installations designed to carry persons (Directive 2000/9/EC)  
Radio and telecomm equipment (Directive 1999/5/EC and 2014/53/EU)

Active implantable medical devices (Directive 90/385/EEC)  
Medical devices (Directive 93/42/EEC)  
Pressure equipment (Directive 97/23/EC and Directive 2014/68/EU)  
Transportable Pressure equipment (Directive 2010/35/EU)  
Aerosol Dispensers (Directive 75/324/EEC)  
Lifts (Directive 95/16/EC and 2014/33/EU)  
Recreational craft (Directive 94/25/EC and Directive 2013/53/EU)  
Personal protective equipment (Directive 89/686/EEC)  
Marine equipment (Directive 96/98/EC and Directive 2014/90/EU)  
Noise emission by equipment for use outdoors (Directive 2000/14/EC)  
Emissions from non-road mobile machinery (Directive 97/68/EC)  
Energy labelling (Directive 2010/30/EU)

# GPS Directive

The GPSD is the EU law protecting consumer health and safety, and applies to all goods sold in the region that may be used by consumers (whether they are actually intended for consumers or not).



L 11/4	EN	Official Journal of the European Communities	15.1.2002
<b>DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMT AND OF THE COUNCIL of 3 December 2001 on general product safety (Text with EEA relevance)</b>			
THE EUROPEAN PARLIAMT AND THE COUNCIL OF THE EUROPEAN UNION,	(3)	In the absence of Community provisions, horizontal legislation of the Member States on product safety, imposing in particular a general obligation on economic operators to market only safe products, might differ in the level of protection afforded to consumers. Such disparities, and the absence of horizontal legislation in some Member States, would be liable to create barriers to trade and distortion of competition within the internal market.	
Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,			
Having regard to the proposal from the Commission (1),			
Having regard to the opinion of the Economic and Social Committee (2),			
Acting in accordance with the procedure referred to in Article 231 of the Treaty (3), in the light of the joint text approved by the Conciliation Committee on 2 August 2001,	(4)	In order to ensure a high level of consumer protection, the Community must contribute to protecting the health and safety of consumers. Horizontal Community legislation introducing a general product safety requirement, and containing provisions on the general obligations of producers and distributors, on the enforcement of Community product safety requirements and on rapid exchange of information and action at Community level in certain cases, should contribute to that aim.	
Whereas:			
(1) Under Article 16 of Council Directive 92/59/EEC of 29 June 1992 on general product safety (4), the Council was to decide, four years after the date set for the implementation of the said Directive, on the basis of a report of the Commission on the experience acquired, together with appropriate proposals, whether to adjust Directive 92/59/EEC. It is necessary to amend Directive 92/59/EEC in several respects, in order to complete, reinforce or clarify some of its provisions in the light of experience as well as new and relevant developments on consumer product safety, together with the changes made to the Treaty, especially in Articles 152 concerning public health and 153 concerning consumer protection, and in the light of the precautionary principle. Directive 92/59/EEC should therefore be recast in the interest of clarity. This recasting leaves the safety of services outside the scope of this Directive, since the Commission intends to identify the needs, possibilities and priorities for Community action on the safety of services and liability of service providers, with a view to presenting appropriate proposals.	(5) It is very difficult to adopt Community legislation for every product which exists or which may be developed: there is a need for a broad-based, legislative framework of a horizontal nature to deal with such products, and also to cover lacunae, in particular pending revision of the existing specific legislation, and to complement provisions in existing or forthcoming specific legislation, in particular with a view to ensuring a high level of protection of safety and health of consumers, as required by Article 95 of the Treaty.		
(2) It is important to adopt measures with the aim of improving the functioning of the internal market, comprising an area without internal frontiers in which the free movement of goods, persons, services and capital is assured.	(6)	It is therefore necessary to establish at Community level a general safety requirement for any product placed on the market, or otherwise supplied or made available to consumers, intended for consumers, or likely to be used by consumers under reasonably foreseeable conditions even if not intended for them. In all these cases the products under consideration can pose risks to the health and safety of consumers which must be prevented. Certain second-hand goods should nevertheless be excluded by their very nature.	
(3) OJ C 337 E, 28.11.2000, p. 169 and OJ L 184 E, 29.12.2000, p. 285.			
(4) OJ C 367, 20.12.2000, p. 14.			
(5) Opinion of the European Parliament of 15.11.2000 (OJ C 223, 28.11.2001, p. 154), Council Common Position of 12.2.2001 (OJ C 93, 23.2.2001, p. 24) and Decision of the European Parliament of 16.3.2001 (not yet published in the Official Journal), Decision of the European Parliament of 4.10.2001 and Council Decision of 27.9.2001.			
(6) OJ L 228, 11.8.1992, p. 24.	(7)	This Directive should apply to products irrespective of the selling techniques, including distance and electronic selling.	



# GPS Directive

Businesses should place on the market only products which are safe, and inform consumers of any risks associated with the products they supply.



L 11/4 EN Official Journal of the European Communities 15.1.2002

**DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMT AND OF THE COUNCIL**  
**of 3 December 2001**  
**on general product safety**  
(Text with EEA relevance)

THE EUROPEAN PARLIAMT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 231 of the Treaty (3), in the light of the joint text approved by the Conciliation Committee on 2 August 2001,

Whereas:

(1) Under Article 16 of Council Directive 92/59/EEC of 29 June 1992 on general product safety (4), the Council was to decide, four years after the date set for the implementation of the said Directive, on the basis of a report of the Commission on the experience acquired, together with appropriate proposals, whether to adjust Directive 92/59/EEC. It is necessary to amend Directive 92/59/EEC in several respects, in order to complete, reinforce or clarify some of its provisions in the light of experience as well as new and relevant developments on consumer product safety, together with the changes made to the Treaty, especially in Articles 152 concerning public health and 153 concerning consumer protection, and in the light of the precautionary principle. Directive 92/59/EEC should therefore be recast in the interest of clarity. This recasting leaves the safety of services outside the scope of this Directive, since the Commission intends to identify the needs, possibilities and priorities for Community action on the safety of services and liability of service providers, with a view to presenting appropriate proposals.

(2) It is important to adopt measures with the aim of improving the functioning of the internal market, comprising an area without internal frontiers in which the free movement of goods, persons, services and capital is assured.

(3) In the absence of Community provisions, horizontal legislation of the Member States on product safety, imposing in particular a general obligation on economic operators to market only safe products, might differ in the level of protection afforded to consumers. Such disparities, and the absence of horizontal legislation in some Member States, would be liable to create barriers to trade and distortion of competition within the internal market.

(4) In order to ensure a high level of consumer protection, the Community must contribute to protecting the health and safety of consumers. Horizontal Community legislation introducing a general product safety requirement, and containing provisions on the general obligations of producers and distributors, on the enforcement of Community product safety requirements and on rapid exchange of information and action at Community level in certain cases, should contribute to that aim.

(5) It is very difficult to adopt Community legislation for every product which exists or which may be developed: there is a need for a broad-based, legislative framework of a horizontal nature to deal with such products, and also to cover lacunae, in particular pending revision of the existing specific legislation, and to complement provisions in existing or forthcoming specific legislation, in particular with a view to ensuring a high level of protection of safety and health of consumers, as required by Article 95 of the Treaty.

(6) It is therefore necessary to establish at Community level a general safety requirement for any product placed on the market, or otherwise supplied or made available to consumers, intended for consumers, or likely to be used by consumers under reasonably foreseeable conditions even if not intended for them. In all these cases the products under consideration can pose risks to the health and safety of consumers which must be prevented. Certain second-hand goods should nevertheless be excluded by their very nature.

(7) This Directive should apply to products irrespective of the selling techniques, including distance and electronic selling.

(1) OJ C 337 E, 28.11.2000, p. 169 and OJ L 184 E, 29.12.2000, p. 285.  
(2) OJ C 367, 20.12.2000, p. 34.  
(3) Opinion of the European Parliament of 15.11.2000 (OJ C 223, 8.12.2001, p. 154), Council Common Position of 12.2.2001 (OJ C 93, 23.2.2001, p. 24) and Decision of the European Parliament of 16.3.2001 (not yet published in the Official Journal), Decision of the European Parliament of 4.10.2001 and Council Decision of 27.9.2001.  
(4) OJ L 228, 11.8.1992, p. 24.



# GPS Directive

Article 2, Paragraph b) of the Directive, defines this to be: “‘safe product’ shall mean any product which, under normal or reasonably foreseeable conditions of use including duration where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible to the product’s use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular

- i. The characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;
- ii. The effect of other products, where it is reasonably foreseeable that it will be issued with other products
- iii. The presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product
- iv. The categories of consumers at risk when using the product, in particular children and the elderly.”

When a manufacturer (producer) is working to demonstrate compliance with the GPSD, they must not only review the product with an eye to the characteristics of that product, but also with an eye on who might potentially be using those products. Paragraph 8 says “The safety of products should be assessed taking into consideration all of the relevant aspects, in particular the categories of consumers which can be vulnerable to the risks posed by products under consideration, in particular children and the elderly”



# GPS Directive

Producers shoulder most of the compliance burden with the General Product Safety Directive. Their obligations are sunned up in Article 3, paragraph 1 – “Producers shall be obliged to place only safe products on the market”. Within this activity they must:

- Provide consumers with relevant information that enables them to evaluate the potential risks (obvious or not) of a product during use or foreseeable use
- Be themselves informed of the risks their products may pose
- Notify the relevant authorities if a product they have supplied turns out to be dangerous.
- Take appropriate action relating to their unsafe product – including if appropriate a product recall that gives consumers appropriate compensation – such as refund or exchange.
- Provide on the product or packaging, the details of the Producer, the product reference and where applicable a batch number
- Where appropriate carry out sample testing of marketed products, keeping a register of safety complaints and the investigation of them.
- To co-operate with the competent authorities with regards to issues over dangerous products

# Safety Directives

**When selling in any country, it must be regulatory compliant**

**Compliance generally requires a safety analysis.**

**Designers must document that they analyzed the design to ensure it is adequately safe.**

**Designers must document that they analyzed the design to ensure the consumer has adequate warnings of risks.**

**That's the law. Failure to do so carries legal liability.**

# Overview

Safety Assurance

Code of Ethics

Regulatory Compliance

**Safety Assessment**

**Design for Safety**



# GPS Directive

When selling in the EU, it must be regulatory compliant  
GPS compliance requires a safety analysis.

A Design FMEA is a useful analysis procedure to

- Ensure it is adequately safe.
- Ensure the consumer has adequate warnings of risks.

# Think About Abuse!

Design for safety does not mean design to the most experienced, alert and best case operator.

Design for safety = Design for atypical use cases



How will the product be abused?

What reasonably foreseeable foolish situations will a person get into?

# Think About Abuse!

What reasonably foreseeable foolish situations will a person get into?

To consider this, you must define the atypical but foreseeable scenario.

- What is the user doing?
- Who are other actors in the scenario?
- What are other systems in the scenario?





# Define the User Environments

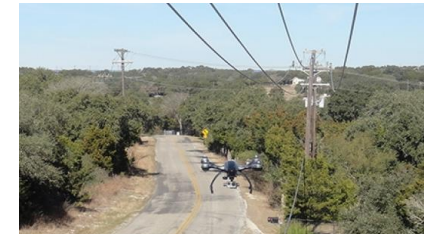
## Example: Drone Flying



**“The typical user environment is indoor or outdoor, with adult supervision, in benign weather, with separation of the drone.”**

# Define the User Environments

## Example: Drone Flying



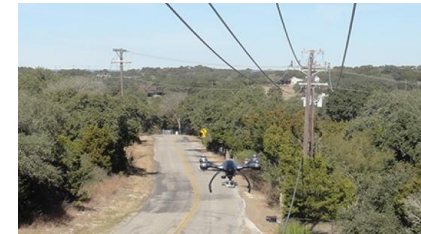
**“The typical user environment is indoor or outdoor, with adult supervision, in benign weather, with separation of the drone.”**

### **Atypical but foreseeable:**

- Crowded indoors. Living rooms. Basements. Bedrooms. Bathroom. Kitchen.
- Playgrounds, pools, sports areas, areas with unobservant others
- Hazardous areas. Power lines. Traffic.
- Poor weather conditions. Rain. Snow. Wind.

# Define the User Environments

## Example: Drone Flying



## Forseeable conditions to consider

- Crowded indoors. Appliances.
- Playground area with unobservant others
- Hazardous areas. Power lines. Traffic.
- Poor weather conditions. Rain. Snow. Wind.

# EXERCISE

**Recall who uses your product.**

**Describe their typical use case.**

- Where are they?
- What are they doing?
- What other actors and systems interact?

**Describe three atypical but foreseeable use cases.**

- Where are they?
- What are they doing?
- What other actors and systems interact?

# Definition of FMEA

## Failure Modes and Effects Analysis

### A structured approach for:

- Identifying the ways a system can fail at any level
  - *System-of-systems level*
  - *System level*
  - *Subsystems*
  - *Component level*
  - *Materials level*
- Quantifying the risk posed by each potential failure
- Prioritizing corrective action on potential high priority failure modes

# History of FMEA

**FMEA dates to 1949 with release of MIL-P 1629**

**Adopted for use by auto industry in late '70s**

- Quality problems, Product liability
- One of the quality design tools that helped the comeback of the auto industry from the plague of quality problems that affected them

**Now required standard work in automotive, aerospace and medical device industries**

# Types of Projects for FMEA

## System FMEA

- Focus on customer usage: what if they use it wrong?
- Focus on worst cases: what if the environment gets extreme?
- Focus on neighboring systems: what if the power fails? etc.
- Aids in evaluating test specifications

## Component FMEA

- Applied at the lowest level to improve design of basic system elements
- Evaluation of design failures relating to:
  - *Component function. How can the part fail?*
  - *Component failure's impact on the system. What happens?*

## Process FMEA

- Applied to production process, to provide the specified design
- Focus on manufacturing, assembly
  - *How can the process impart defects? What happens to the design?*

# General Observations

**Most failures don't happen because of a math error in your engineering calculations.**

**That analysis is often reviewed by others in peer or design reviews.**

**It's usually the things that aren't looked at that become problems.**

**The problem is the analysis you don't do!**





# Design FMEA Process Flowchart

1. Consider a use case.
2. Define the actors and systems in the use case.
3. Define their normal, safe operating conditions.
4. Start with the user.
5. Define Failure-Modes:  
How can it generate safety risks during the use case?
6. Repeat over actors and use cases
7. Rank the failure modes on severity and likelihood

**Mitigate high risk failure modes.**

# Systems – Example

## PowerUp Drone

### Forseeable Safety Use Case

- Flying indoors around many unaware persons

### Actors and Systems

- Pilot
- Drone
- Smartphone
- PowerUp App
- Indoor appliances, furniture
- Toddlers and impaired bystanders
- Walls, ceilings, hanging lamps



### Normal Safe Operation

- Pilot, drone and software fully functioning
- Bystanders watching, aware, and safe distance away

# Design FMEA Chart

System	Failure Modes	Effects	Severity	Occurrence

# Design FMEA

System	Failure Modes	Effects	Severity	Occurrence
<b>Pilot</b>	<b>Inept flying</b>	<b>Drone crashes into wall or ground</b>		
		<b>Drone crashes into electric appliance</b>		
		<b>Drone crashes into and injures unaware person</b>		
	<b>Drops phone</b>			
	<b>Becomes distracted</b>			
	<b>Flys plane behind a wall and cannot see drone</b>			

# High Risk Failure Modes

System	Failure Modes	Effects	Severity	Occurrence
Pilot	Drops phone	Drone crashes into wall or ground	Low	High
		Drone crashes into electric appliance	High	Med
		Drone crashes into and injures unaware person	High	High
	Becomes distracted	Drone crashes into wall or ground	Low	High
		Drone crashes into electric appliance	High	Med
		Drone crashes into and injures unaware person	High	High
	Flys plane behind a wall and cannot see drone	Drone crashes into wall or ground	Low	High
		Drone crashes into electric appliance	High	Med
		Drone crashes into and injures unaware person	High	High

# Design FMEA

System	Failure Modes	Effects	Severity	Occurrence
Drone	Comm fails	(SAME)		Low
	Circuit board fails	(SAME)		Low
	Powertrain fails	(SAME)		Low
	Battery drains	(SAME)		Medium
Smartphone	System software fails	(SAME)		Low
	Call comes in	(SAME)		High
	Slow and laggy	(SAME)		High
Flying App	App crashes	(SAME)		Low
	Comm fails	(SAME)		Low

# Design FMEA

System	Failure Modes	Effects	Severity	Occurrence
Unaware persons	Moving to a position the pilot is unaware	Drone crashes into and injures unaware person	High	High
	Gets close to drone and hair gets pulled into prop	Drone crashes into person	Medium	High
Walls, ceilings, hanging lamps	None	None	None	None
Electrical appliances	None	None	None	None

# Prioritized Failure Modes

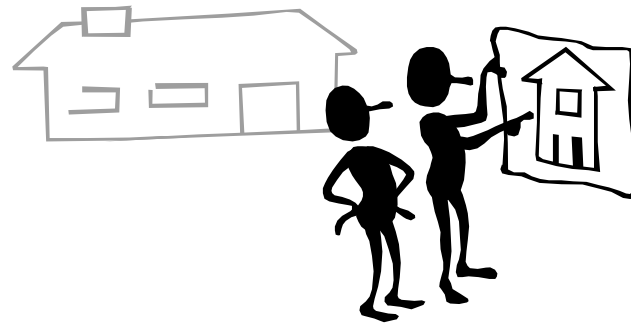
System	Failure Modes	Effects	Severity	Occurrence
Pilot	Dropping phone	Drone crashes into and injures unaware person	High	High
Pilot	Flys behind walls	Drone crashes into and injures unaware person	High	High
Pilot	Becomes distracted	Drone crashes into and injures unaware person	High	High
Unaware person	Moving to a position the pilot is unaware	Drone crashes into and injures unaware person	High	High
Smartphone	Call comes in	Drone crashes into and injures unaware person	High	High
Smartphone	Slow and laggy	Drone crashes into and injures unaware person	High	High



# Reduce High Risk Failure Modes

## Actions Needed for Risk Reduction

- Start with causes having highest RPN
- How would you eliminate them?
- If you can't eliminate them, how can we minimize them by making the system robust against failures?



# Overview

Safety Assurance

Code of Ethics

Regulatory Compliance

Safety Assessment

**Design for Safety**



# What Design Changes Help?

Demonstration test indicating it is ok

Parametric size changes

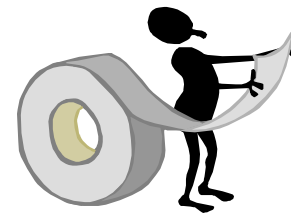
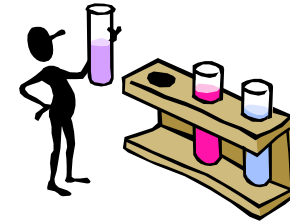
Redundancy

Different controls

Different components

Different element

Different function



# Three Possible Actions

**Eliminate the failure**

**Reduce the effect**

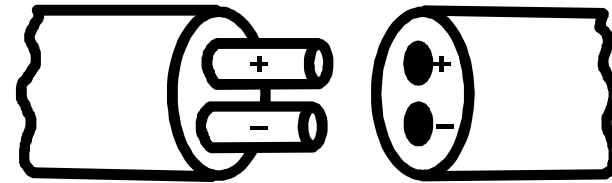
**Reduce the occurrence**

# What are the possible actions?

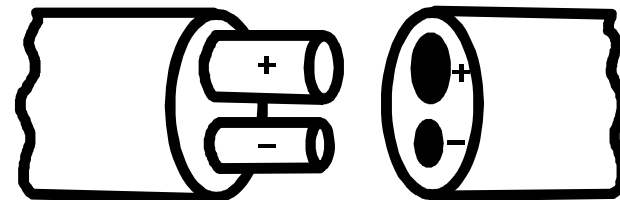
Eliminate the failure

Reduce the effect

Reduce the occurrence



Weak Design



Mistake-proofed Design

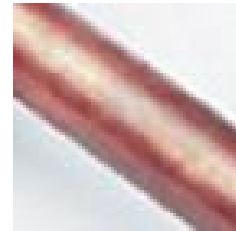
Mistake proof the design so the failure cannot happen

# What are the possible actions?

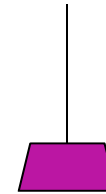
Eliminate the failure

Reduce the effect

Reduce the occurrence



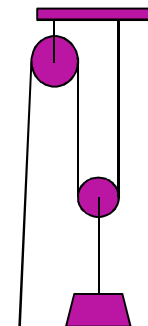
Too hot



Too heavy



Reduced hot



Reduced Weight

# What are the possible actions?

Eliminate the failure

Reduce the effect

Reduce the occurrence



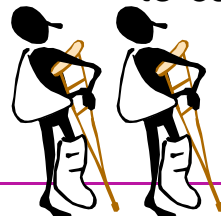
Single action



Redundant action

It will still happen.  
Severe failures need happen only once  
to cause a severe problem.

Not recommended  
as only action



# Design Mitigations

What can you do the design out these failure mode effects?

System	Failure Modes	Effects	Design Mitigation
Pilot	Dropping phone	Drone crashes into and injures unaware person	Soft bumpers. Propellor stop. Propellor guards. Low mass.
Pilot	Flys behind walls	Drone crashes into and injures unaware person	Soft bumpers. Propellor stop. Propellor guards. Low mass.
Pilot	Becomes distracted	Drone crashes into and injures unaware person	Soft bumpers. Propellor stop. Propellor guards. Low mass.
Unaware person	Moving to a position the pilot is unaware	Drone crashes into and injures unaware person	Soft bumpers. Propellor stop. Propellor guards. Low mass.
Smartphone	Call comes in	Drone crashes into and injures unaware person	Prevent calls during flying mode
Smartphone	Slow and laggy	Drone crashes into and injures unaware person	Prevent flying if loaded processor



# Provide Warnings of the Risks

For all reasonably foreseeable risks, provide consumers with information that enables them to assess potential risk

## Safety Information

Age Recommendation: Not for children under 14 years. This is not a toy. Keep these instructions for future reference - do not discard. Nevertheless, be sure to take the following precautions:

- Individuals with long hair should pull their hair back and fasten it with an elastic band. If hair becomes caught in the propeller, detach the propeller from the motor to release the hair.
- Never allow the propeller to get close to anyone's eyes.
- Before holding the airplane in your hand or making any adjustments to it, move the throttle slider in the smartphone app to minimum so that the propeller stops turning.

- Never hold propeller while throttle is raised. If propeller is jammed reduce throttle immediately. Resolve the reason before raising the throttle again.
- To avoid damaging the PowerUp Smart Module, always attach it to a paper airplane before activating the propeller.

## Charging Warnings

Read the following safety instructions and warnings before handling, charging or using the Li-ion battery.

**Caution:** All instructions and warnings must be followed exactly. Mishandling of Li-ion batteries can result in a fire, personal injury, and/or property damage.

- By handling, charging or using the included Li-ion battery, you assume all risks

- associated with lithium batteries.
- If at any time the battery begins to balloon or swell, discontinue to use immediately. If charging or discharging, discontinue and disconnect. Continuing to use, charge or discharge a battery that is ballooning or swelling can result in fire.
- Always store the battery at room temperature in a dry area for best results.
- Always transport or temporarily store the battery in a temperature range of -20°C to 35°C. Do not store battery or aircraft in a car or direct sunlight. If stored in a hot car, the battery can be damaged or even catch fire.
- Always charge batteries away from flammable materials.
- Always inspect the battery before

- charging and never charge damaged batteries.
- Always disconnect the battery after charging, and let the charger cool between charges.
- Always constantly monitor the temperature of the battery pack while charging.
- **Only use charger specifically designed to charge li-ion batteries.** Failure to charge the battery with a compatible charger may cause fire resulting in personal injury and/or property damage.
- Never cover warning labels with hook and loop strips.
- Never leave charging batteries unattended.

# Design for Safety

**It is the designer's responsibility for the safe operation of their provided products**

**Products must be safe against intended and reasonably foreseeable uses**

**Provide consumers with information that enables them to assess potential risk**

**Complete a Design FMEA on the product and its surroundings for the reasonable foreseeable uses cases**

**Mitigate risks by changing the design**

# Homework Assignment

## Complete a safety FMEA for your product

1. Define reasonably foreseeable use cases with safety concerns
2. Define the actors (other systems and persons) in the environment
3. For one use case of concern, fill out the FMEA table over all actors
4. Develop potential mitigations for each high risk failure mode

System	Failure Modes	Effects	Severity	Occurrence	Mitigation