



**FMEA**  
**(Lunch Presentation)**

**Accepting and Correcting Failure  
Consequences Early in the Design**

**Dr. Ron Carlson**

*The Boeing Company Integrated Defense System*

*October 7-8, 2008*

*[Return to Session Directory](#)*

---

# **Anticipating and Correcting Failure Consequences Early in the Design**

**Dr. Ron Carson, Technical Fellow,  
The Boeing Company  
Fellow, International Council on Systems Engineering**

**7 October 2008**

# Why Worry About Failure?

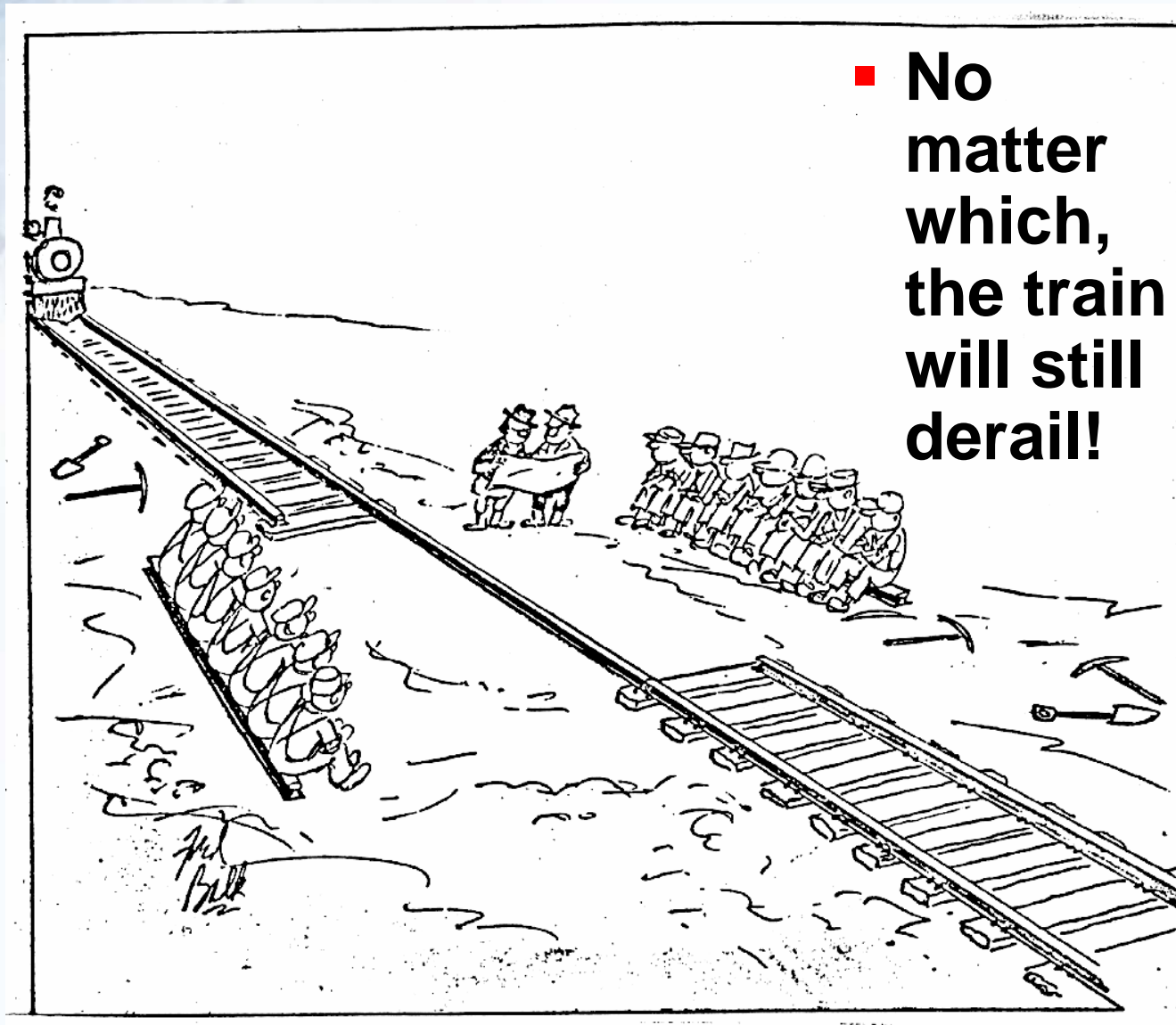
---

- **Stuff breaks**
- **Murphy's Law: If anything can go wrong, it will**



# Requirements, Design, or Construction Failure?

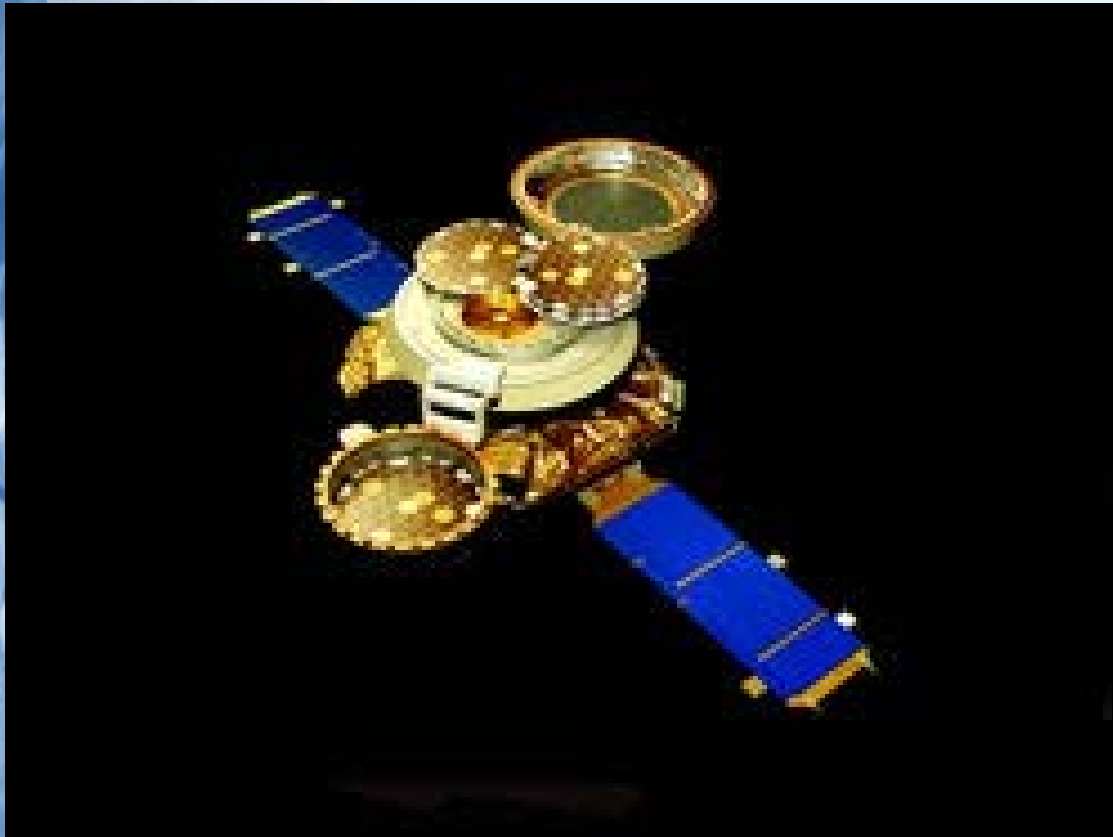
---



- **No matter which, the train will still derail!**

# Genesis Spacecraft – Cosmic Particle Collector

---



[http://en.wikipedia.org/wiki/Genesis  
\(spacecraft\)](http://en.wikipedia.org/wiki/Genesis_(spacecraft))



## Genesis Probe - Failure Source

- “The failure was traced to four tiny switches designed to trigger the release of the two Genesis parachutes, the drogue chute and the main parafoil. [All of] The switches were installed backward....”  
Rocky Mountain News, 03/15/2006, Jim Erickson
- Failure mode was “Incorrect design”
- Consequence: The same as not having a parachute

## Consequences of Delaying Analysis

---

- Delaying analysis until design/fabrication leads to rework
- Must have correct
  - Mission
  - Functions
  - Requirements
  - Design
  - Fabrication



***Must examine the failure of functions prior to beginning design.***

# Industry Guidance on Functional Failure

---

- **ARP5580, “Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications”, SAE, 2001\***
- **Purposes**
  - **Identify potential system (or functional) failures**
  - **Identify unacceptable failure consequences**
    - **Hazardous conditions**
    - **Mission impacts**
    - **Design problems**

\*[http://www.sae.org/servlets/productDetail?PROD\\_TYP=STD&PROD\\_CD=ARP5580](http://www.sae.org/servlets/productDetail?PROD_TYP=STD&PROD_CD=ARP5580)

# Functional or Design-less FMEA

- A physical design is not required in order to perform a failure analysis – Safety “Functional Hazard Analysis” is an example
- Failure analysis is based on asking “What if...?” questions regarding functions
  - What if this function is not performed correctly?
  - What if the precipitating or trigger event for the function does not occur as expected?

Type	Description
Loss of function	The required function is not performed at all
Inadequate performance	The required function is degraded
Incorrect performance	The required function is not performed correctly (e.g., wrong state)
Incorrect timing (early, late, or wrong duration)	The required function is not performed at the correct time
Combinations	Timing errors in combination with performance errors

## Generic Functional Failure Modes

## Example of Functional Failure Analysis: The Door

---

- **What does a door do (function)?**
  - Partitions space – but so does a wall
  - Allows passage when opened – but so does a gateway
- **Combining - The key function of a door is to provide *controllable* isolation of spaces.**
  - “Open” to enable passage
  - “Closed” to provide isolation
  - Under the control of the user – degree of control can range from “public” to “private”



# What Are the Functional Failures?

---

- **Start with the functions:**
  - **Isolate when selected by user**
    - **AND**
  - **Enable passage when selected by user**
- **“Fail the function” by taking the logical complement**
  - **NOT (Isolate when selected AND Enable passage when selected)**
- **Equivalent statement (per DeMorgan’s Law):**
  - **(Fails to isolate when selected) OR (Fails to enable passage when selected)**

# What About Mechanisms of Failure?

---

- For the door, what are the physical failure modes for
  - (Fails to isolate when selected) OR
  - (Fails to enable passage when selected)???
- ....It depends on how the solution is implemented
- Consider
  - Basic home door with handset (no key)
  - Electronically controlled automatic door with keypad security



# Physical Failure Modes for Fails to Isolate

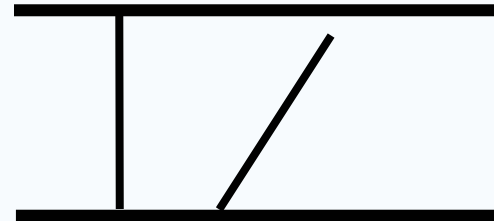
---

- Failure modes are different for each type of mechanism
  - Home door
    - Lock jams so that door cannot close
    - Hinges freeze so door cannot close
    - Door gets a hole in it
  - Automatic door
    - Keypad fails to provide security
    - Automatic door jams open
    - Glass in door shatters
- In each case, the functional failure consequence of the functional failure is realized regardless of implementation, and can be anticipated prior to implementation

# Key Benefit of Design-less FMEA

---

- “Fails to isolate when selected”
  - Add a second door in series in the design as a backup (e.g, airlock)

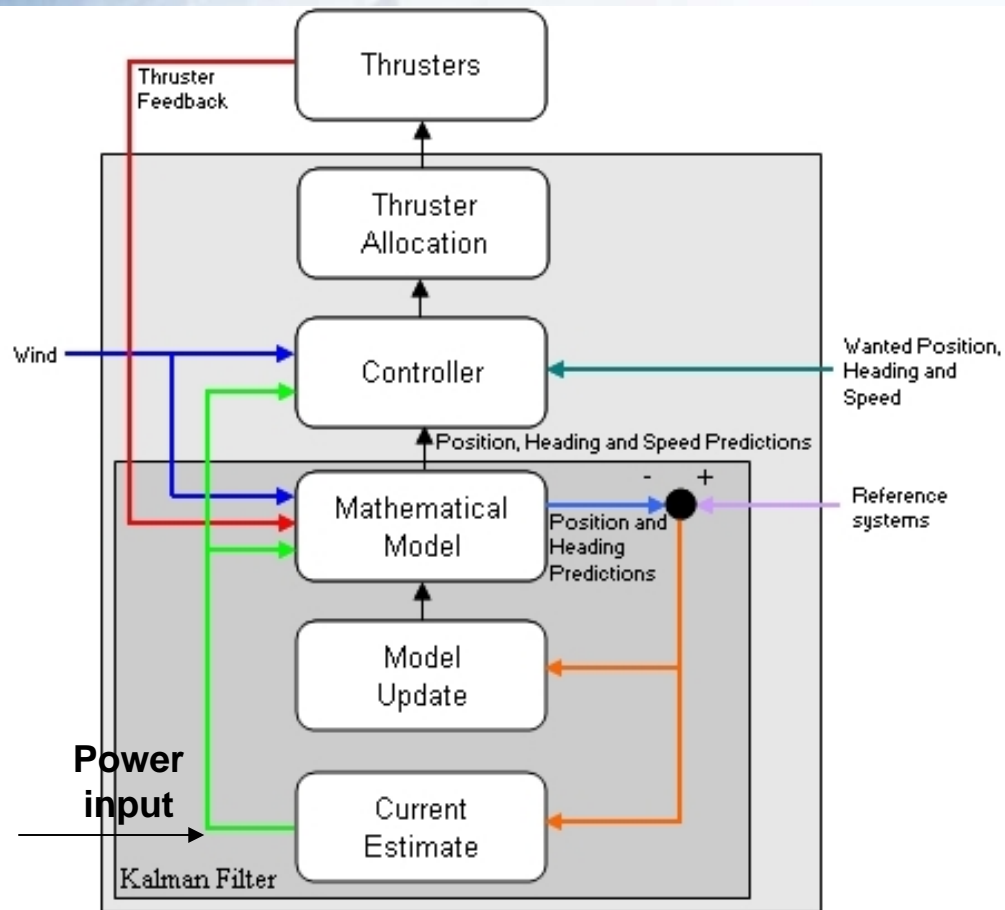


- “Fails to enable passage when selected”
  - Add a second door function in parallel to the system under consideration



***Mitigation can be applied well  
before final design***

# How do we use this for Dynamic Positioning?



<http://en.wikipedia.org/wiki/Image:Controller.jpg>

## ■ Determine Functions

- Determine wanted position, heading, speed
- Sense position
- Sense wind, waves, current
- Move to intended position
- Maintain intended position
- Maintain intended orientation

# DP Functional Failure Analysis

---

## ■ Functions

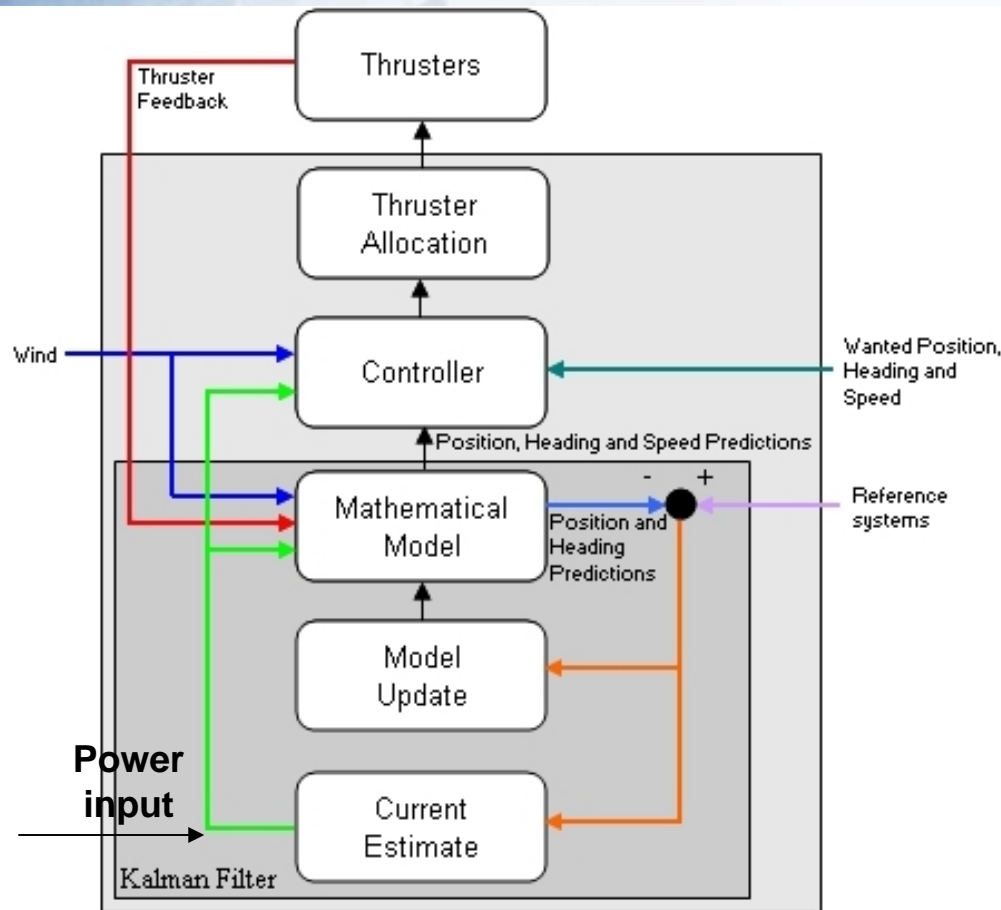
- Determine wanted position, heading, speed
- Sense position
- Sense wind, waves, current
- Move to intended position
- Maintain intended position
- Maintain intended orientation

## ■ Functional Failures

- Incorrect or latent position, heading, speed
- Incorrect position
- Incorrect assessment of wind, waves, current
- Failure to move, incorrect move, too slow/fast
- Fail to maintain intended position; incorrect position
- Fail to maintain intended orientation; incorrect orientation

***What do we do with this information?***

# Design Mitigation in the System Architecture



- Determine which are intolerable
- Add mitigation
- Example
  - Fail to maintain intended position
  - Maintains incorrect position
- Allocated to
  - Position sensors
  - Controller
  - Thrusters

<http://en.wikipedia.org/wiki/Image:Controller.jpg>

# Other Dynamic Positioning Needs

---

## Sea Launch



[http://en.wikipedia.org/wiki/Sea\\_Launch](http://en.wikipedia.org/wiki/Sea_Launch)

- Even in aerospace we're depending on dynamic positioning functions – performance attributes and consequences will differ
- Functional failure techniques for FMEA apply

# Summary

---

- **Failure modes and effects analysis can begin as soon as we begin discussing mission and function of a system**
- **Discovery of system design problems earlier shortens cycle time by avoiding late rework**

