Requirements for Extremely Complex Systems

David Hetherington

Introducing the "System of Systems"

Classic "System of Systems"

Multiple Levels

Each Level is a "System" in its own right.

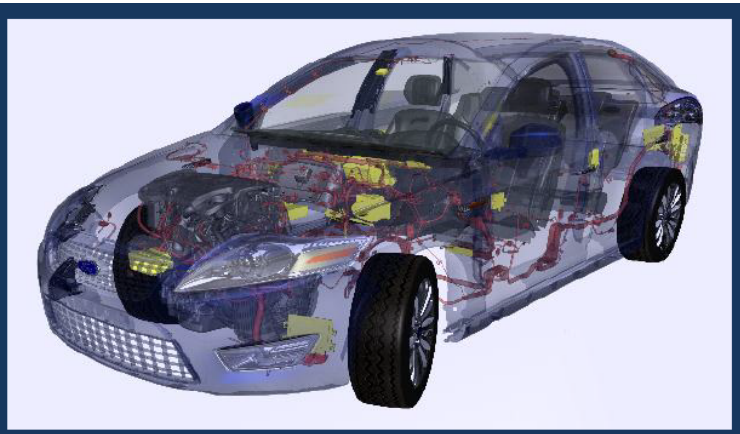
Requirements at any level affect all the levels below.

“System of Systems” Common Features

Mission-Critical	“Five Nines” Availability Required
Safety-Critical	Software/Requirements mistakes can kill people
High Stakes	Software/Requirements mistakes can cause huge financial losses
Multiple Suppliers	Tower of Babel

How Complicated do Such Systems Get?

Ford Example – Car Complexity



CD Class Vehicle has approx.

- 50-70 Computers on board with multi-core SW process management
- > 10 MByte of Control Software
- >15 Million LOC/Instructions
- > 5,000 Software Parameters
- > 50,000 functional requirements
- > 1,000,000 pages of specifications
- > 10,000 buildable Vehicle-Series-Variants (based on ECU component permutations per Vehicle line)

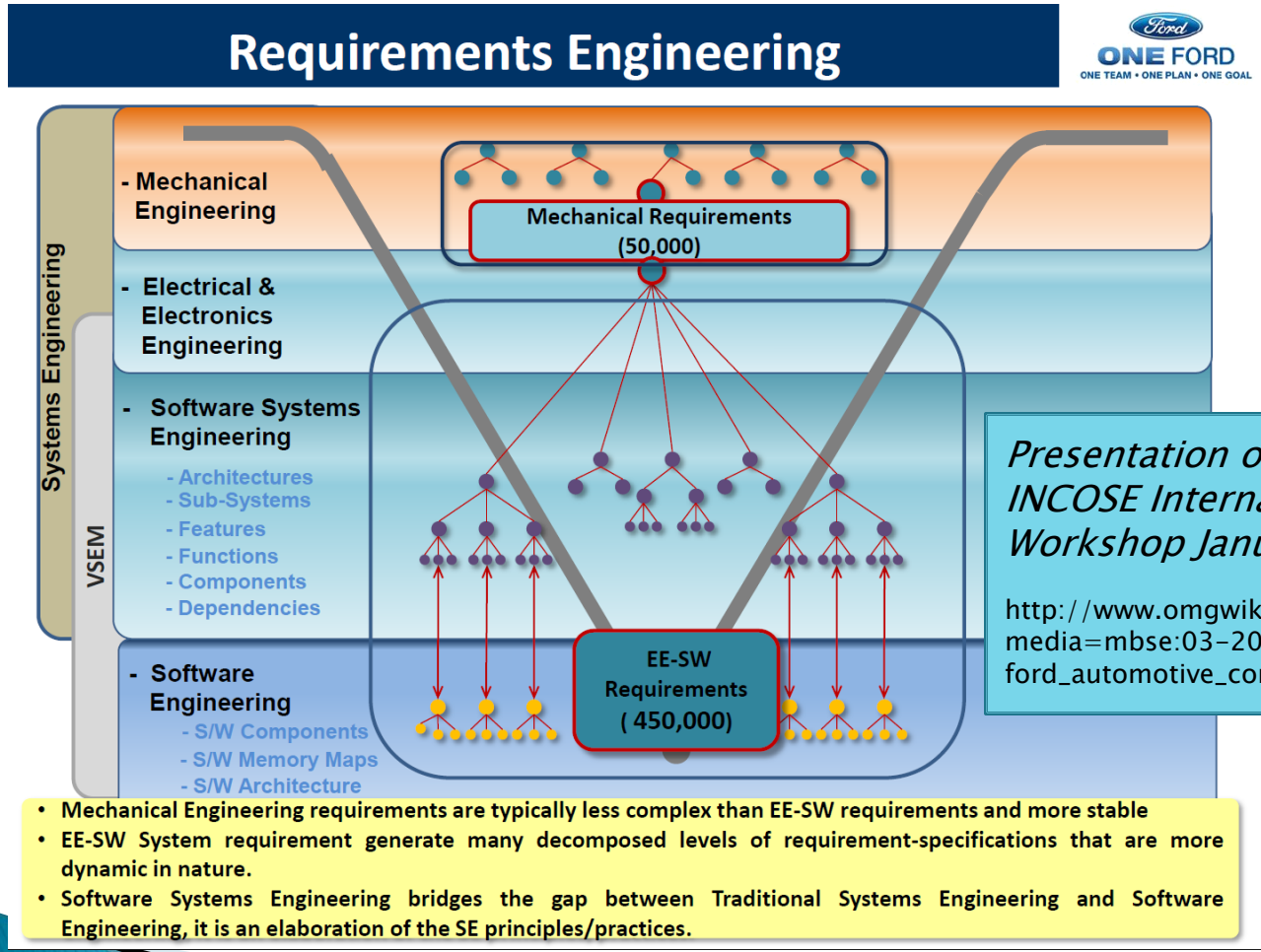
A luxury car can have more than 100 onboard computers

Many "requirements" need multiple onboard computers to cooperate with each other in a tightly choreographed dance.

Presentation of Christopher Davey at the INCOSE International Workshop MBSE Workshop January 26th-28th, 2013

http://www.omgwiki.org/MBSE/lib/exe/fetch.php?media=mbse:03-2013_incose_mbse_workshop-ford_automotive_complexity_v4.0-davey.pdf

Ford Example – 450,000 Requirements



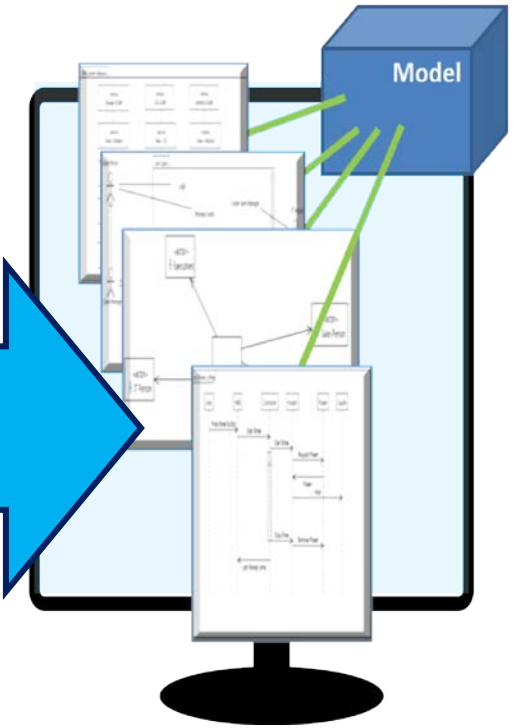
Working out all that choreography produces 450,000 requirements.

Presentation of Christopher Davey at the INCOSE International Workshop MBSE Workshop January 26th-28th, 2013

http://www.omgwiki.org/MBSE/lib/exe/fetch.php?media=mbse:03-2013_incose_mbse_workshop-ford_automotive_complexity_v4.0-davey.pdf

Humans and Complexity Management

How do We Manage Complexity?



Stage 1

Stage 2

Stage 3

Stage 1 – Requirements in Our Head

Skilled Professionals

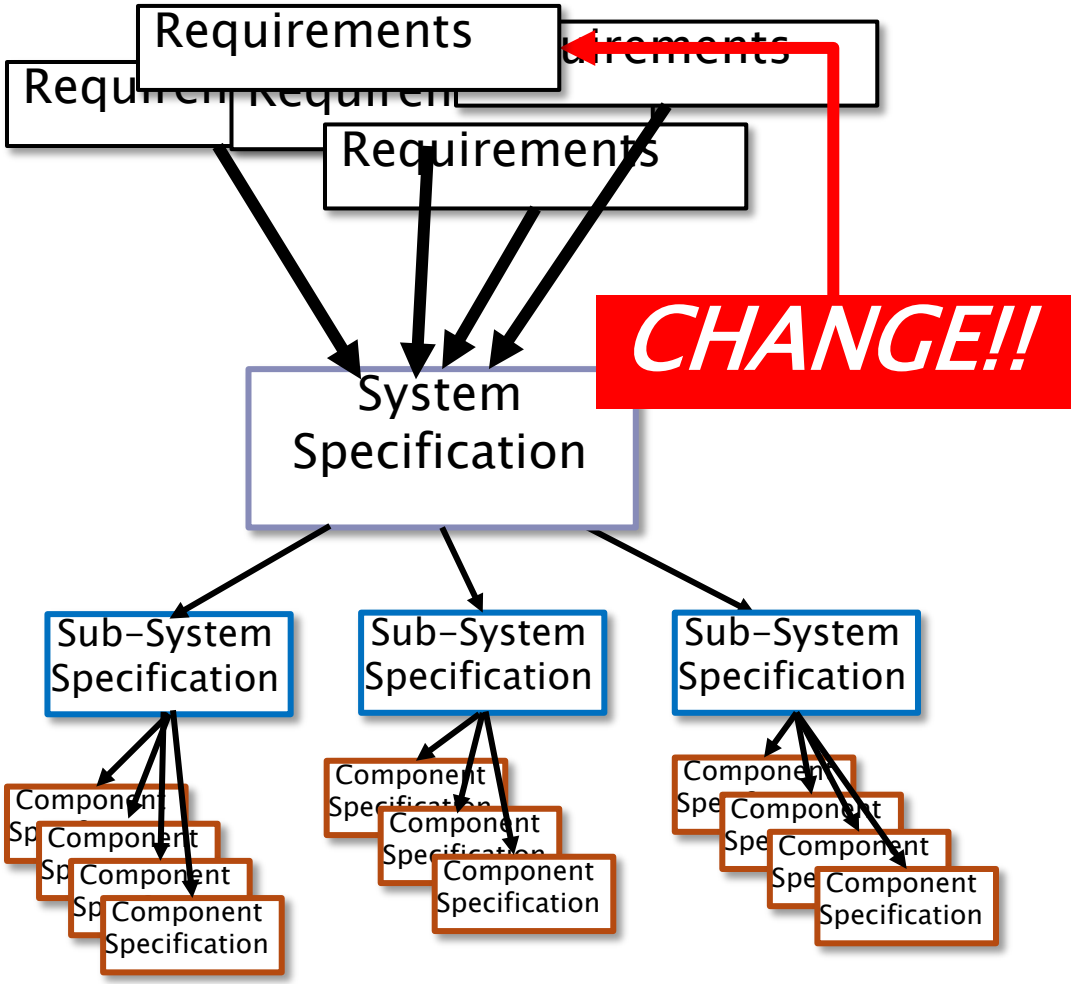
Hate “Bureaucracy”

“Tell Me What You Need”

“I’ll Make it Happen!”

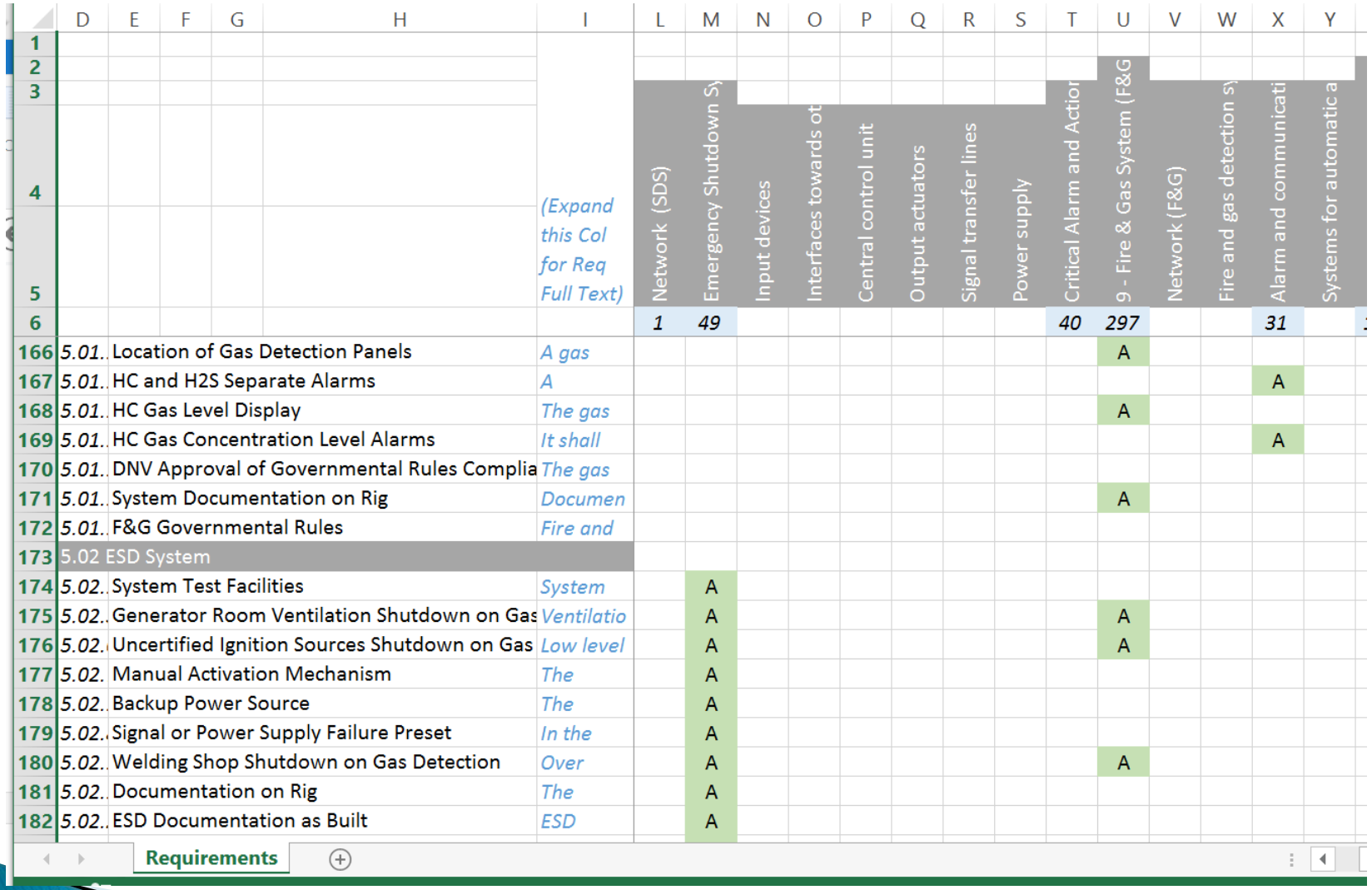
Not Scalable

Stage 2 – Requirements and Specification Documents



Requirements Traceability

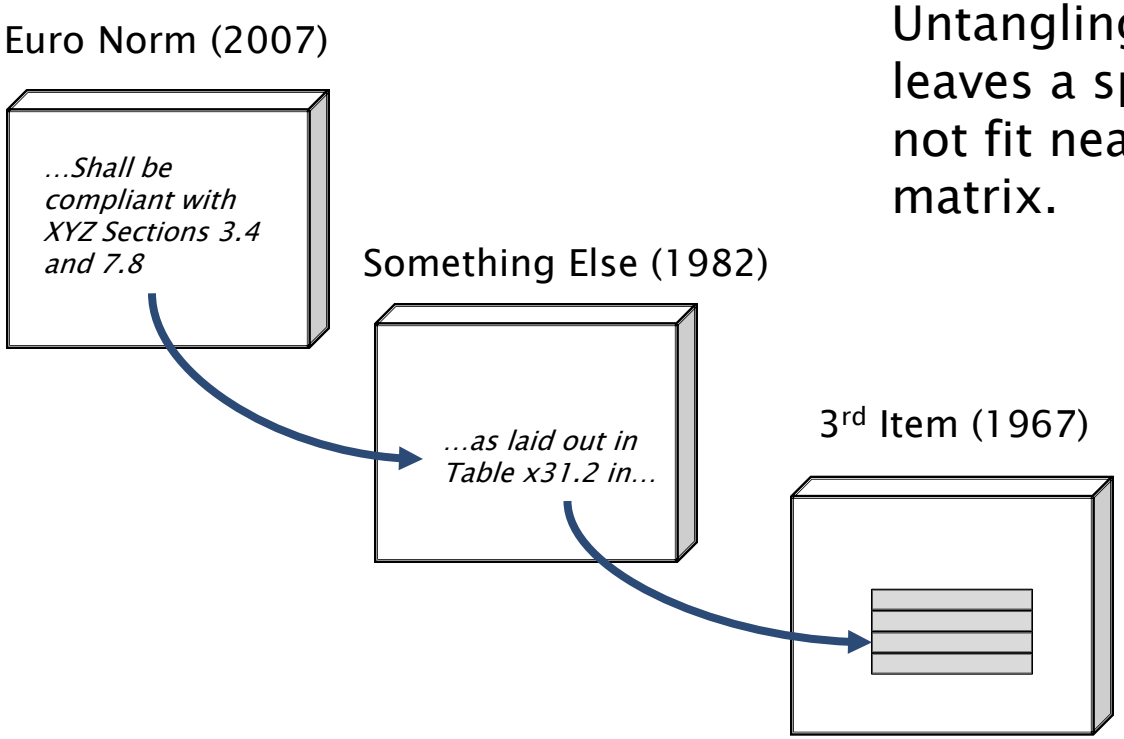
Traceability Matrices



	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1																				
2																				
3							Network (SDS)	Emergency Shutdown Sy	Input devices	Interfaces towards ot	Central control unit	Output actuators	Signal transfer lines	Power supply	Critical Alarm and Actior	9 - Fire & Gas System (F&G	Network (F&G)	Fire and gas detection sy	Alarm and communicati	Systems for automatic a
4						(Expand this Col for Req Full Text)														
5																				
6							*1*	*49*							*40*	*297*			*31*	
166	*5.01..*	Location of Gas Detection Panels				*A gas*										A				
167	*5.01..*	HC and H2S Separate Alarms				*A*													A	
168	*5.01..*	HC Gas Level Display				*The gas*										A				
169	*5.01..*	HC Gas Concentration Level Alarms				*It shall*													A	
170	*5.01..*	DNV Approval of Governmental Rules Complia				*The gas*														
171	*5.01..*	System Documentation on Rig				*Documen*										A				
172	*5.01..*	F&G Governmental Rules				*Fire and*														
173	5.02 ESD System																			
174	*5.02..*	System Test Facilities				*System*		A												
175	*5.02..*	Generator Room Ventilation Shutdown on Gas				*Ventilatio*		A								A				
176	*5.02..*	Uncertified Ignition Sources Shutdown on Gas				*Low level*		A								A				
177	*5.02..*	Manual Activation Mechanism				*The*		A												
178	*5.02..*	Backup Power Source				*The*		A												
179	*5.02..*	Signal or Power Supply Failure Preset				*In the*		A												
180	*5.02..*	Welding Shop Shutdown on Gas Detection				*Over*		A								A				
181	*5.02..*	Documentation on Rig				*The*		A												
182	*5.02..*	ESD Documentation as Built				*ESD*		A												

Requirements

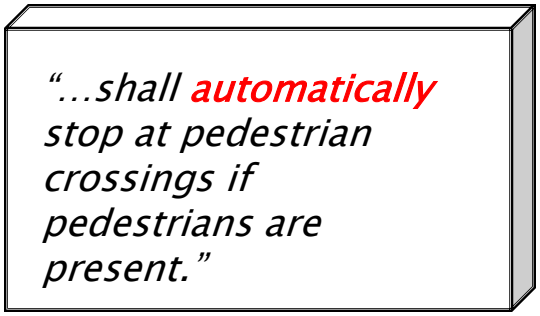
Standards Discovery



Untangling this sort of mess leaves a spider web that does not fit neatly in a traceability matrix.

Standards Analysis

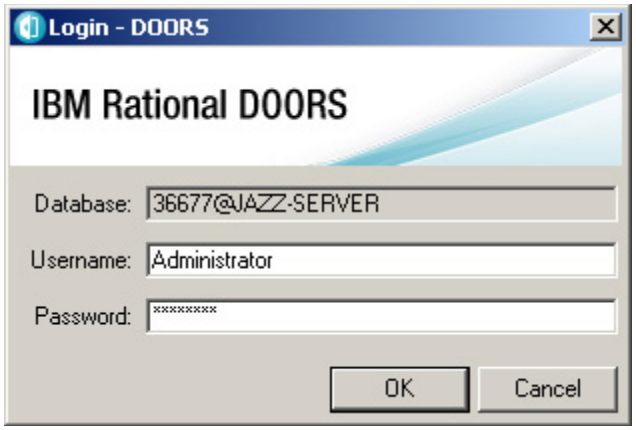
Some Standard



So…what does this standard actually require? A lot of analysis and interpretation will be required!

Text-Only Requirements Tools

Automate the Cut-and-Paste



Contents	Satisfies	Artifact Type
1 Functional Requirements		Heading
1.1 Power car		Heading
1.1.1 Move car		Heading
1.1.1.1 Move forwards		Heading
The car shall be able to move forwards at all speeds from 0 to 220 kilometers per hour on standard flat roads with winds of 0 kilometers per hour, with 280 BHP.	1120:Users shall be able to travel in safety according to the Road Research Laboratories Safety standards dated 1 January 2003. (Stakeholder Requirements)	System Requirement

visure

hp Agile Manager

Strengths/Limitations

Strengths

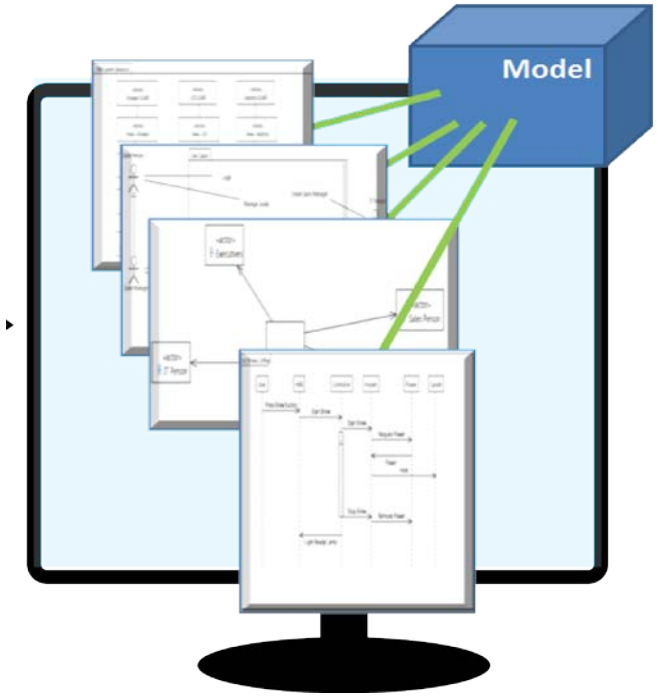
- Semi-Automated document input
- Drag-and-drop
- Easy output of Word documents
- Good traceability functions

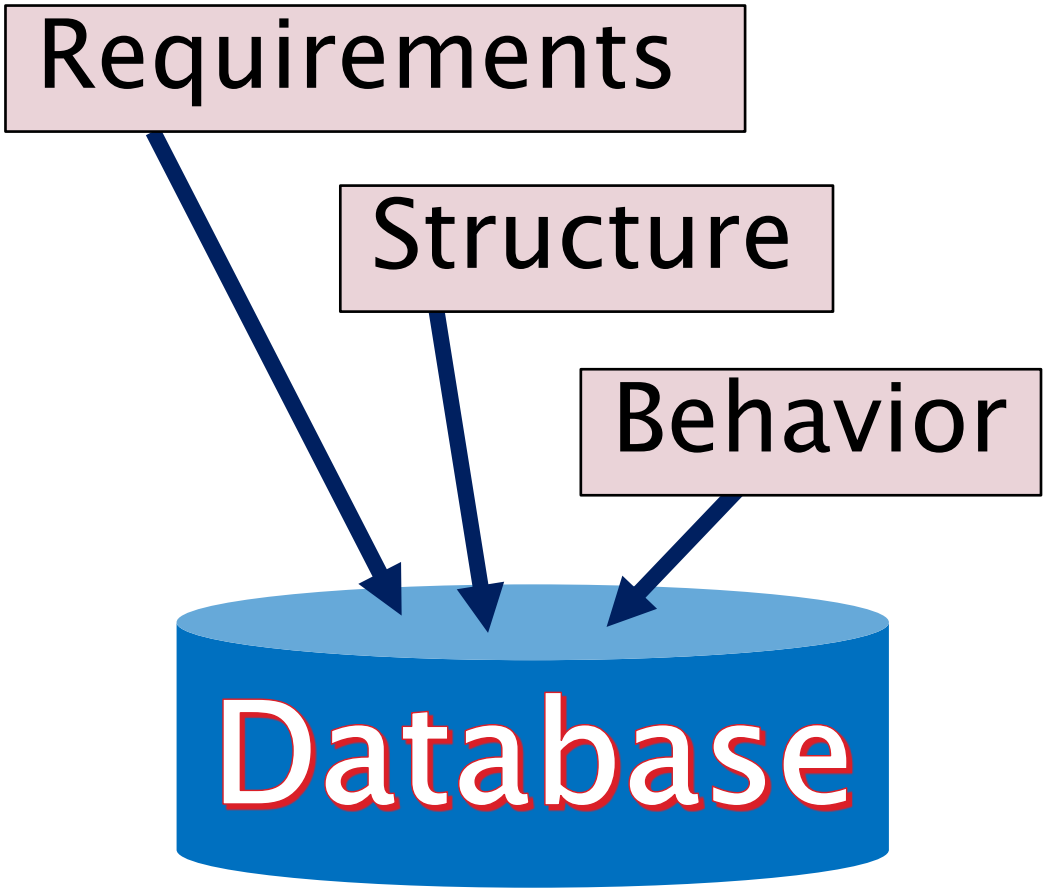
Weaknesses

- Text-only is cumbersome
- “A picture is worth a thousand words”
- Requirements reviews are painful
- Hard to link to other tools

Model-Based Systems Engineering

Solution – Add Graphical Modeling to Text



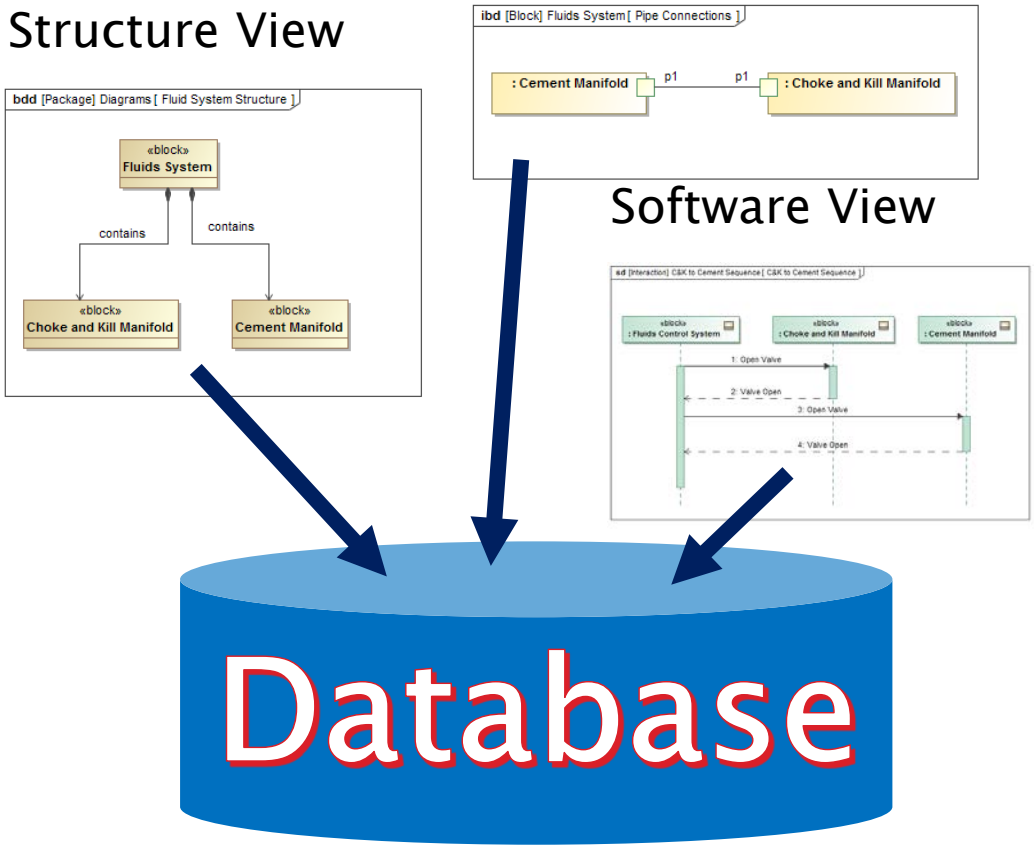


The Database Keeps Track of the Relationships

Introducing Model-Based Systems Engineering

Plumbing View

Structure View



Simple Diagrams

One Concept per Diagram

Different Diagrams for Different Stakeholders

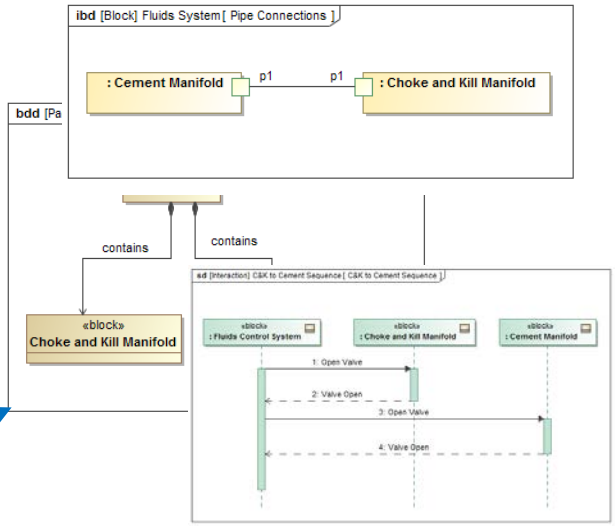
As Many Diagrams as Needed

Model Database Consolidates Information

"Model-Based Systems Engineering" is the More Formal Term.

Introducing SysML

Precise Diagrams



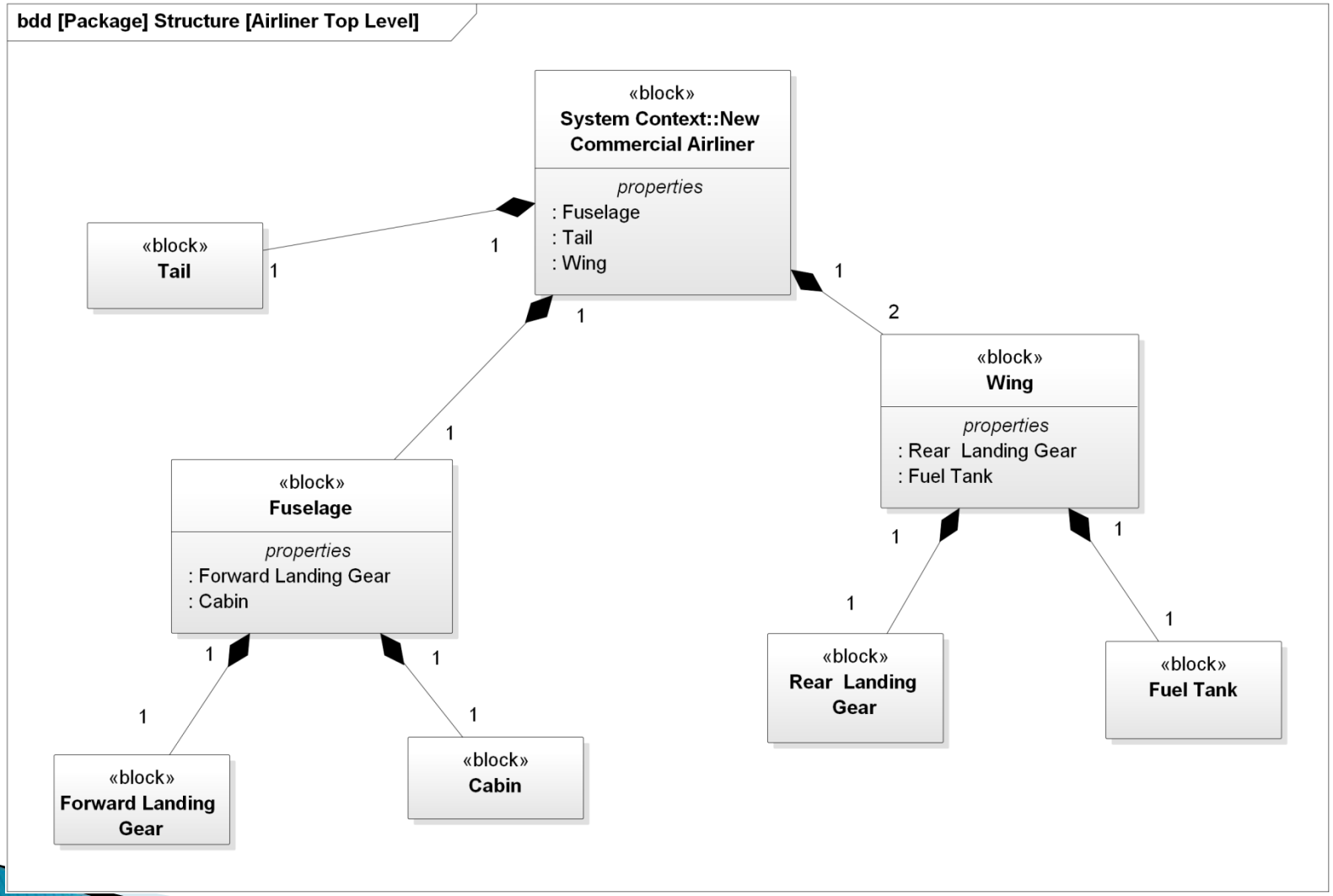
INCOSE
International Council on Systems Engineering

OMG
WE SET THE STANDARD™

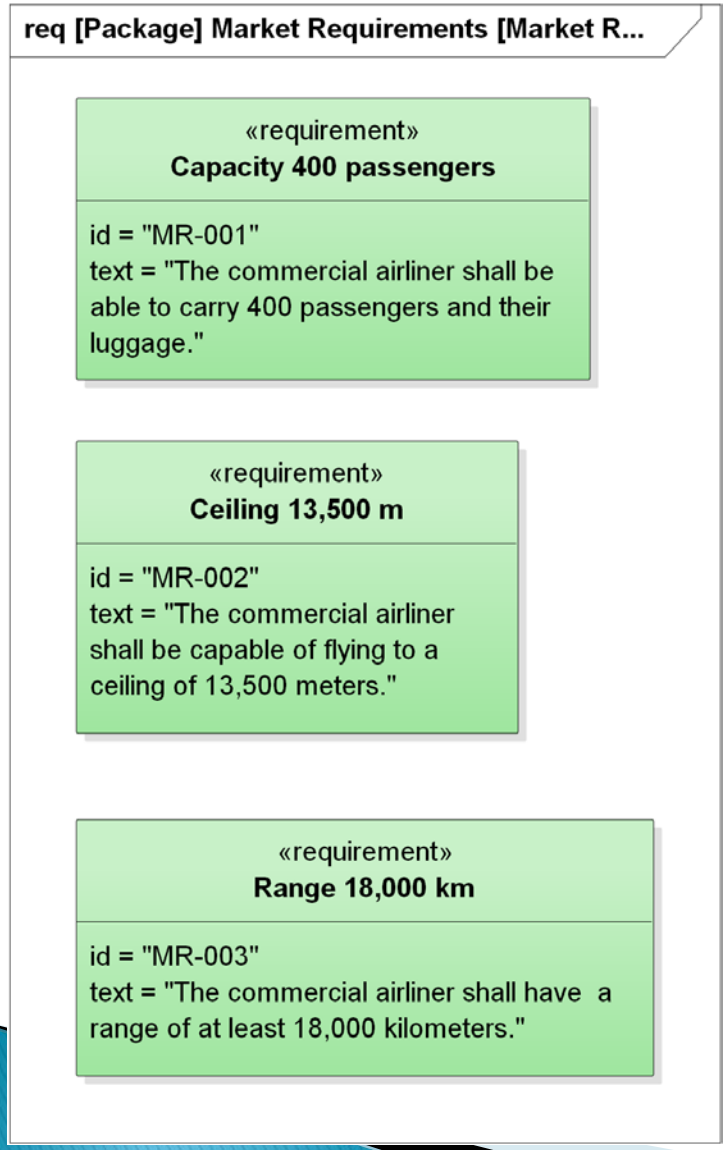
OMG SYSTEMS MODELING LANGUAGE
SysML™

XML Model Data Representation

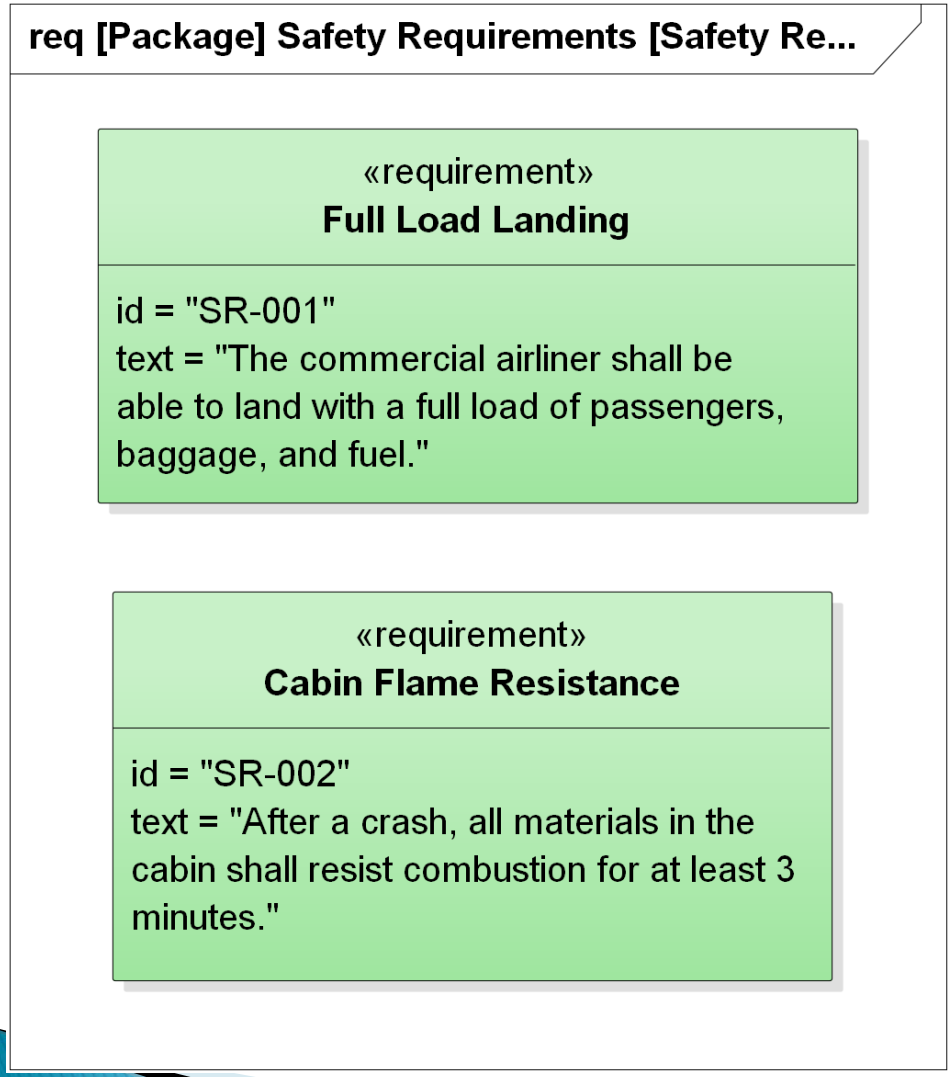
SysML – System Structure



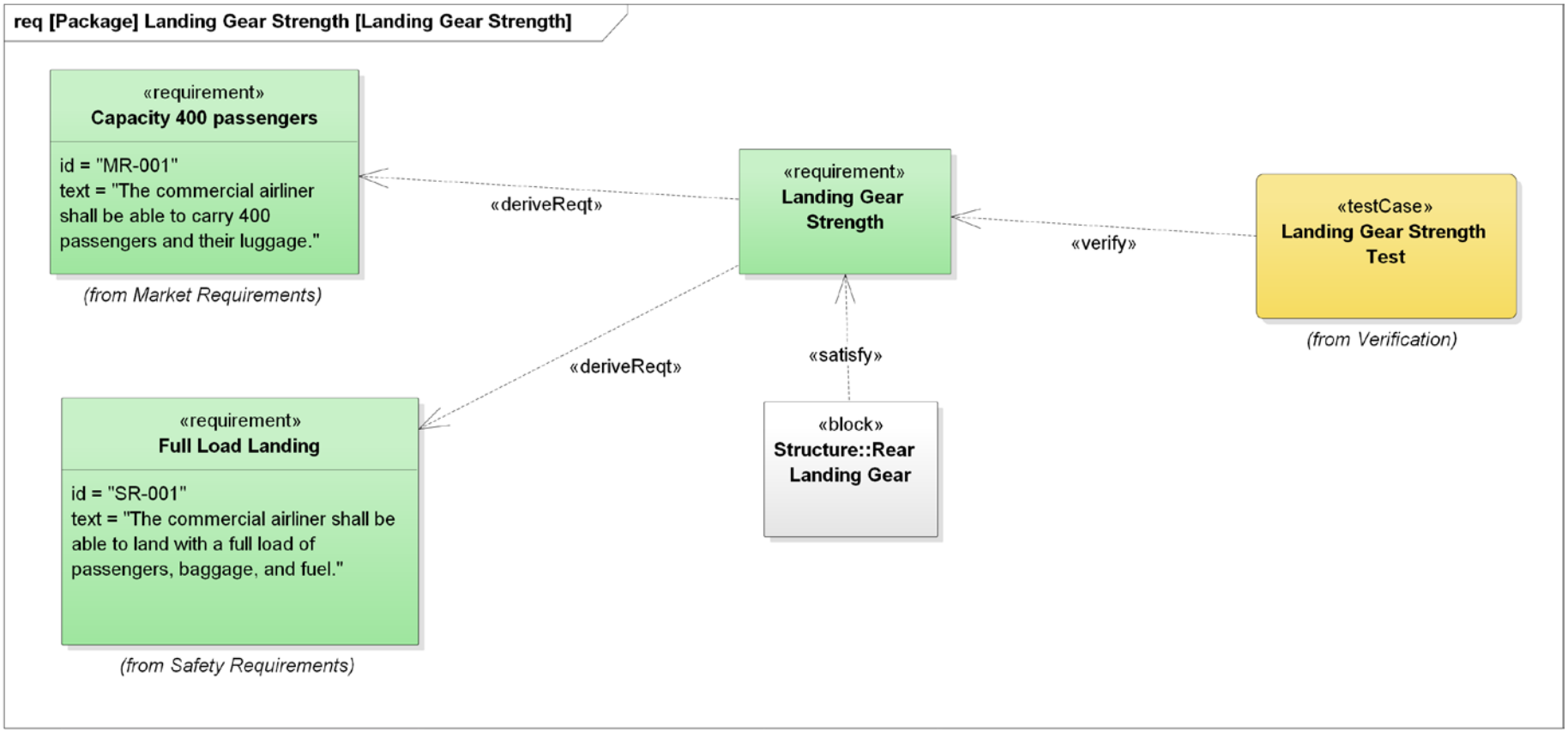
The Market Requirements



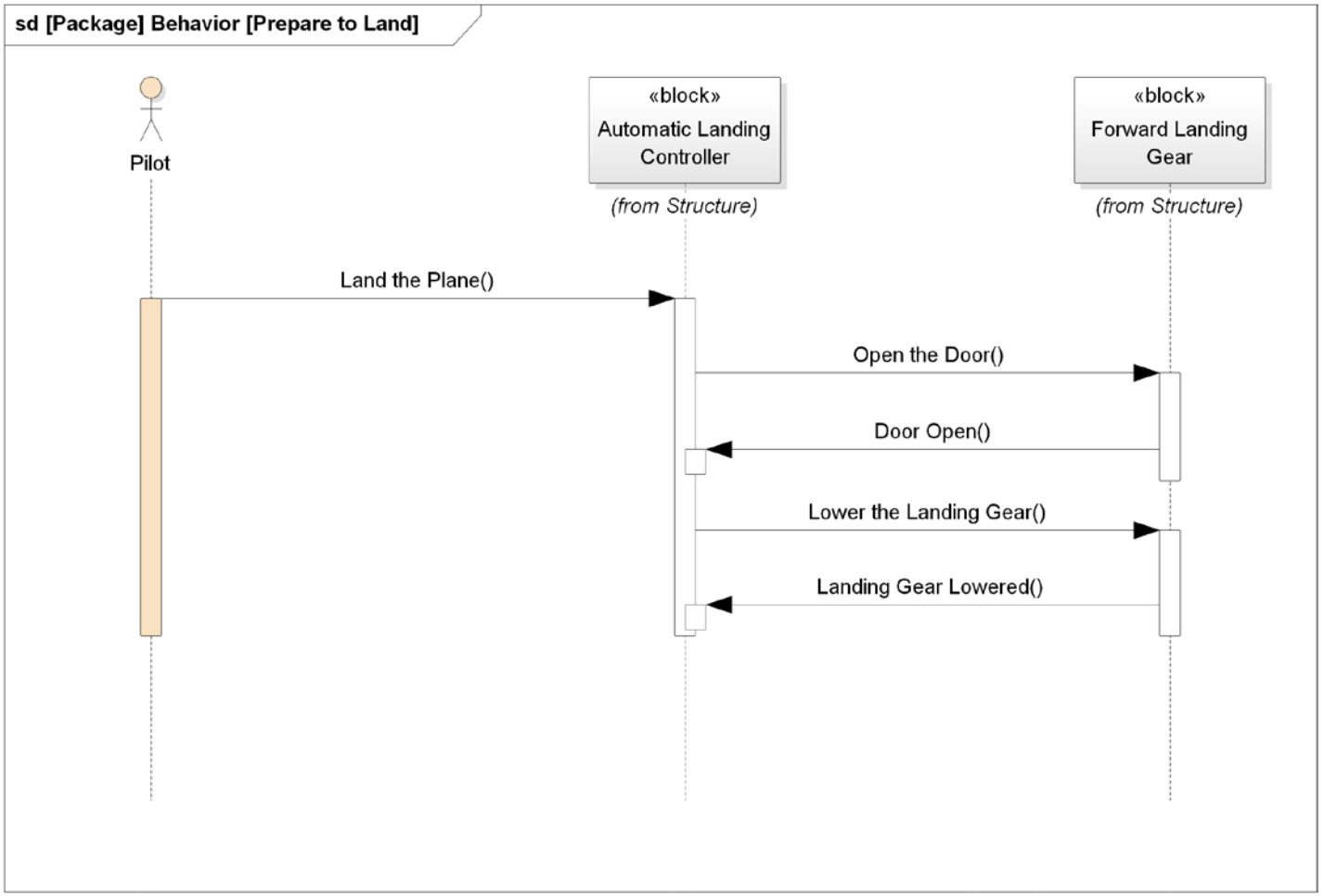
The Safety Requirements



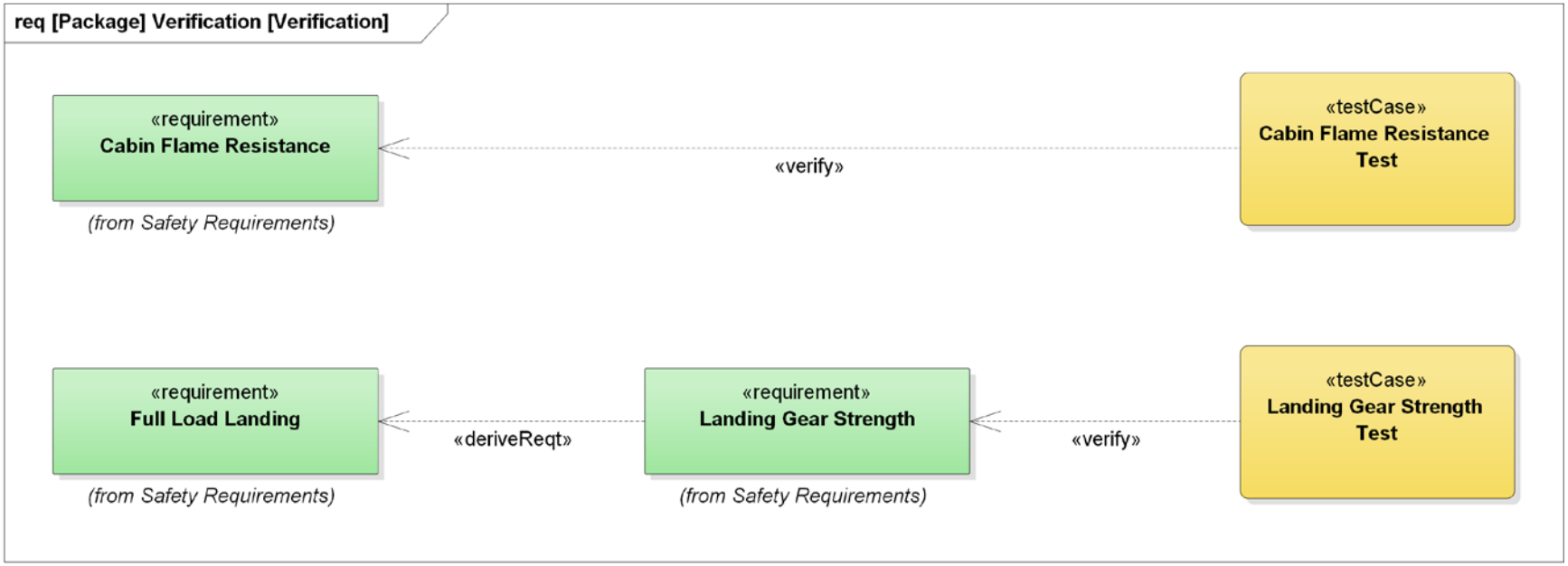
Elaborating the Requirements



Modeling Behavior



Trace to Test Cases



Agile vs Safety-Critical

Not Every Application Needs Careful Planning

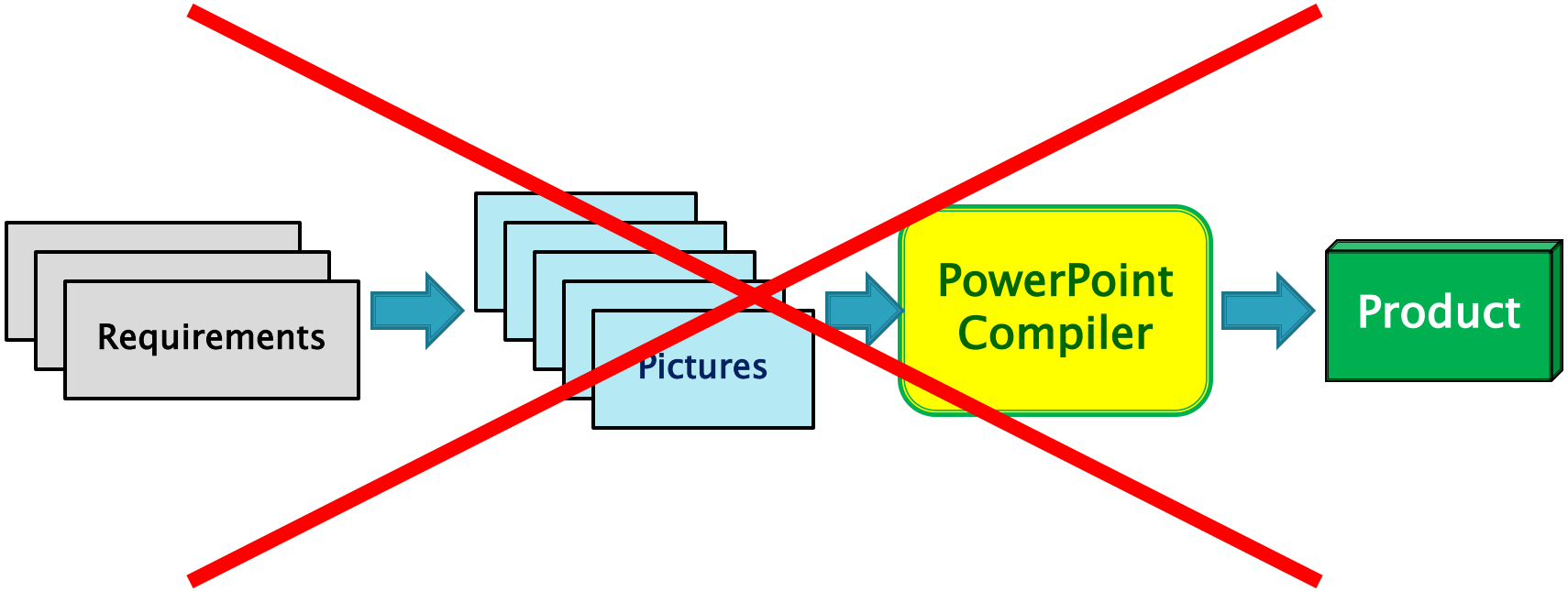
Animation by Kalia Pickett

Safety-Critical Apps

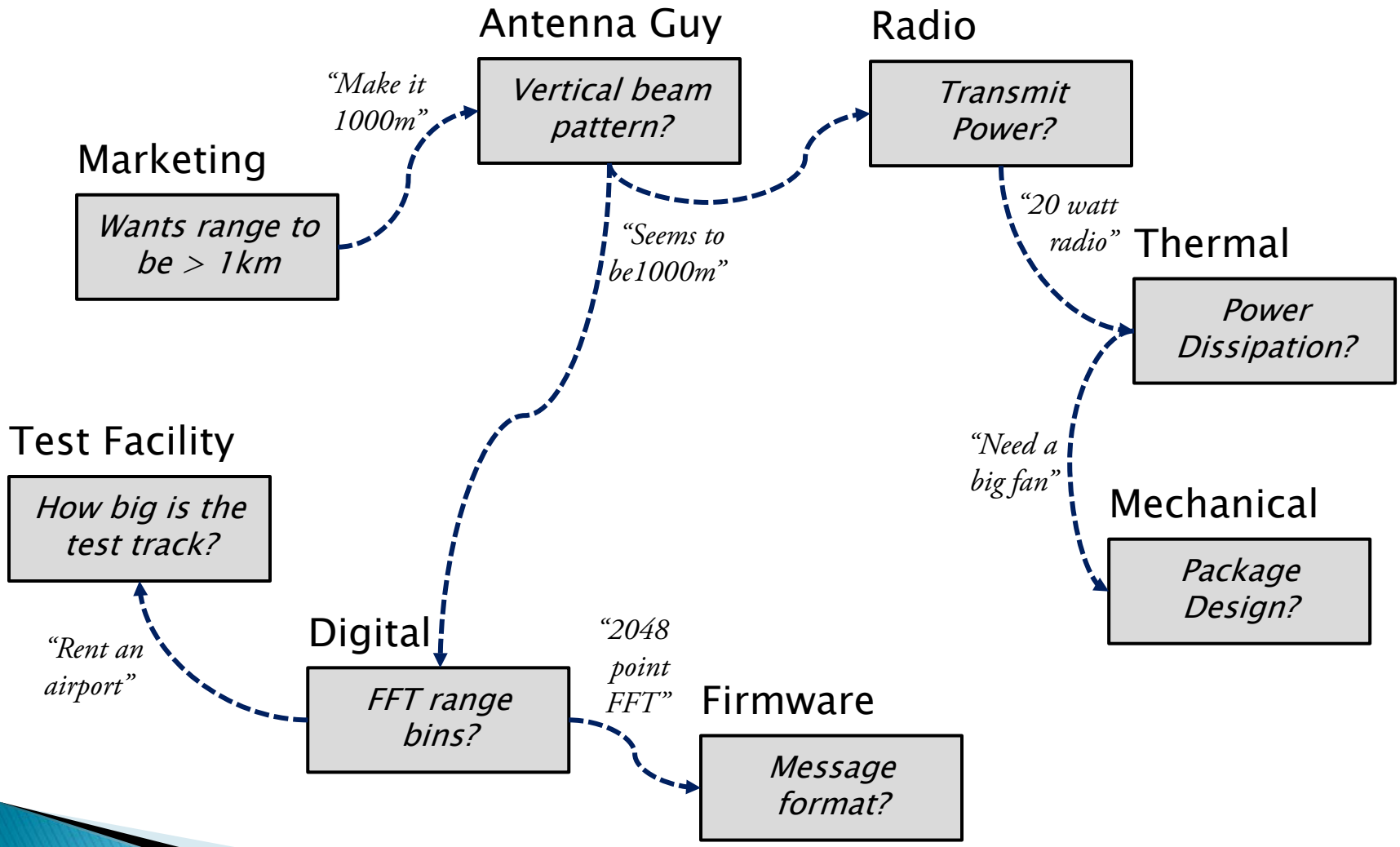
If a careless mistake in your requirements, coding, or verification can incinerate a crew of 150 people, it is immoral to “blow off the documentation”…

Understanding the Role of MBSE

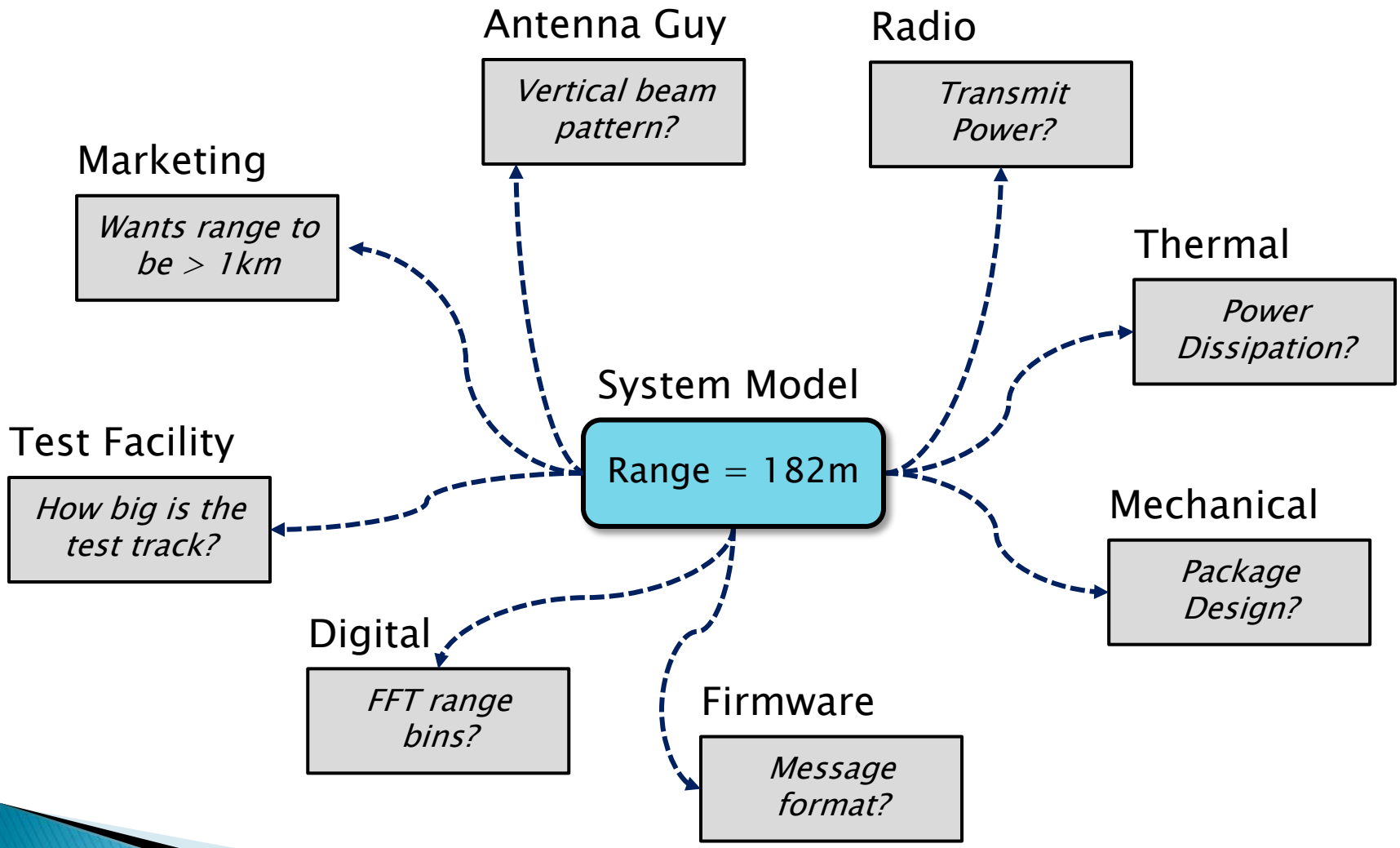
Systems Model – NOT a PowerPoint Compiler



Systems Model – Tower of Babel



Systems Model – Single Version of Truth



Agile in a Complex Systems Environment

First… We Need to Lose Some Baggage

Traditional Side

- Illusion of predictability
- Elaboration too early
- Long periods without working code

Agile Side

- Moaning about "Waterfall"
- Skipping the documentation
- Flexible definition of "done"

Next… Recognize Each Other's Strengths

Traditional Side

- Precision
- Accountability
- Project Scale

Agile Side

- Frequent checkpoints reduce risk
- Efficient management of uncertainty
- Superior team throughput

Road to Certain Failure

Collect lots of requirements documents

→ Make beautiful “Logical” architecture model

→ Elaborate 20 levels of logical architecture and increasingly detailed requirements

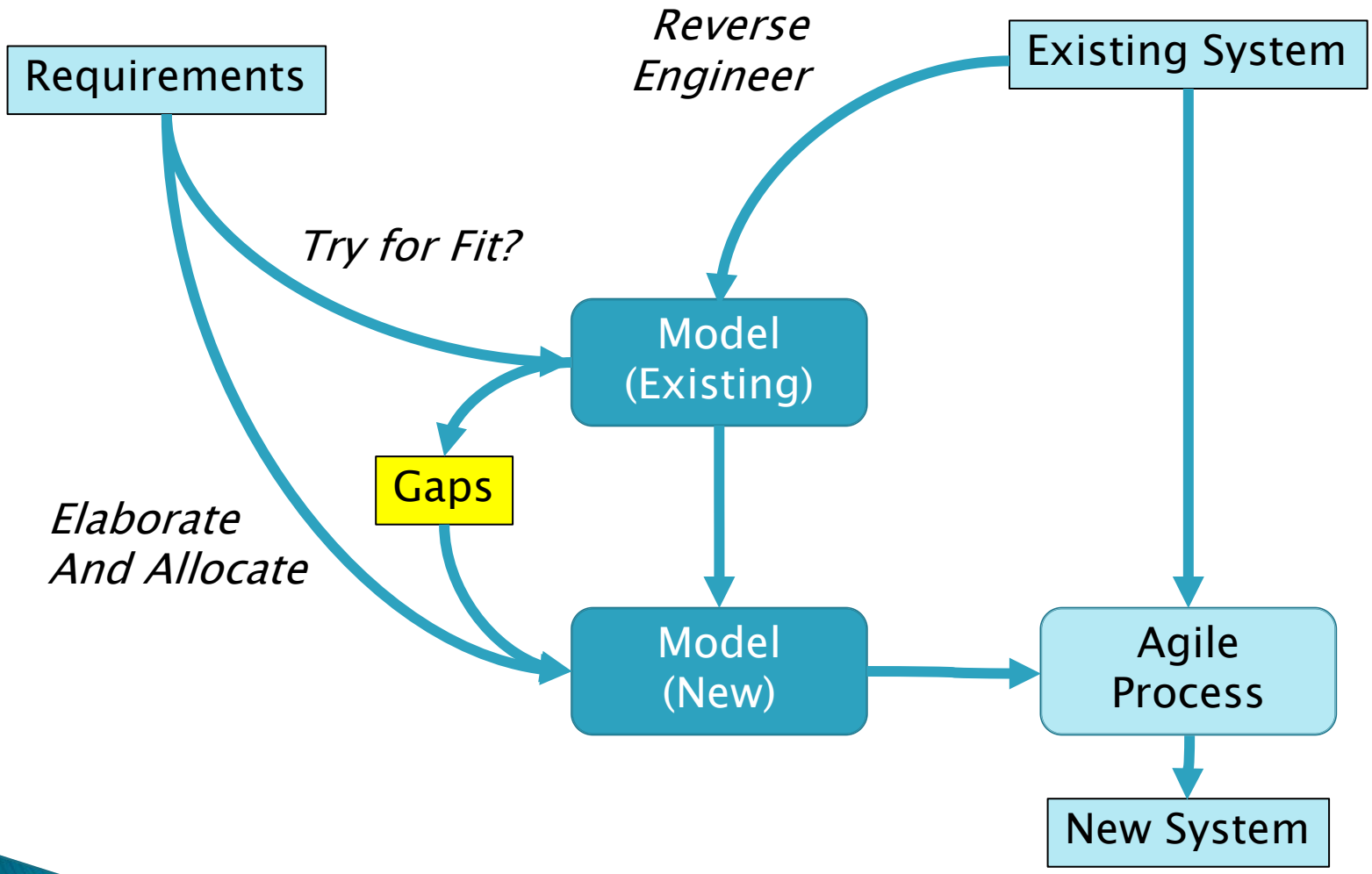
→ Publish voluminous specifications based on above

Attempt to “allocate” logical architecture to real world subsystems

→ **Discover that nothing works**

→ **Blame the tools!!**

Better Approach



Reference

Contact

- David Hetherington
  - LinkedIn: https://www.linkedin.com/in/djhetherington
  - GitHub: https://github.com/DavidHetherington
  - Dave's "Minimal SaaS" Demo: http://cities.asattepress.com/