Präsentiert von

Henning Butz


# Die Grenzen des MBD bei Entwurf und Validierung komplexer Systeme durch „Contract Based Design (CBD)" überwinden

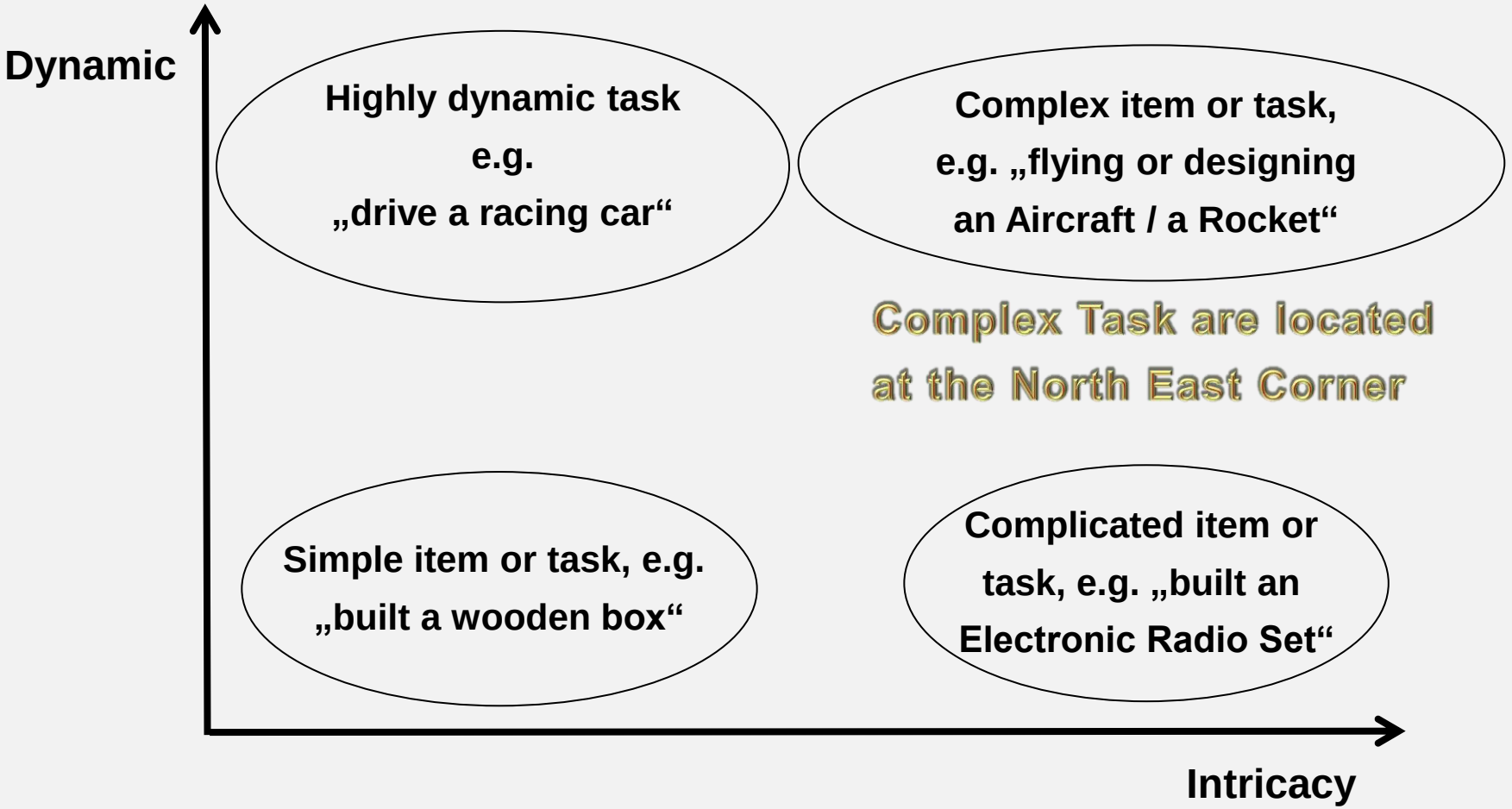
# Getting beyond the limits of MBD in Complex System Design and Validation by „Contract Based Design (CBD)"

MESCONF, München, October 10th 2015

# We are going to talk about …

- The nature and the features of complexity
- Two examples of fatal accidents caused by complexity effects
- The meaning of MBD in the frame of complex system design
- Why MBD fails in complex system design
- The method of contract based design (CBD)
- The advantage of CBD application to the given examples
- Further benefits of CBD in the frame of complex system design

# The Features of „Complexity“

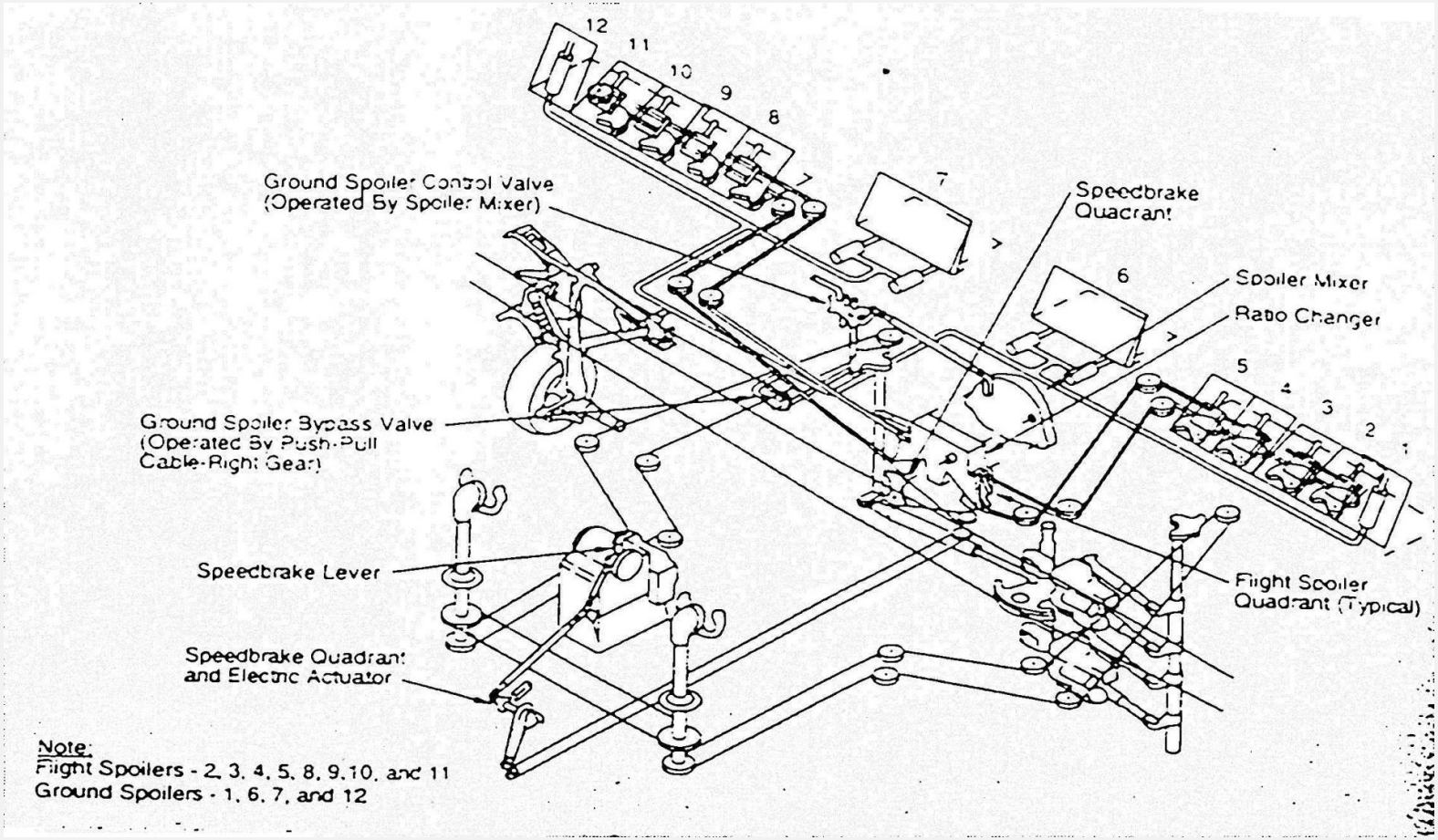





ASES
Advanced Systems
Engineering Solutions

# From mechanical Automaton .....

**Roll controls / air brake of Boeing 737, „Complicated Design“**




**The functions of roll- and air brake surfaces for any operating case**

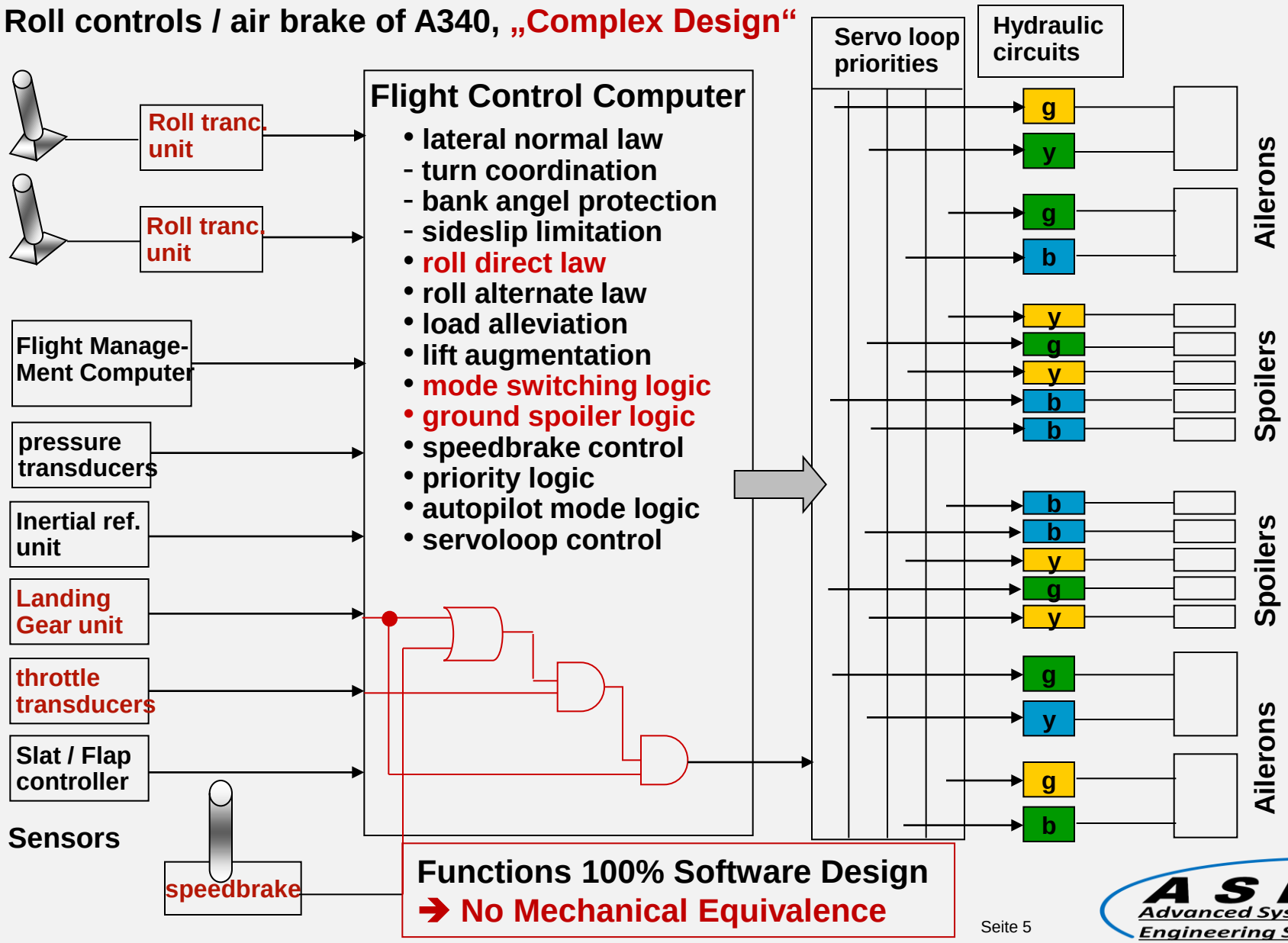
**(Rejected Take Off, A/C On Ground, Cruise, ...) purely mechanical design**

**➔ Limited state space ➔ quite easy to validate**



ASES Advanced Systems Engineering Solutions

# .... to digital Algorithms – ”virtual Functions”

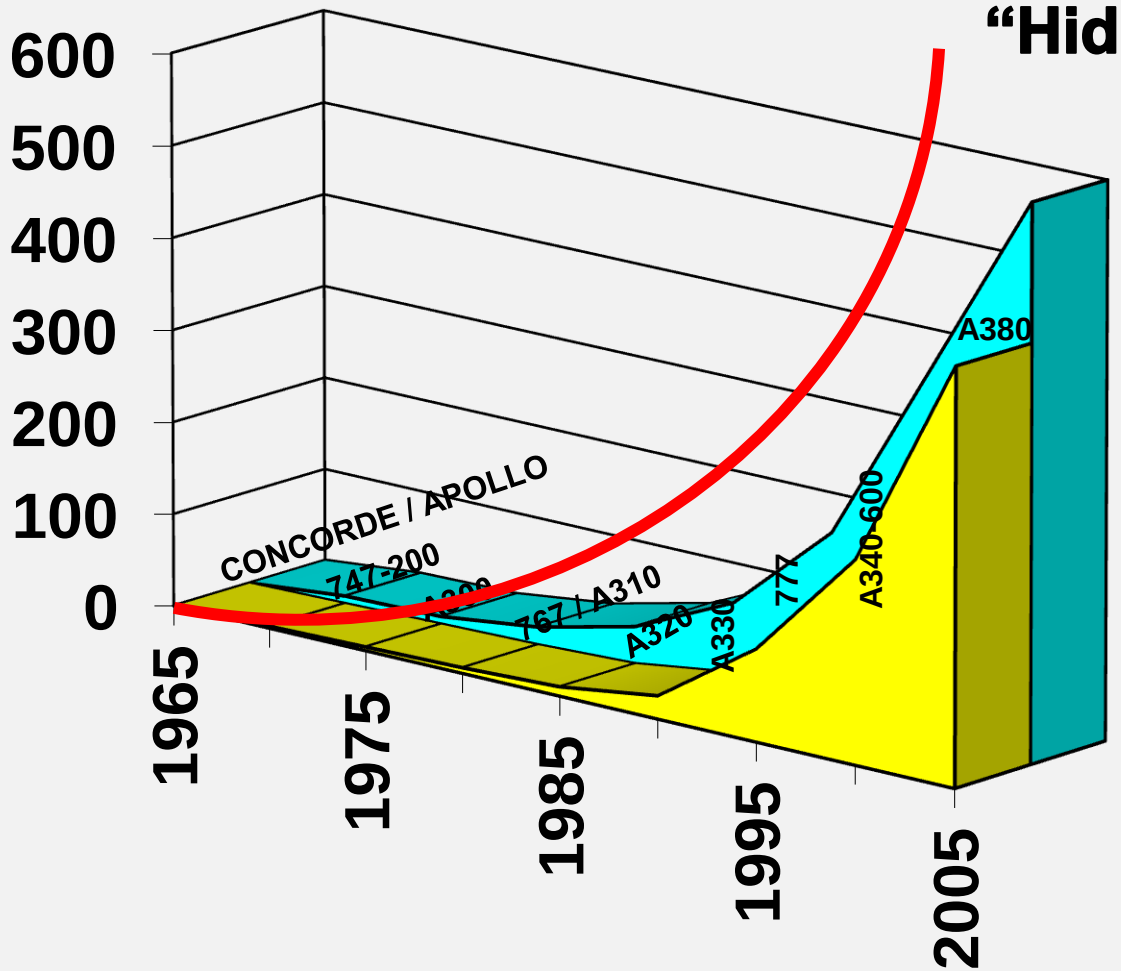





ASES Advanced Systems Engineering Solutions

# Aircraft: Intense Interference of Dynamic Functions

**Complexity Effects: “Emergence", “Hidden Links" and “Dys-Functionality”**

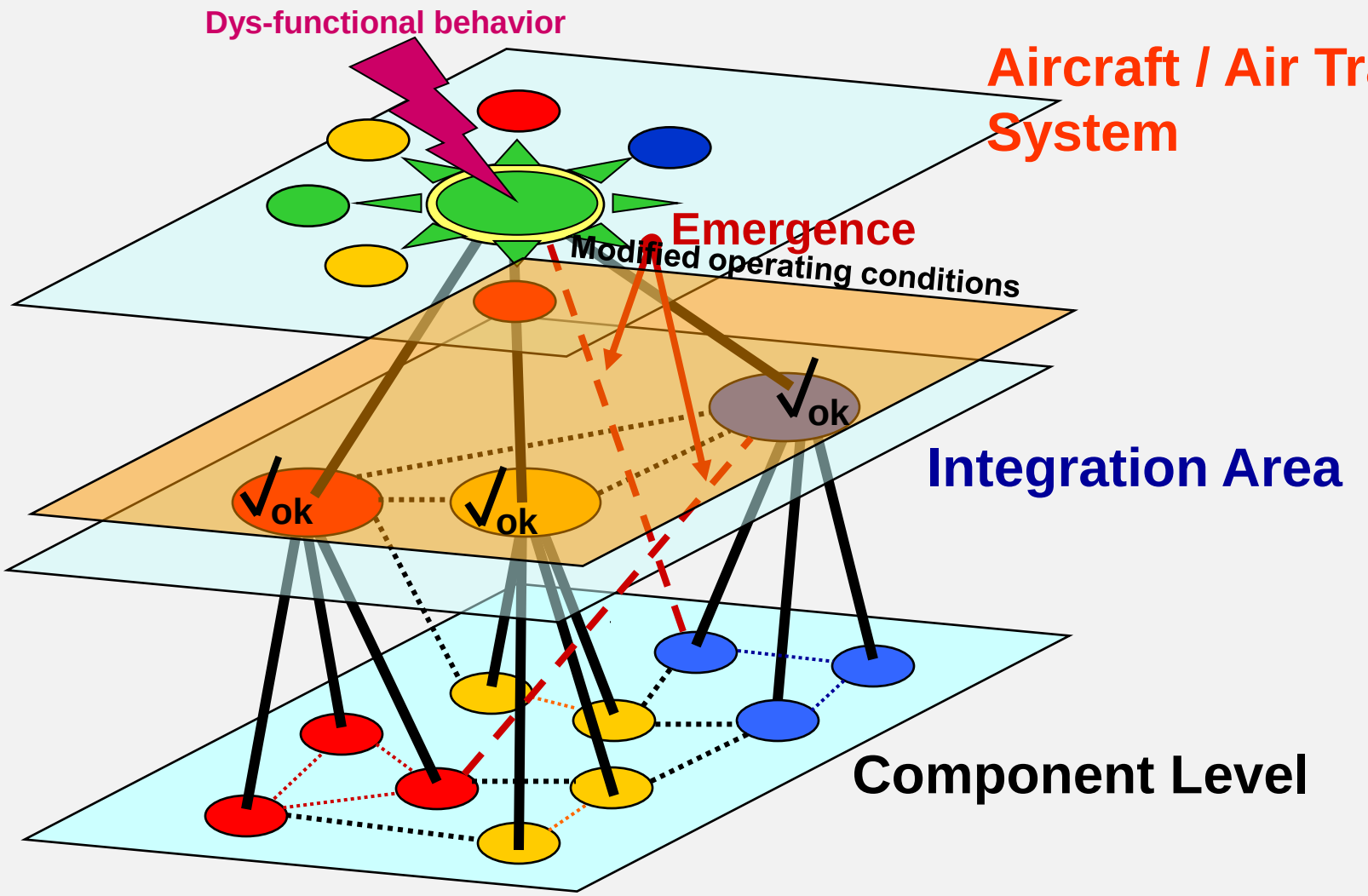



- Function SW in MB
- Signal Interfaces x 1000

Sources: 14. DASC Boston, MA Nov. 1995 & Airbus Data

ASES Advanced Systems Engineering Solutions

# Emergence, Hidden Links and Dys-Functionality




..... "hidden links" are subject to the actual operation conditions

ASES
Advanced Systems Engineering Solutions

# “ARIANE V” Accident by Re-Use of “ARIANE IV” IRS ➔ EMERGENCE

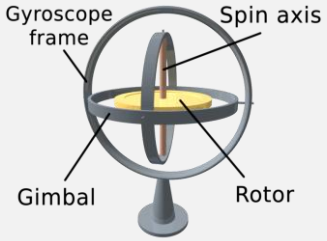
***4. Juni1996, Kourou / French Guyana: Maiden Flight* of Carrier Rocket Ariane V :**

**Inertial Reference System fault “aligment mode” disconnects Fight control ➔**

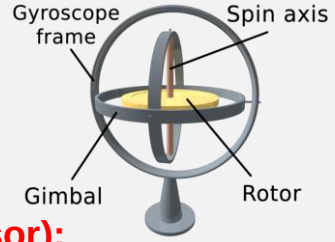
**„format error at „horizontal_velocity“ (64-bit real ➔ 16-bit Integer)**


```
declare
vertical_veloc_sensor: float;
horizontal_veloc_sensor: float;
vertical_veloc_bias: integer;
horizontal_veloc_bias: integer;
...
begin
declare
pragma suppress(numeric_error, horizontal_veloc_bias);
begin
sensor_get(vertical_veloc_sensor);
sensor_get(horizontal_veloc_sensor);
vertical_veloc_bias := integer(vertical_veloc_sensor);
horizontal_veloc_bias := integer(horizontal_veloc_sensor);
...
exception
when numeric_error => calculate_vertical_veloc();
when others => use_irs1();
end;
end irs2;
```

**IRS #1**




**IRS #2**



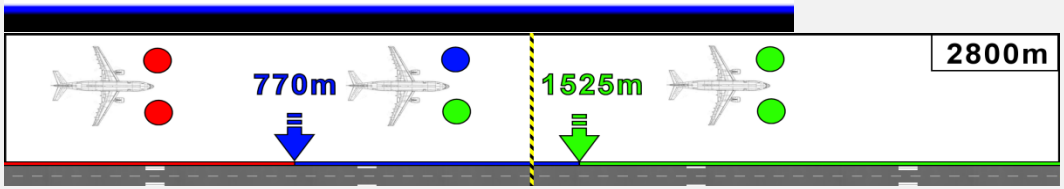

ASES Advanced Systems Engineering Solutions

# The Warsaw Accident September 14th , 1993 ➔ Dys-Functional Operation

**on May 26th 1991 a Lauda Air Aircraft had been torn into pieces at 24.700ft cruise altitude and crashed, because the engine#1 thrust-reverser unintentionally had been activated. Consequently a logic is installed to all Airbus Aircraft, which prevents the automatic activation of Thrust Reversers and Air Brakes (the „Auto Break“ Function), if the Flight Status does not indicate: „A/C on Ground“ (weight on both wheels > 12 tons, wheels rotating > 72 kts, altitude below 20ft).**

**Two years later at Warsaw: Strong cross-wind, heavy rain, slippery runway, length 2.800 meter. Bank angel landing: right MLG wheel touch-down at 770 m, left MLG wheel late at 1525 m. „Auto-Brake“ selected. Aquaplaning (no wheel speed) and weight only on one wheel indicate: „A/C in Flight“. The Automatic consequently does not release the brakes until both wheels get weight and rotate. Despite full braking (wheels, air brakes, thrust reverser), the aircraft overrun the runway.**

**Result: Collision with a mound, crash, fire, 2 fatalities, 54 injured.**

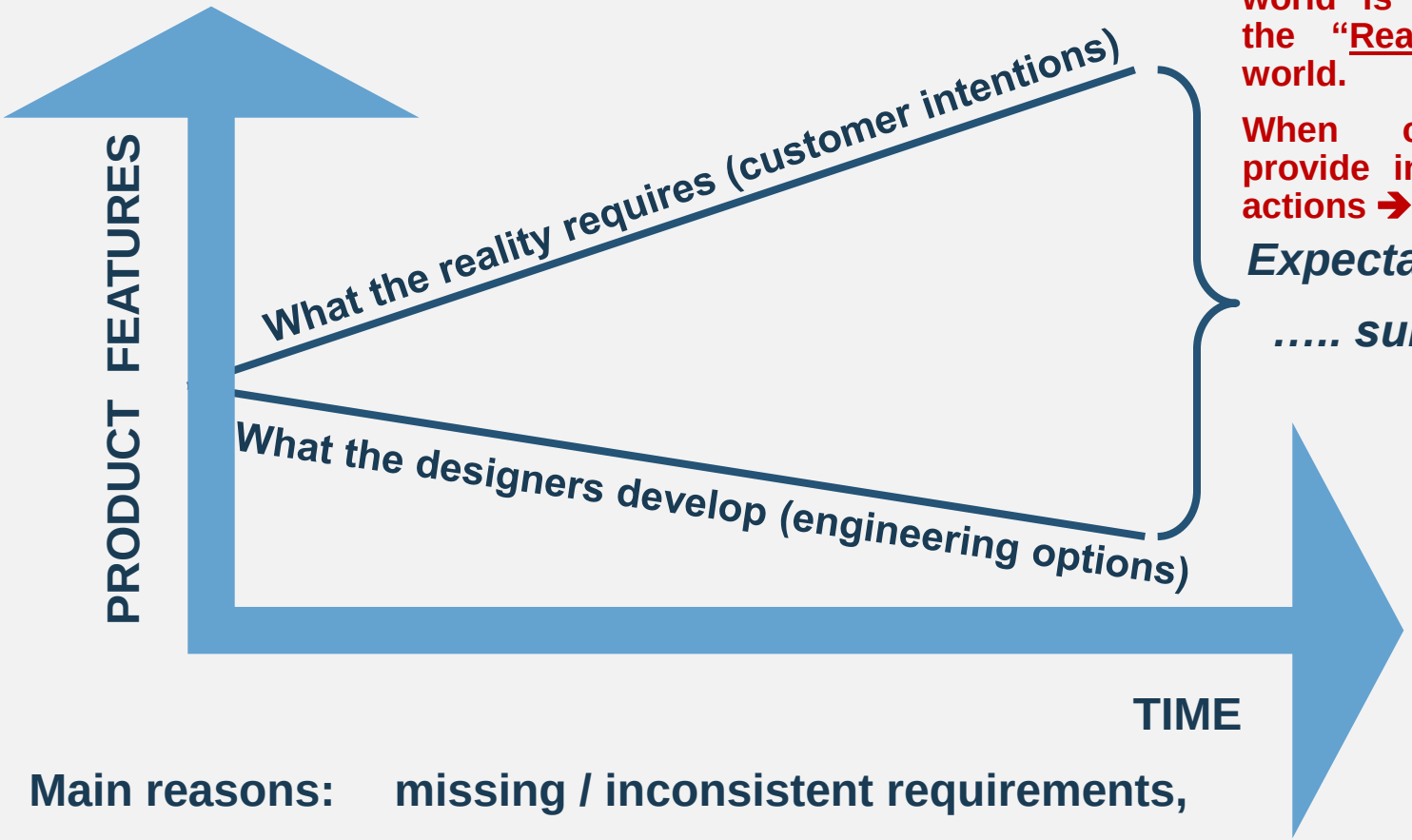





ASES Advanced Systems Engineering Solutions

# The Expectation Gap at the End of the “classical” V-Model

## Effect of incomplete state space prognosis and constraint definition




The ”Model” of the real world is inconsistent with the “Real State” of the world.

When controllers then provide inadequate control actions ➔ Accidents occur.

*Expectation gap*

*….. surprise!!!*

The knowledge of the system states (the Right Model) is critical at

- Design and
- Operation

**Main reasons:** missing / inconsistent requirements, misperceptions, unforeseen states, “hidden” links ➔ in short: Wrong Models

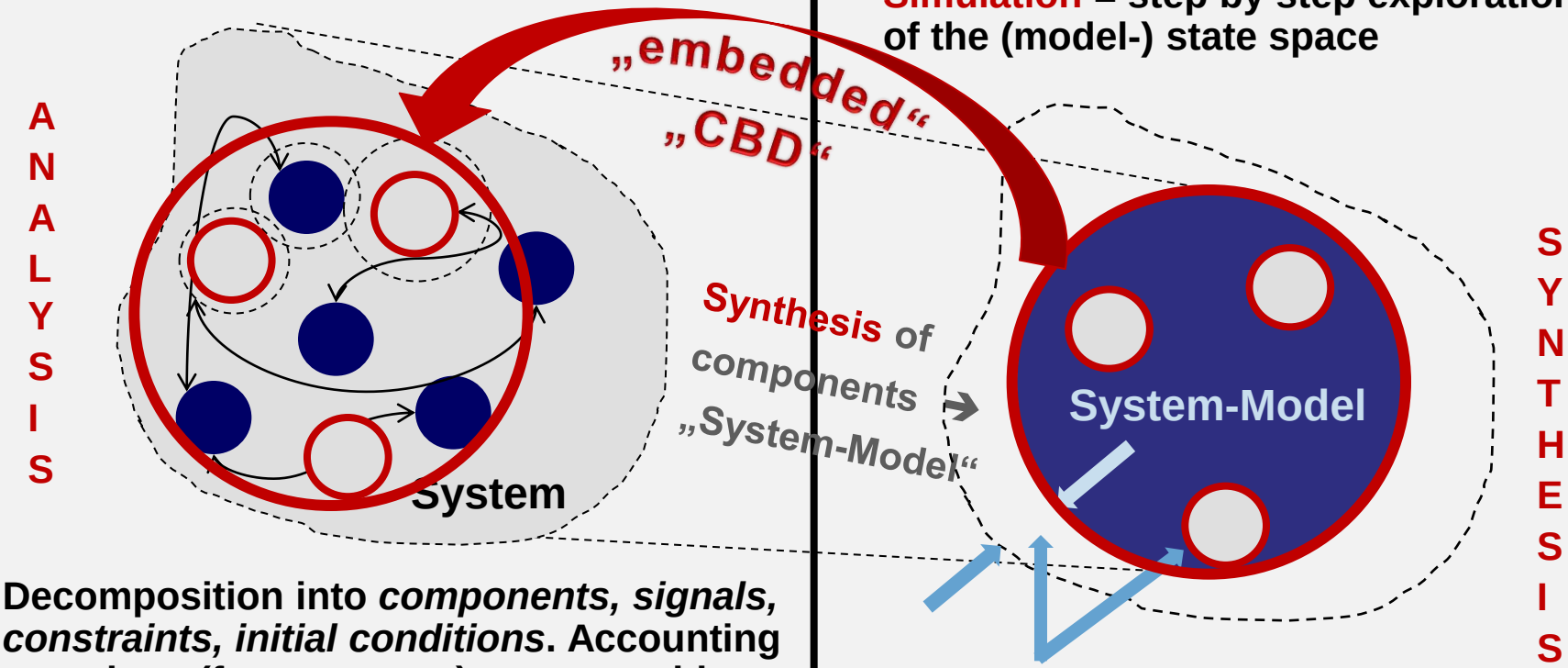
ASES
Advanced Systems Engineering Solutions

# Model Based Design (MBD): State Space Anticipation Aid

**Real World = Ambiguous Reality**

**„Formal“ World = Reasonable Model**

**Simulation** = step by step exploration of the (model-) state space




**Decomposition into *components, signals, constraints, initial conditions*. Accounting equations (force, energy), state machines**

**Components / Models (known state space)**

**Achievable state space**

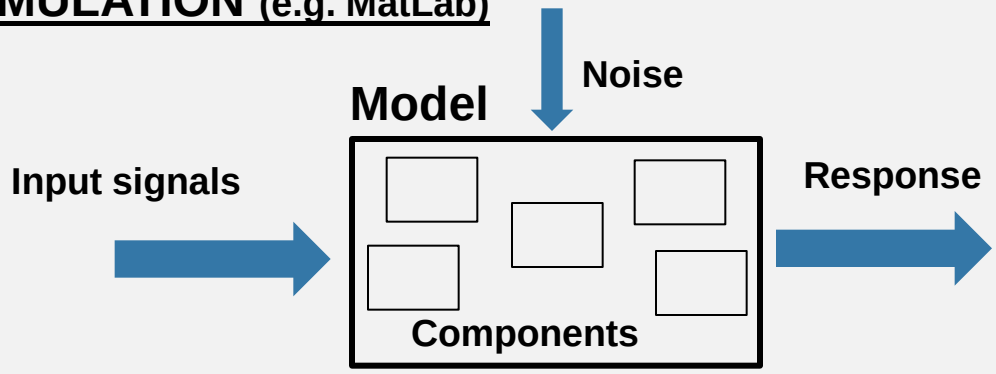
***„Terra Incognita“* – two options**

1. ***Exploration*** **(model expansion, Co-Simulation, Model Checking)**
2. ***Isolation*** **(surveillance, monitoring)**

ASES
Advanced Systems Engineering Solutions

# Anticipation by (Co-)Simulation

## SIMULATION (e.g. MatLab)

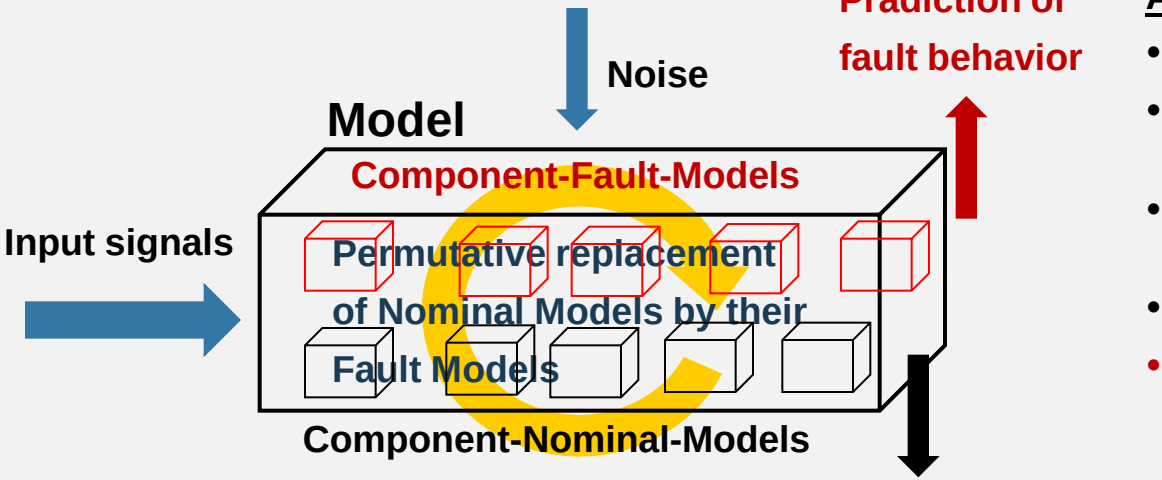



**Analysis: Prediction of**

- I/O behavior
- error detection / compensation
- parameter sensitivity
- concept Validation
- Some „Terra Incognita“ remains due to: time and state constraints

*“Essentially all models are wrong, but some models are useful” - George E. P. Box, 1919 - 2013*

## CO-SIMULATION (e.g. RODON)

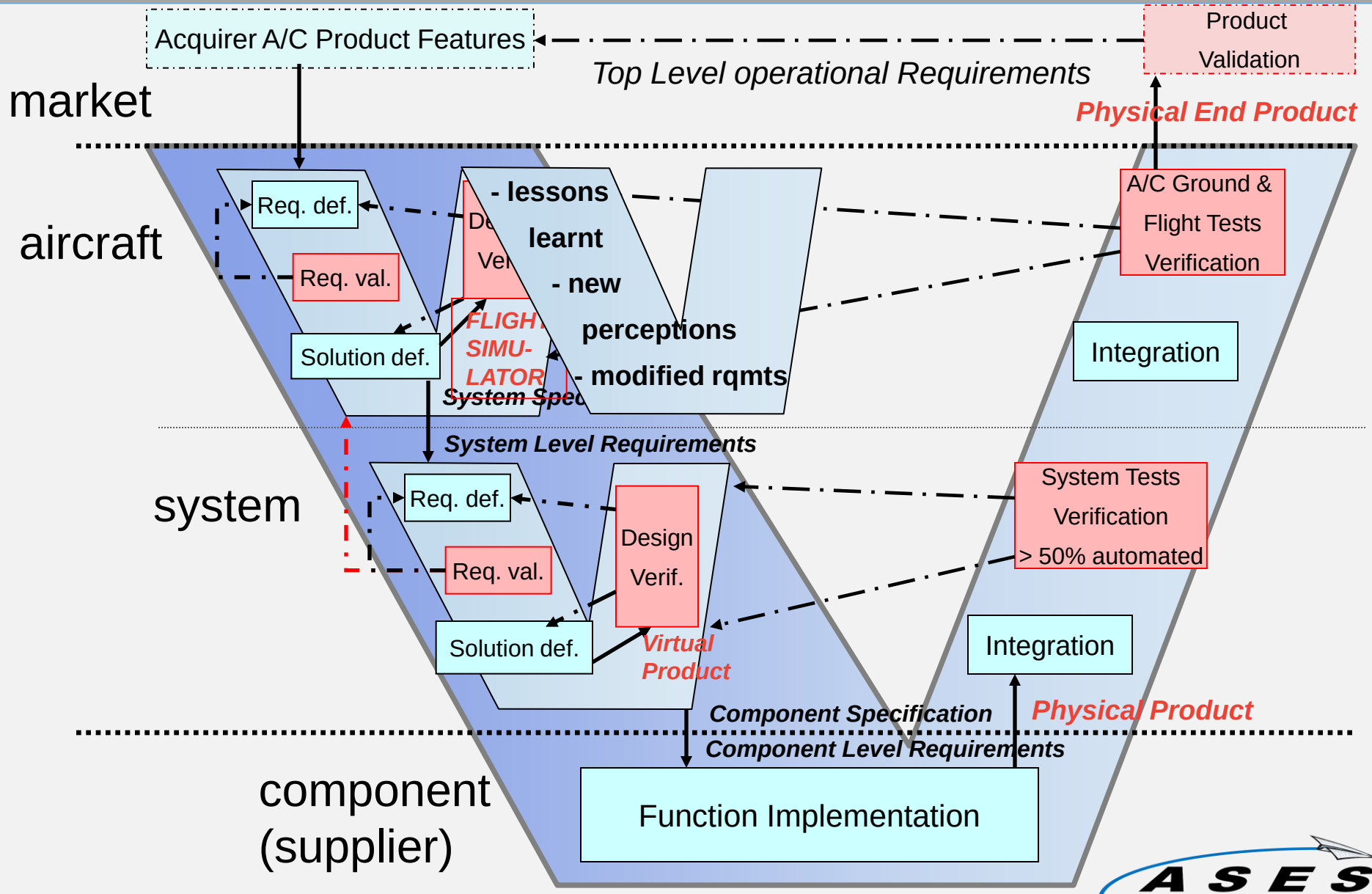



**Analysis: Prediction of**

- Context-behavior
- Diagnosability of „arbitrary“ component-fault-combinations
- Applicable for „analogue“ and „discrete“ Systems.
- Can be automated
- „Terra Incognita“ smaller, however confined to steady state behavior

ASES Advanced Systems Engineering Solutions

# From V to W: Models in the Design Process



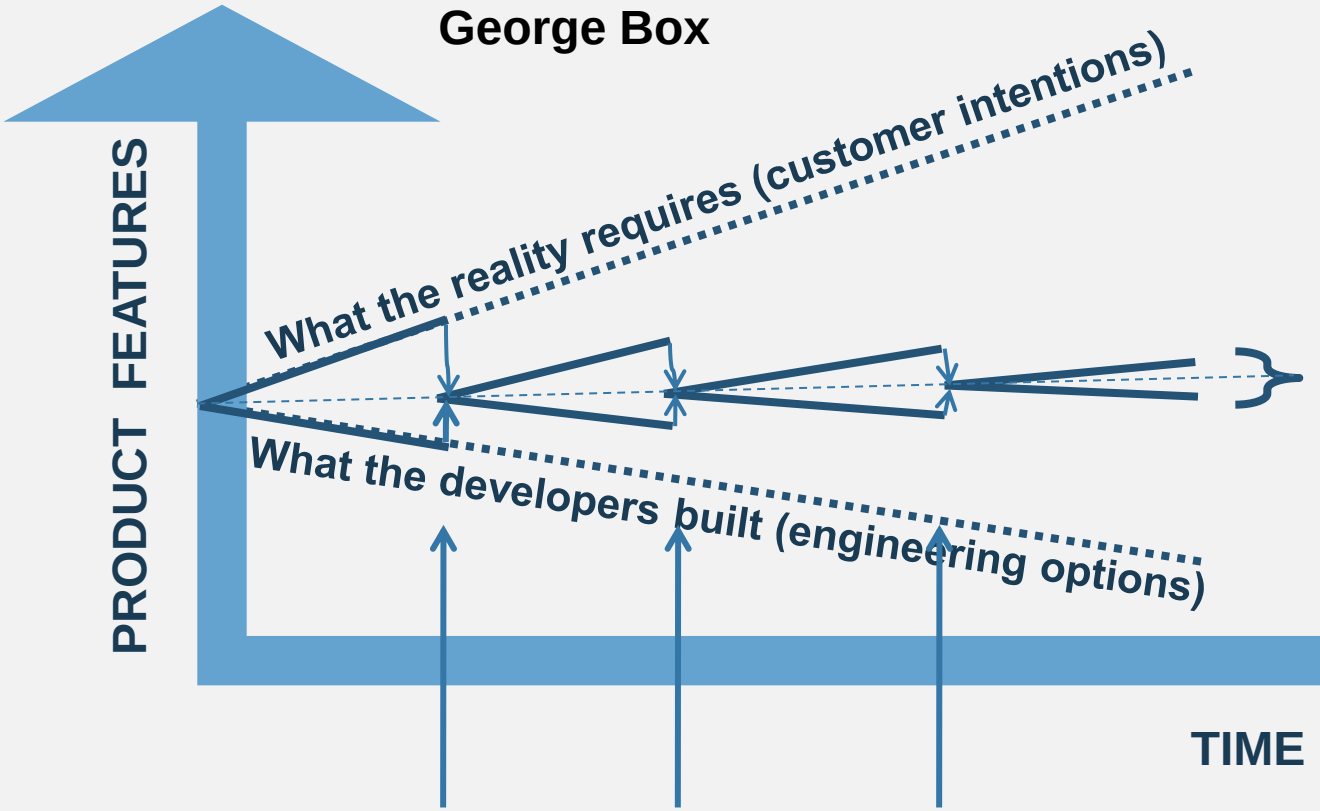



ASES Advanced Systems Engineering Solutions

# Shrink the Expectation Gap through state limitation

**“All models are wrong, some models are useful”**

**George Box**




***Expectation gap:***

**In terms of Safety still a risk.**

***How to close it?***

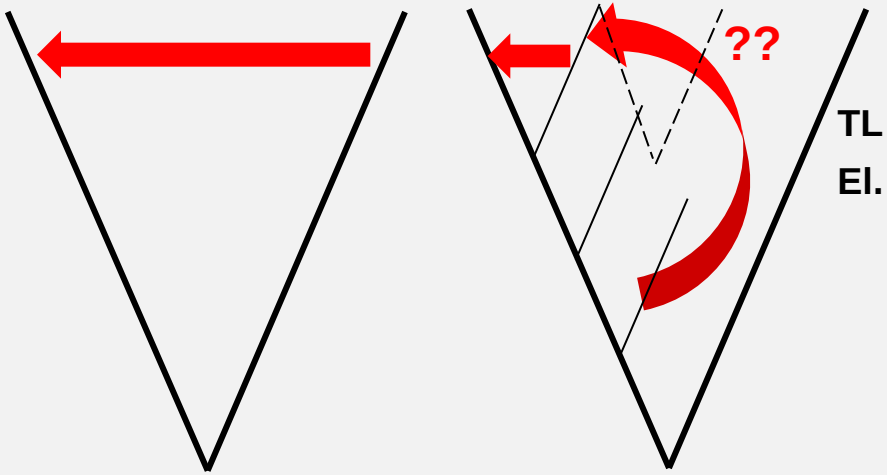
- **Simulation, virtual prototyping, performance- / cost-prognosis**
- **State space modeling, anticipation and limitation**
- **Design & Process model simulation for Reviews and RBE Validation**

ASES
Advanced Systems Engineering Solutions

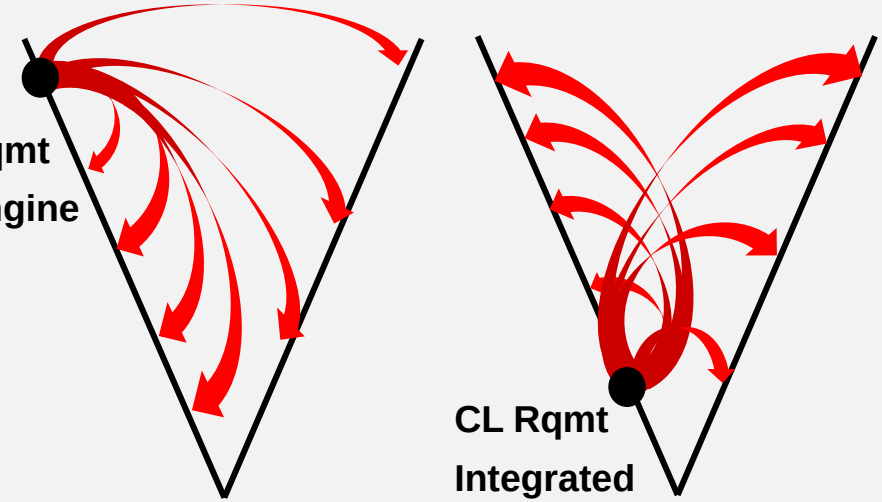
# From V by W to Contract Based Design

**The convential development approach**

**V / W Model: late-limited-low-range prognosis**




**The risk of hidden links require early, total, wide range state-space prognosis**




**"Total and large scale state-space-interoperability prognosis" can be achieved if the quantity of possible (admissible) states is kept low.**

**A „Contract" reduces the No. of states by translating Component Features into „Assumptions" vs. „Promises" Relations and by "Information Hiding"**

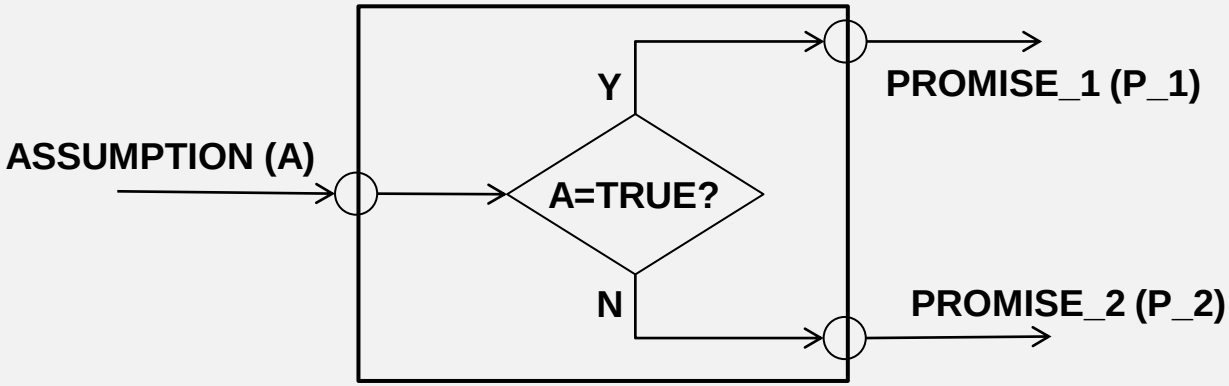


ASES Advanced Systems Engineering Solutions

# CONTRACT BASED DESIGN

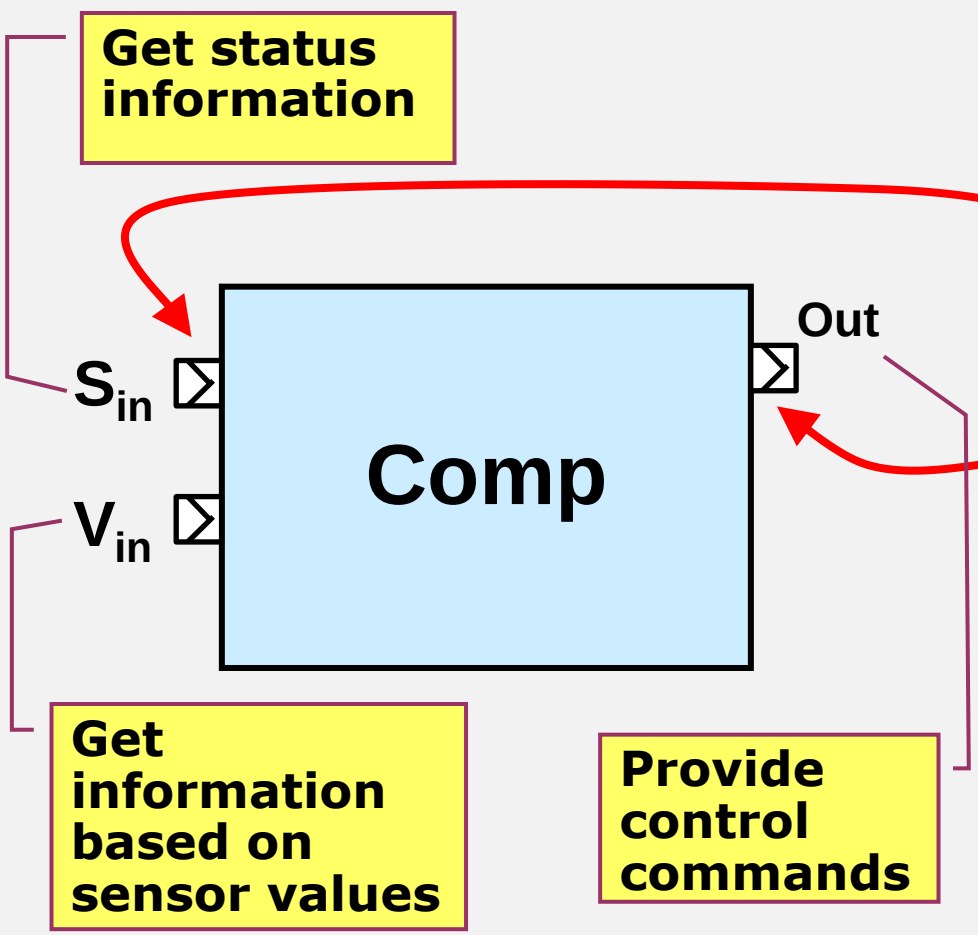
# The Idea behind Contract Based Design

**A system is composed of components, which mutually exchange / provide data and services – however, only under distinct conditions and constraints. I.e. each component feature an ASSUMPTION ➔ PROMISE relation, just like a legal contract**




**Contracts only reference ports. The component internal mechanisms, which make-up the contract are irrelevant. We call this „INFORMATION HIDING“. This rule considerably reduces the No. of states to be considered**

# Contract Example




## Contracts

**Assumption :**

$S_{in}$ available every 10 ms

AND $V_{in} < 10$

**Promise :**

IF $S_{in}$ == enabled AND $V_{in} < 10$

THEN

Out == $f(V_{in})$ WITHIN 100 ms

ELSE Out == 0

Contract Instantiation by e.g.:

Textual Pattern Language OR

Extended State Machines

ASES
Advanced Systems Engineering Solutions

# “Contract Backed Components” = High Integrity Bricks ➔ allow for Automatic Consistency Analysis & Prognosis

A “contract“ translates requirements into “clauses“:

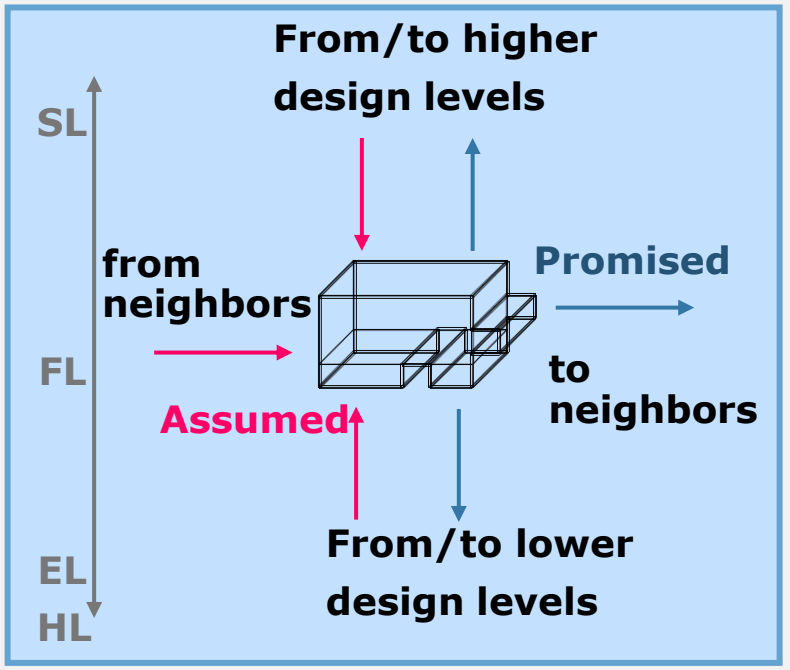
from: “if A > 10, signal B shall be send every 10ms“

get: **A** : “whenever A > 10 holds”

**P** : ”transmission of signal B occurs every 10ms”

(assumption vs. promise)

…. What’s about “A < 10” ???




- “Contracts” are dependable
- “Contracts” oblige to “Completeness”
- “Contracts” are “component” related
- “Contracts” considerably reduce the number of states
- the size of the selected components is arbitrary
- formalized “Contract Clauses” are suited for computer reasoning
- checkers can identify far reaching inconsistencies

ASES
Advanced Systems Engineering Solutions

# Why Design Defects occur with conventional RBE

## MBD

- **A model is an Abstraction of the Real System. i.e. an Incomplete Representation of the Real A – P Relations:**
- **A Model may assume different states than the Real System. This leads to ambiguous A – P relations.**
- **The validation of A-P relations between adjacent and remote components is not formalized ➔ „wide range" Interoperability Analysis questionable**

  ***This particularly applies to Composed Models***
- **➔ only Partial State-Space Vision and Prognosis**
- **➔ the "Analytical" Approach**

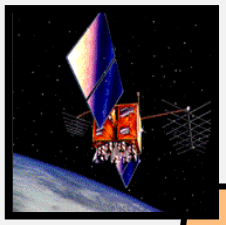
## CBD

- **complete specification of all A – P relations: the Contracts are the Real Representation of the Real System**

  **Formalized Provisions from component level to System level to keep the A – P relations, and only the A – P relations valid. Total suppression of invalid and contradictory A – P relations by *Satisfaction & Consistency Analysis* and Monitoring Means. *Also valid for Composed Components***
- **Complete validation of A – P relations between adjacent and (very) remote components by „*Compatibility & Dominance Analysis*"**
- **➔ Total State-Space Vision and Prognosis**
- **➔ "Synthetic" Approach**

# ARIANE V in Terms of “Components Decomposition“

## Virtual Integration



GPS

Navigation System

Flight Control

Inertial Reference System – IRS

IRS strap down calculus

Propulsion System

„ARIANE“ | „Air Frame“ Dynamic

ASES
Advanced Systems Engineering Solutions

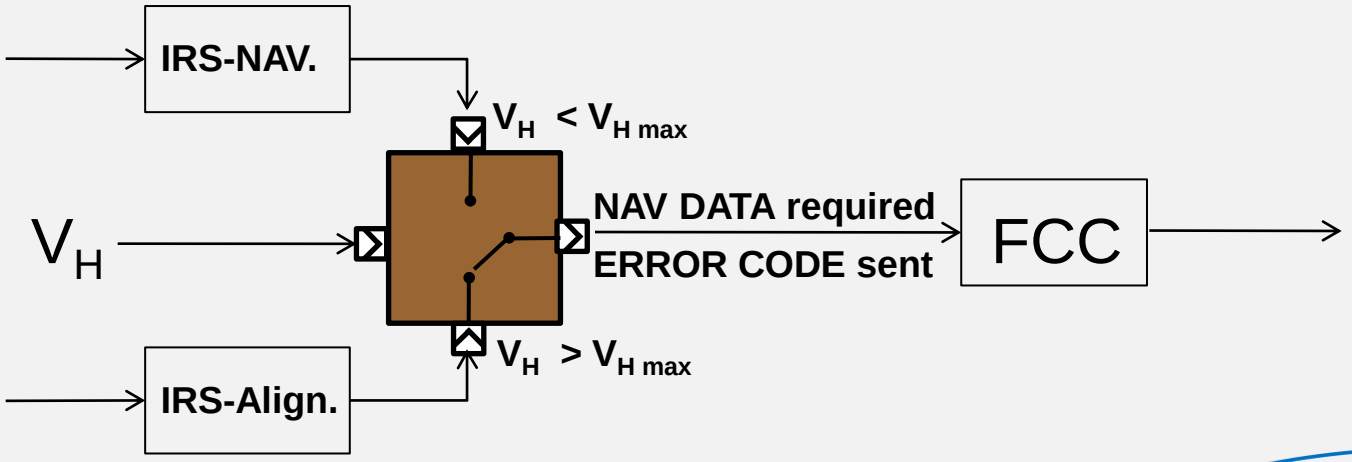
# Two A – P Relations that count

The alignment component signal output of the IRS can assume two different states, triggered by $V_H$

$V_H < V_{H\,max}$ → IRS-Align. → SILENT

$V_H > V_{H\,max}$ → IRS-Align. → ERROR CODE

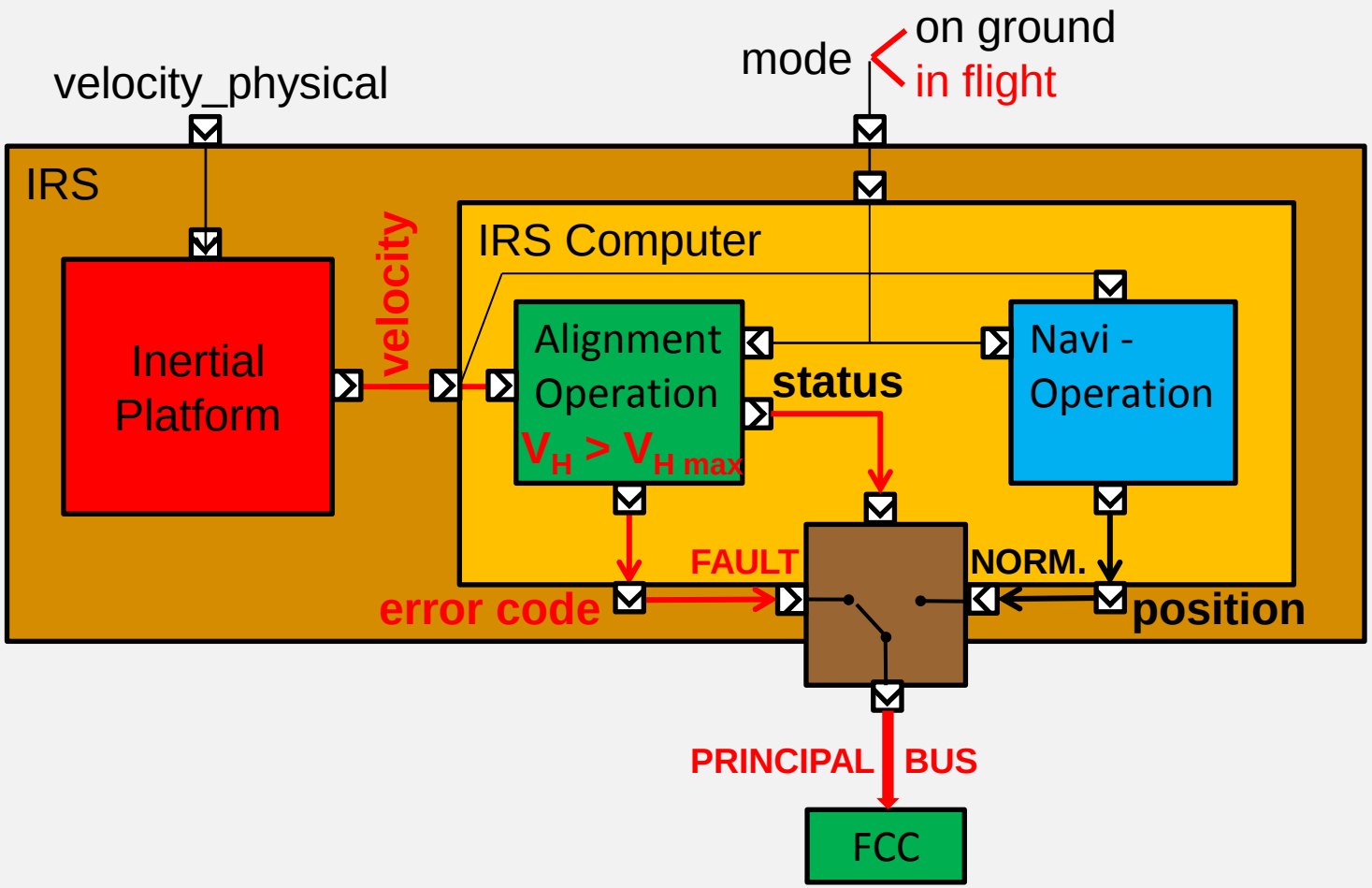
The FC component relies on the IRS to provide valid NAV data during flight operation





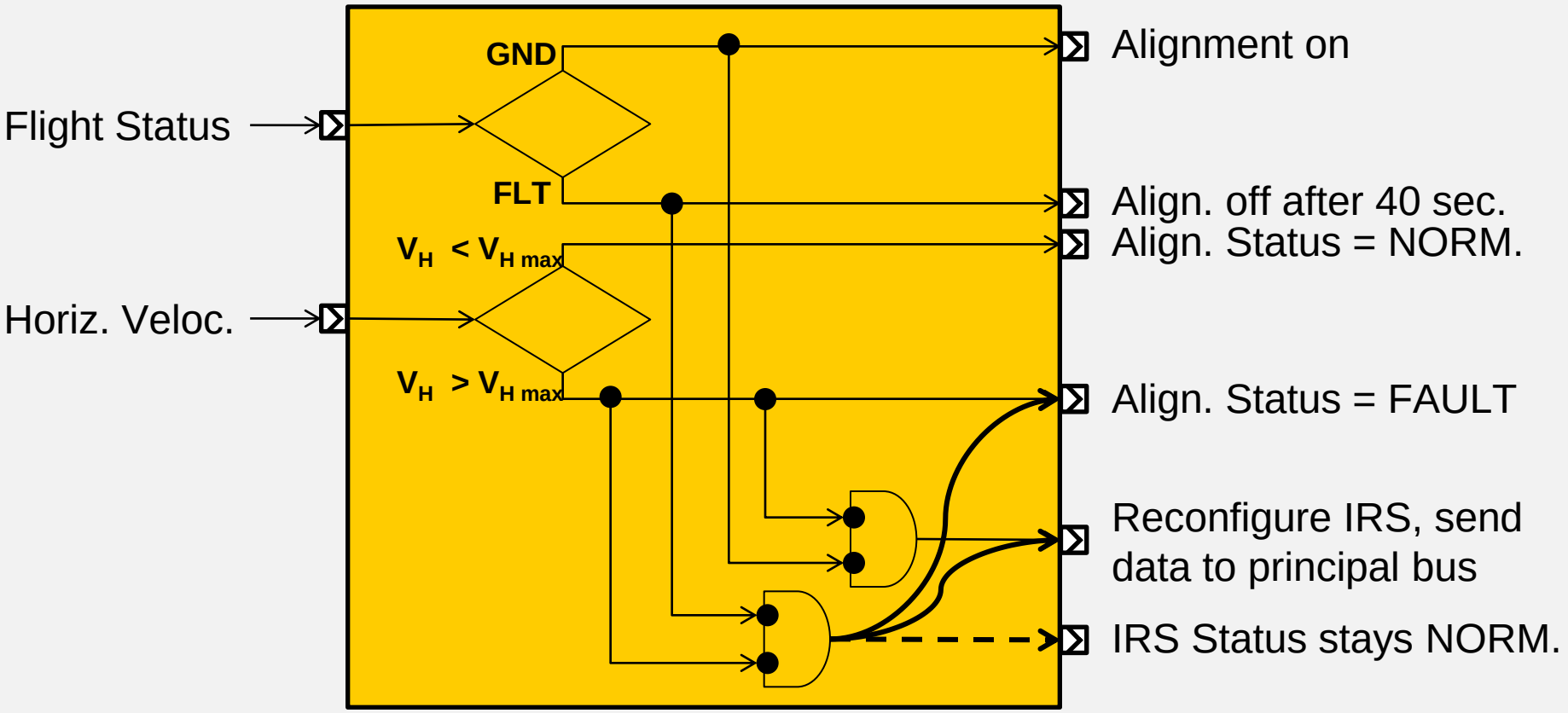

ASES Advanced Systems Engineering Solutions

# ARIANE V - Inertial Reference System (IRS)




Manifestation of the IRS components and their “hidden links”

# Contracts for Alignment Operation

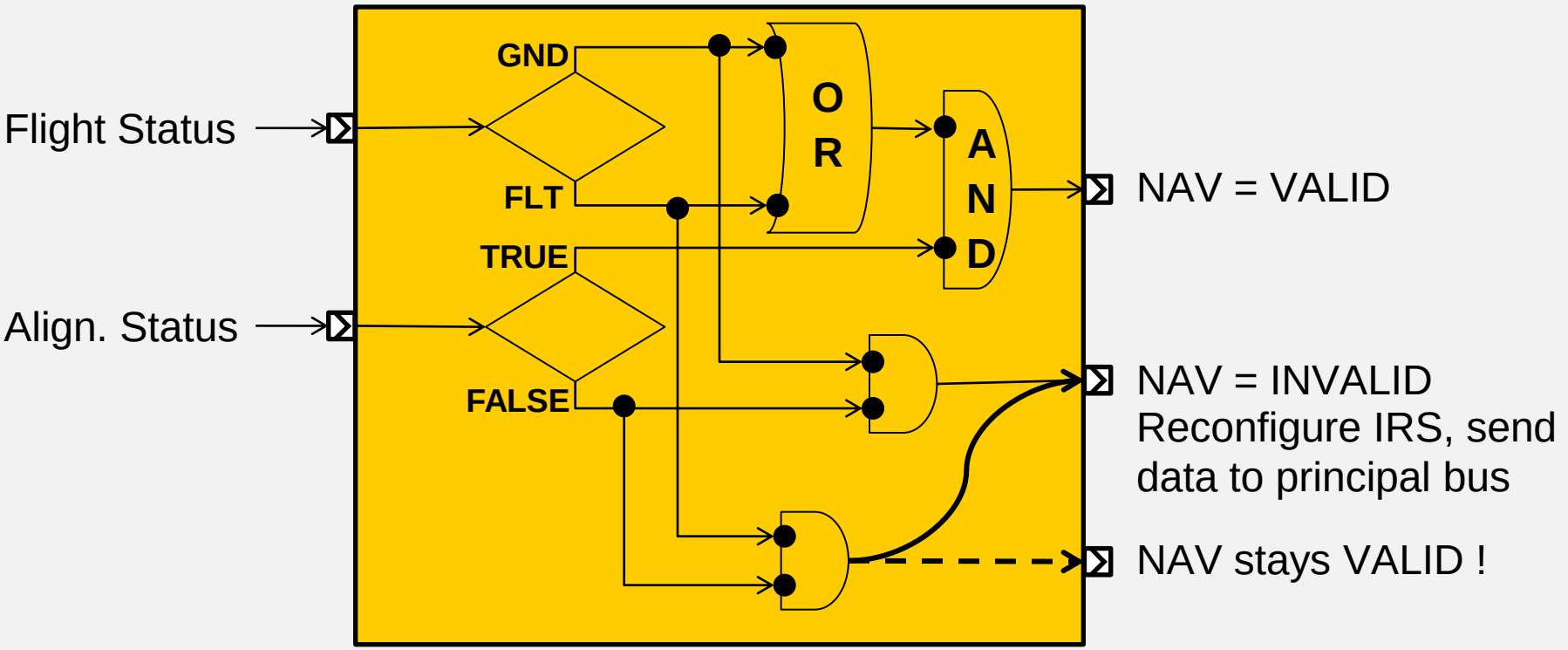



SATISFACTION: protect $V_H > V_{H\,max}$ at **Flight Status = FLT** ➔ clause is missing

CONSISTENCY: Alignment function reconfiguration at **Flight Status = FLT** ➔ contradiction to the needs (needless condition)

ASES Advanced Systems Engineering Solutions

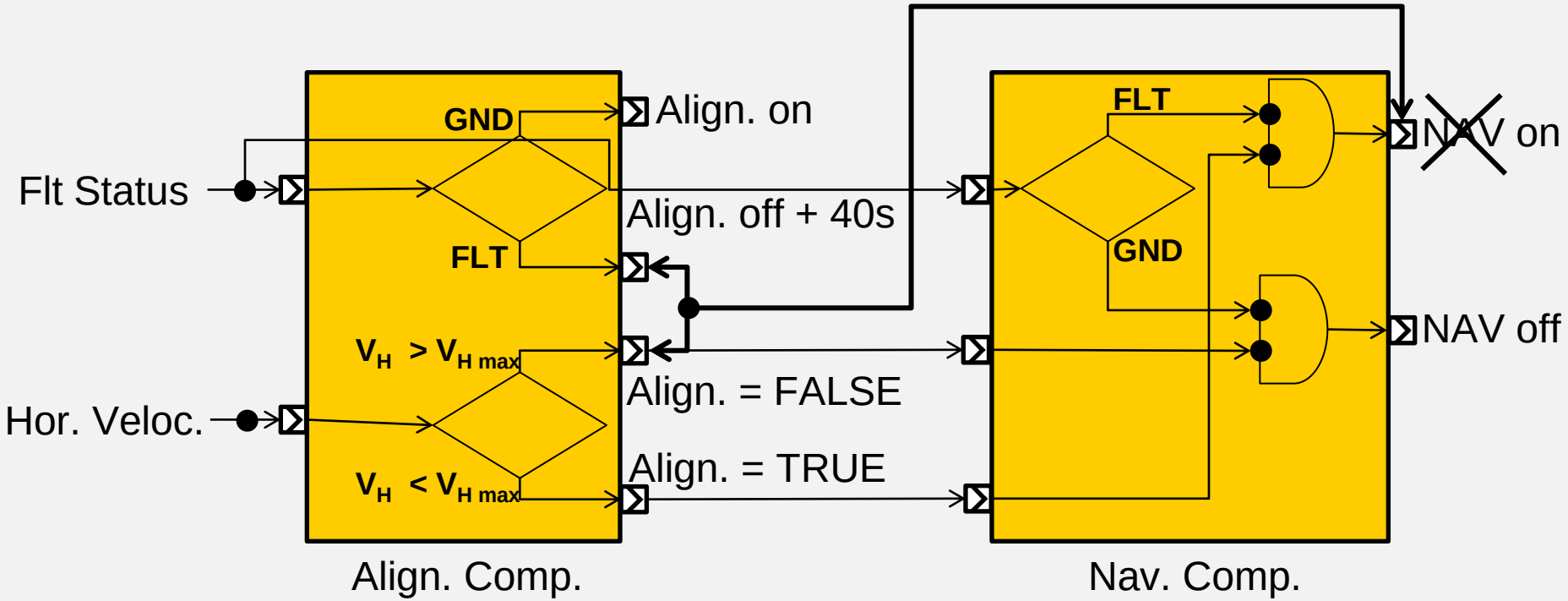
# Contracts for Navigation Operation




SATISFACTION: protect NAV against alignment errors at **Flight Status = FLT** ➔ clause is missing

CONSISTENCY: contradiction against fault tolerance to alignment errors at **Flight Status = FLT** ➔ sensless condition implemented

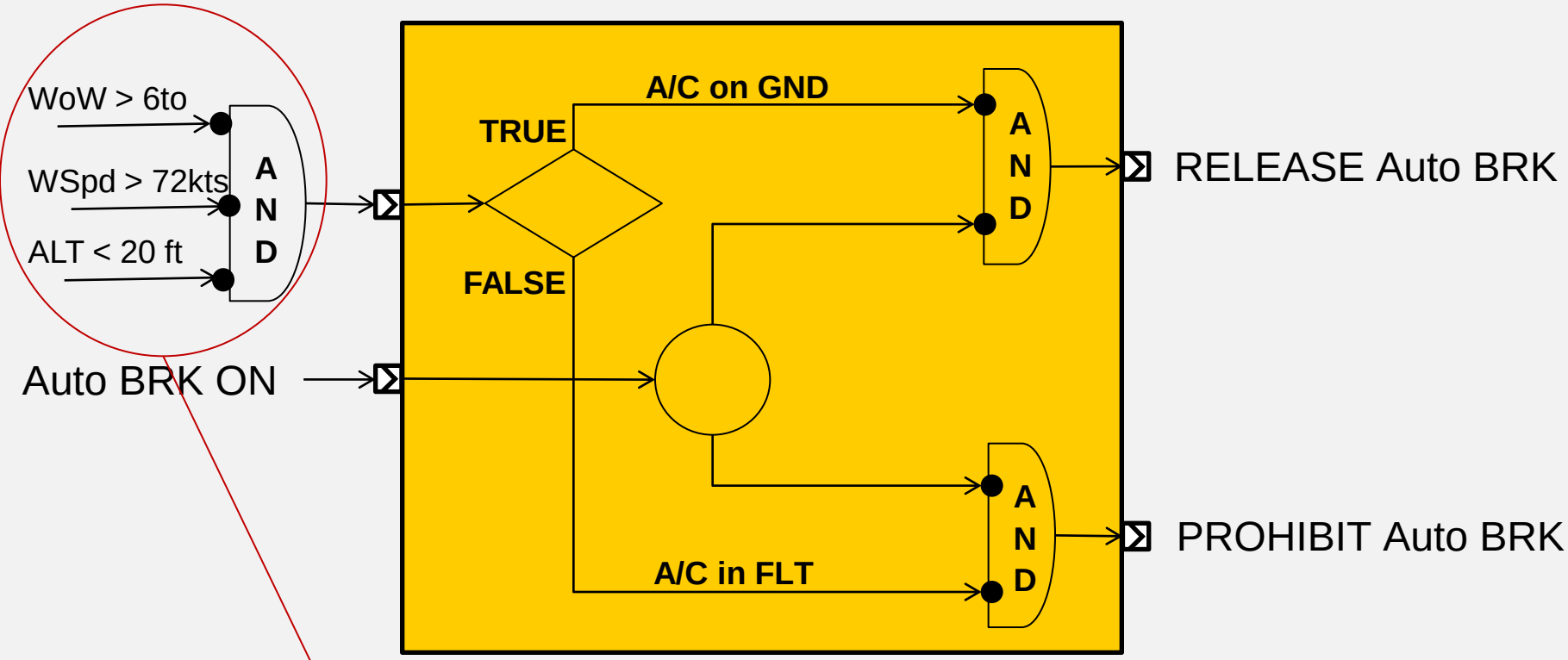
# Compatibility of Component Contracts




COMPATIBILITY: NAV Comp. has no contract on the Condition $V_H > V_{H\,max}$ **or**
**Alignment = FALSE** at **Flight Status = FLT** ➔
**Alignment = FALSE** circumvents NAV component

ASES
Advanced Systems
Engineering Solutions

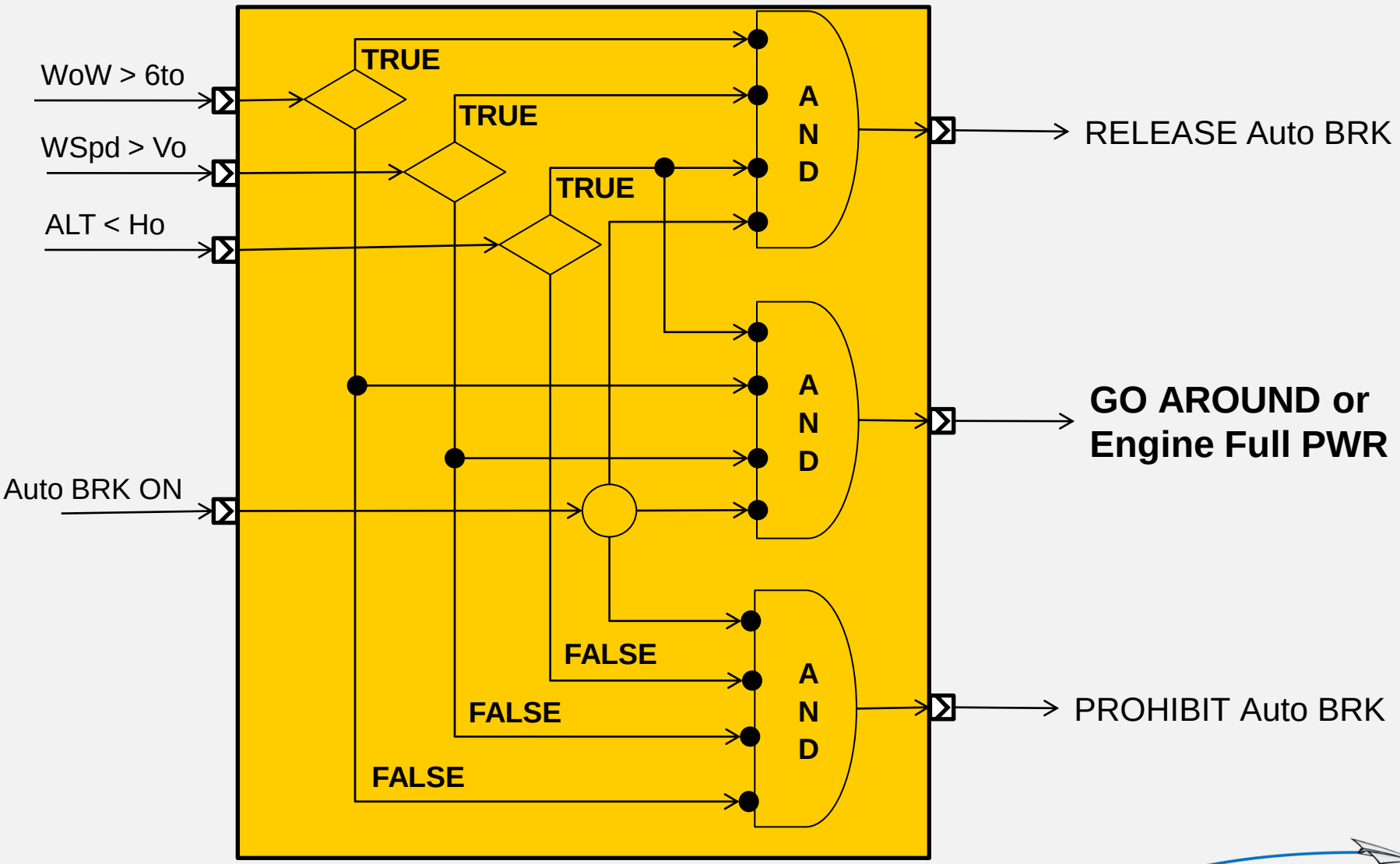
# Warsaw Accident, Auto-Brake as it was




COMPATIBILITY: the conditions of the assumption outside the contract may be incompatible with the conditions of the contract. They should be assessed in the frame of the contract.

DOMINANCE: the assumptions are not in line with the operational conditions of the aircraft („no braking at low altitudes“)

# Warzav Accident, Auto-Brake as it should be






ASES
Advanced Systems
Engineering Solutions

# LIFE CYCLE BENEFITS OF CBD PRODUCTS: EXAMPLE IMA

ASES
Advanced Systems
Engineering Solutions

# 3rd Example: Integrated Modular Avionic Design

Applications

Resource BITE

4

3

2

1

API Services

Operating system

Processor

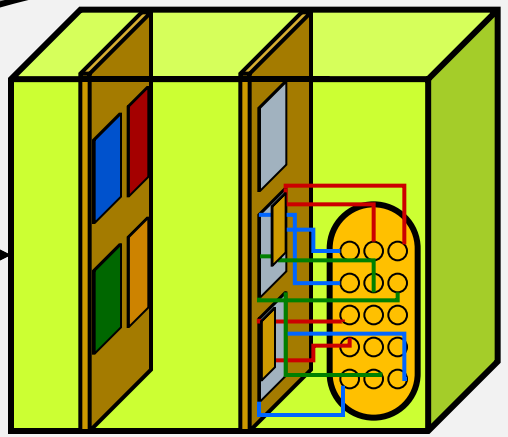
Plug

**Module**

IMA Module Contract

Module User Guide (**MUG**)

„Virtual Controller“



**Challenge: Interope-rability of virtual segments. Compatible if MUG is satisfied**



ASES Advanced Systems Engineering Solutions

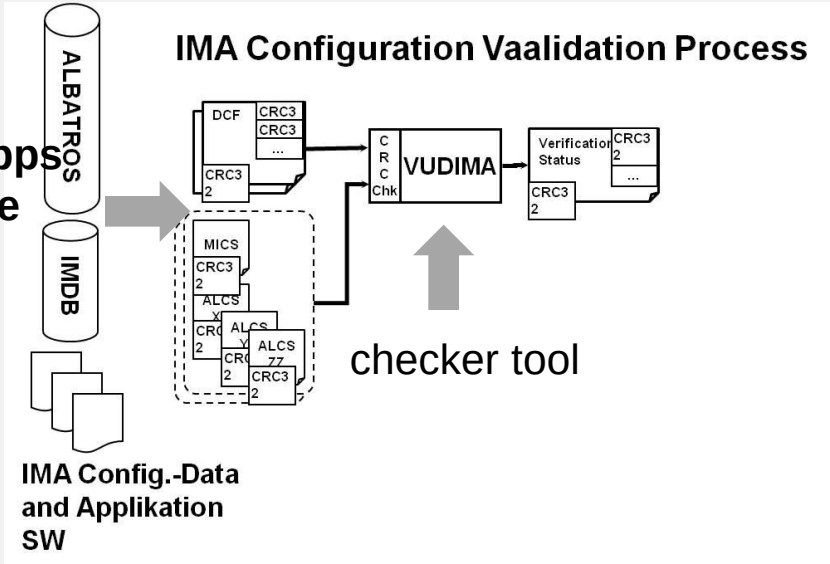
# IMA Contract Based Design Approach

The **“Contracts”** of the IMA platform are implemented into the **IMA API and several “Platform Services” (diagnostic, re-configuration, …)**. They are expressed by the **design rules** (in IMA terms **“Usage Domain”**) as laid down in the **MUG**. Here again, the integrity of the “Contract Clauses” is validated by **“Satisfaction”** and **“Consistency”** analysis in the frame of the **IMA supplier development process**.

**“Compatibility”** and **“Dominance”** verification is performed by the IMA integrator by checking the **configuration parameters** against the **“Usage Domain”** of the IMA Platform (MUG). Due to the huge amount of configuration parameters this task is executed with the help of a **qualified checker tool**.

**Achievements:**

- **no conflicts between remotely developed apps**
- **resource consumption visible at design time**
- **integration test replaced by formal configuration validation ➔**
- **saving some 10.000 tests**
- **easy modification, simply by configuration change and validation**






ASES
Advanced Systems
Engineering Solutions

# Conclusion

- **With growing complexity the integrity and fault tolerance of highly dependable systems is compromised**
- **Classical MBD and V-Model Processes are Analytical approaches to system design. They do not fully defeat the traps of complexity ➔ hidden links, emergence, dys-functionality ➔ too many unknown states, a hardly comprehensible, vast state space**
- **A way to defeat complexity is to reduce it.**
- **Component Contract Based Design cuts down complexity by assembling safeguarded, state-reduced bricks with formally executable checking options**
- **CBD is an “inverted” / “synthetic” approach to system design: it implements A- P confined models into reality.**
- **Broad application of CBD will create a more deterministic and dependable reality**

# Finis !

## Many Thanks !

## Questions ?

mailto:henningbutz@web.de

ASES
Advanced Systems
Engineering Solutions