THALES

Rebalancing Safety
Design, Assessment, Assurance

Emmanuel LEDINOT
TRT France, Palaiseau

ERTS 2020, Toulouse 31 Janvier

Embedded France Working Group

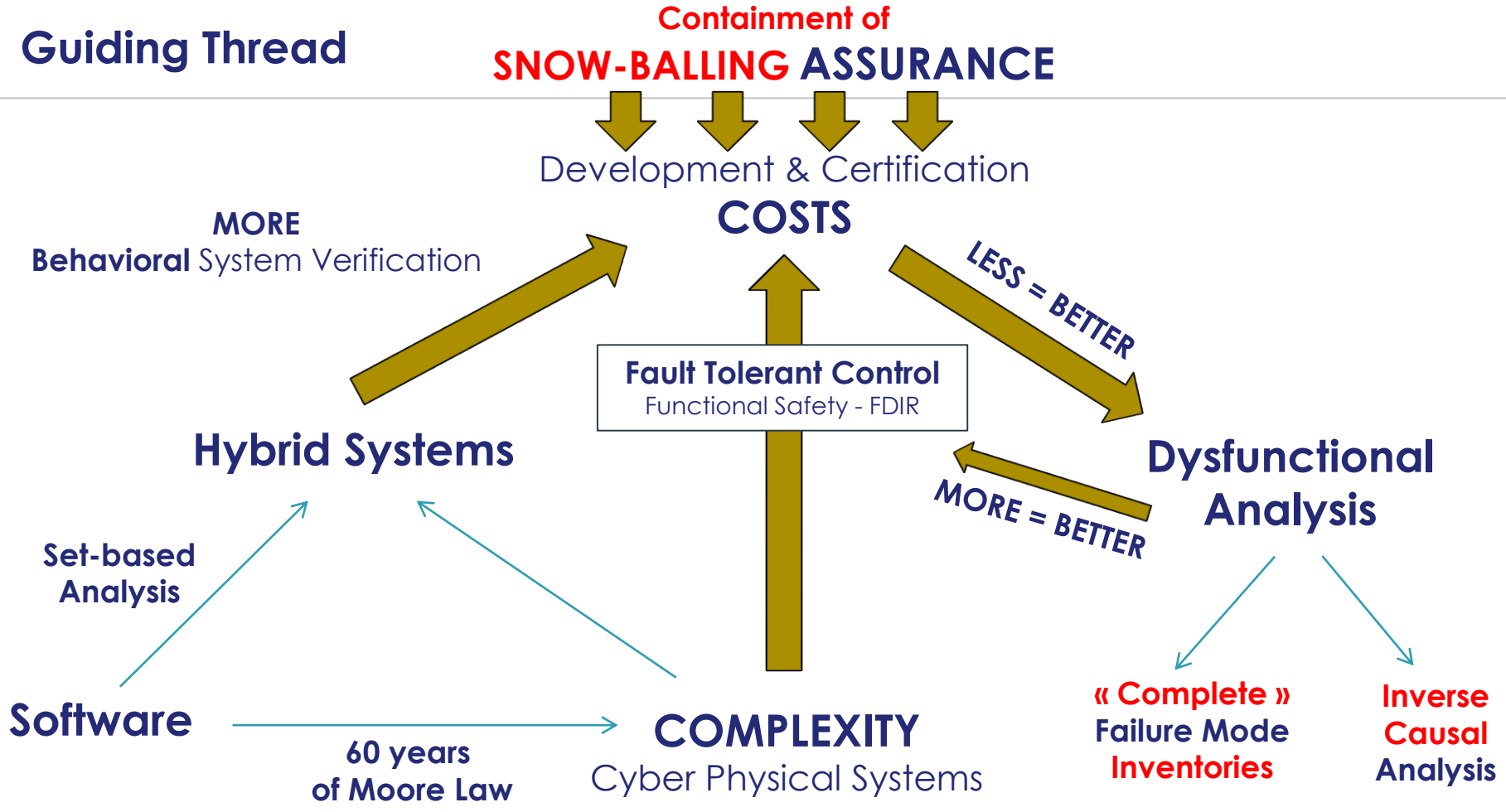
Special Thanks to

- J.P BLANQUART (Airbus D&S) and J. GASSINO (IRSN)

Rémy ASTIER (Rolls Royce)
Philippe BAUFRETON(SAFRAN)
Jean Paul BLANQUART (Airbus Defence & Space)
Jean Louis BOULANGER (CERTIFER)
Jean Louis CAMUS (ANSYS)
Cyrille COMAR (AdaCore)
Gilles DELEUZE (EDF)
Jean GASSINO (IRSN)
Philippe QUERE (Renault)
Bertrand RICQUE (SAFRAN)

THALES

Guiding Thread



THALES

SAFETY – The Paradigm Shift

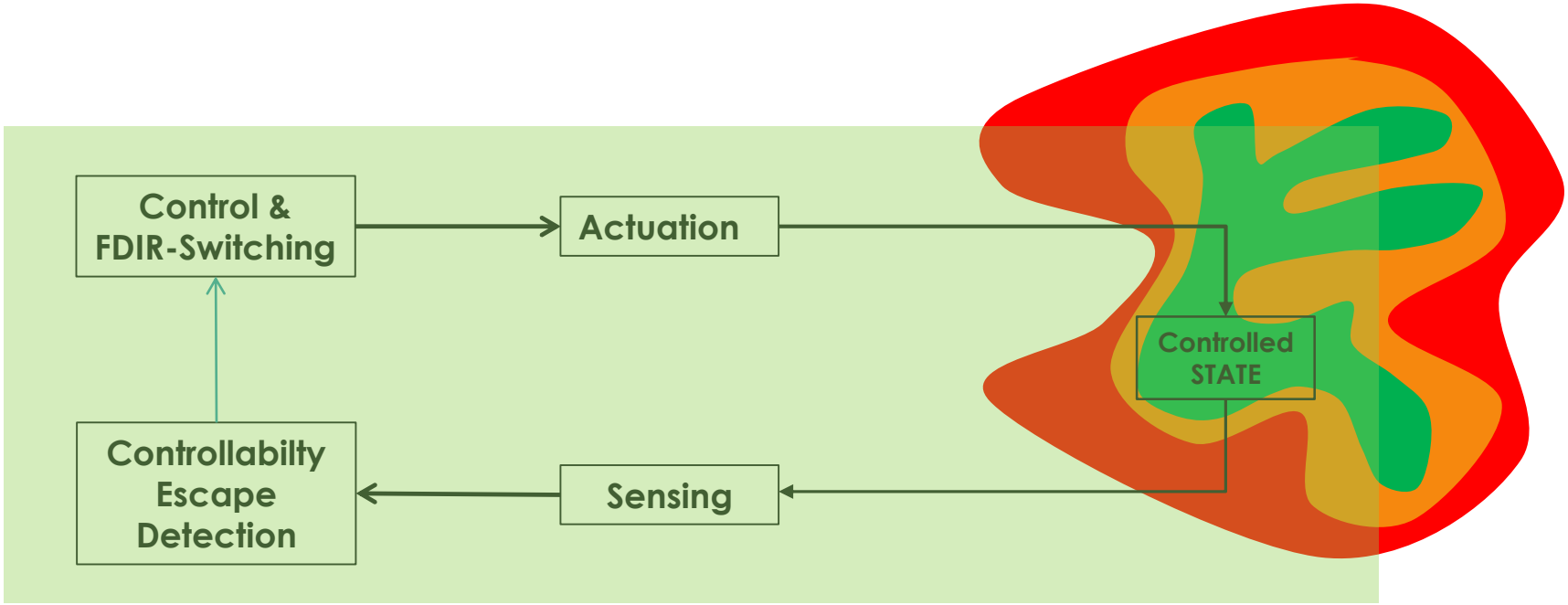
- Controllability Approach (e.g. STAMP/STPA)
- For Design, Assessment, and Assurance

THALES

The Controllability Shift (Integrated Safety)

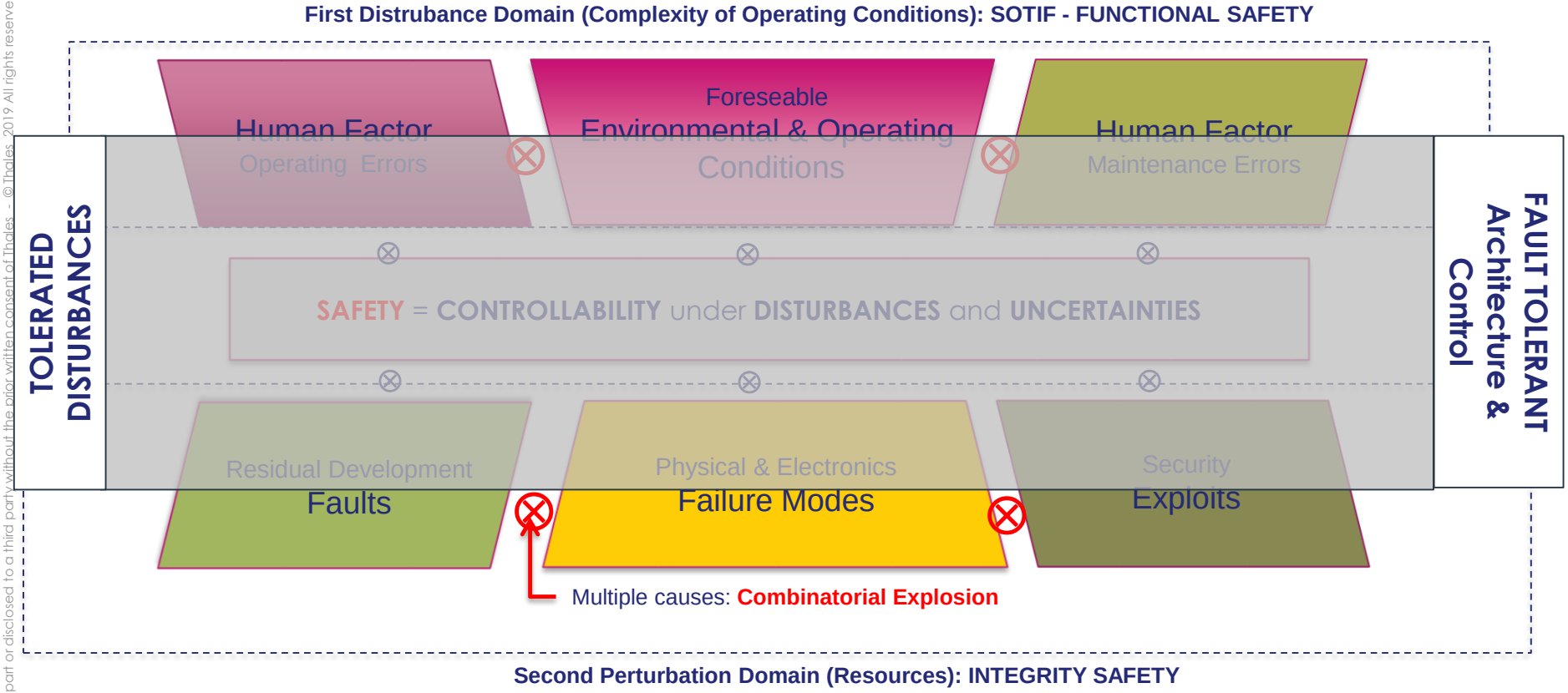
GREEN Engineering: **embedded in the product** to keep the **dynamics in the Green**

RED Engineering: **NOT in the product** (Integrity). What « pushes » the **dynamics in the Red**



THALES

Safety Design & Assessment – The Controllability View



THALES

Emerging Model-based *System* Verification Techniques

- System Structural Analysis
- System Behavioral Analysis

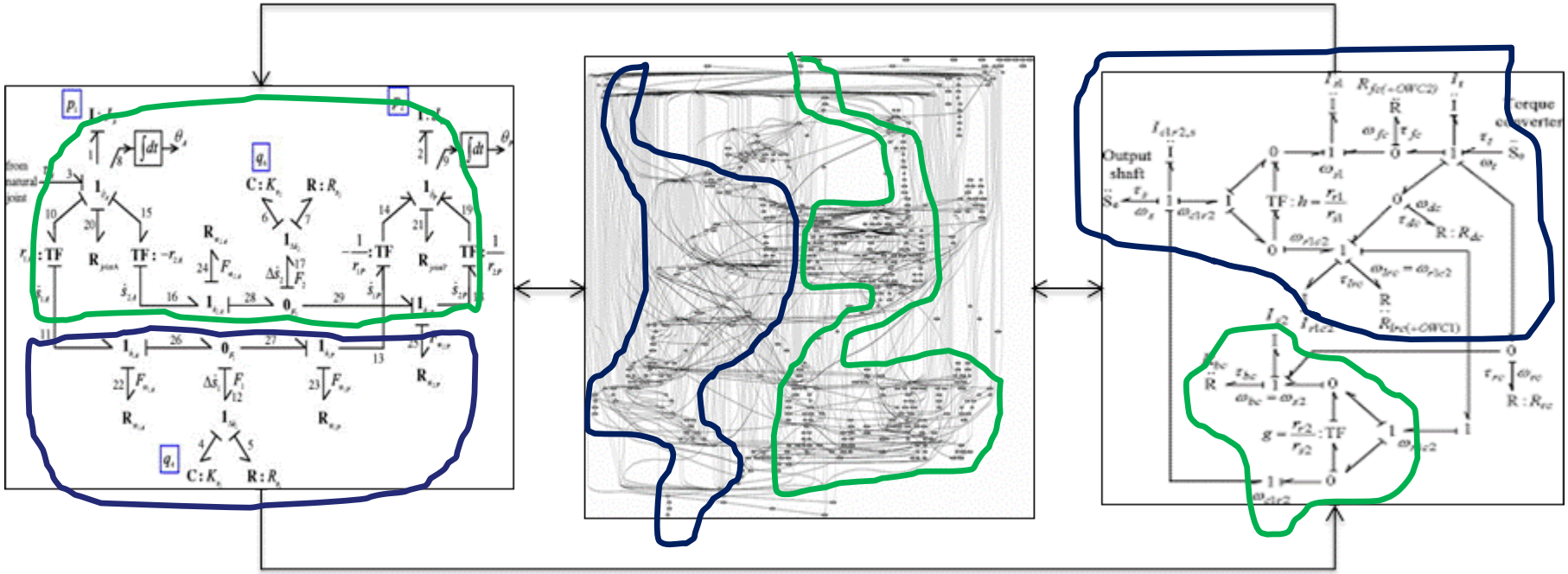
Affordable VerificationTool Qualification: a Critical Issue

THALES

Enhancement of CPS Structural Analysis

Digital –Physical Causal **Influence Networks**
- Forward Influence Cones **(TRL 6+)**
- Backward Influence Cones **(TRL 6+)**

SEPARATION
Functional **Independence** (Failure **Containment**)
Resource **Independence** (Fault **Contaiment**)



THALES

Set-Based Hybrid System Analysis (TRL 2 to 4)

Why ?

- For **System Behavioral** Verification **Coverage** Analysis
- **Exhaustiveness** (local/low dimensional problems)

What ?

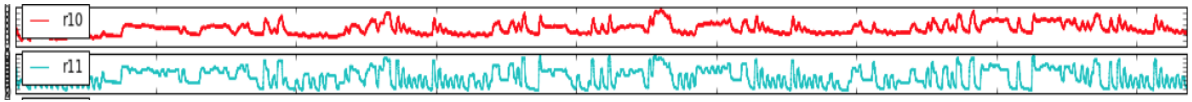
- **Invariant**-based **design** (design for verification)
- **Contract**-based specification
- Hybrid System **Model-Checking**
- Hybrid System Theorem Proving
- Algorithmic **Geometry** & **Topology** of **Physical Dynamics**

THALES

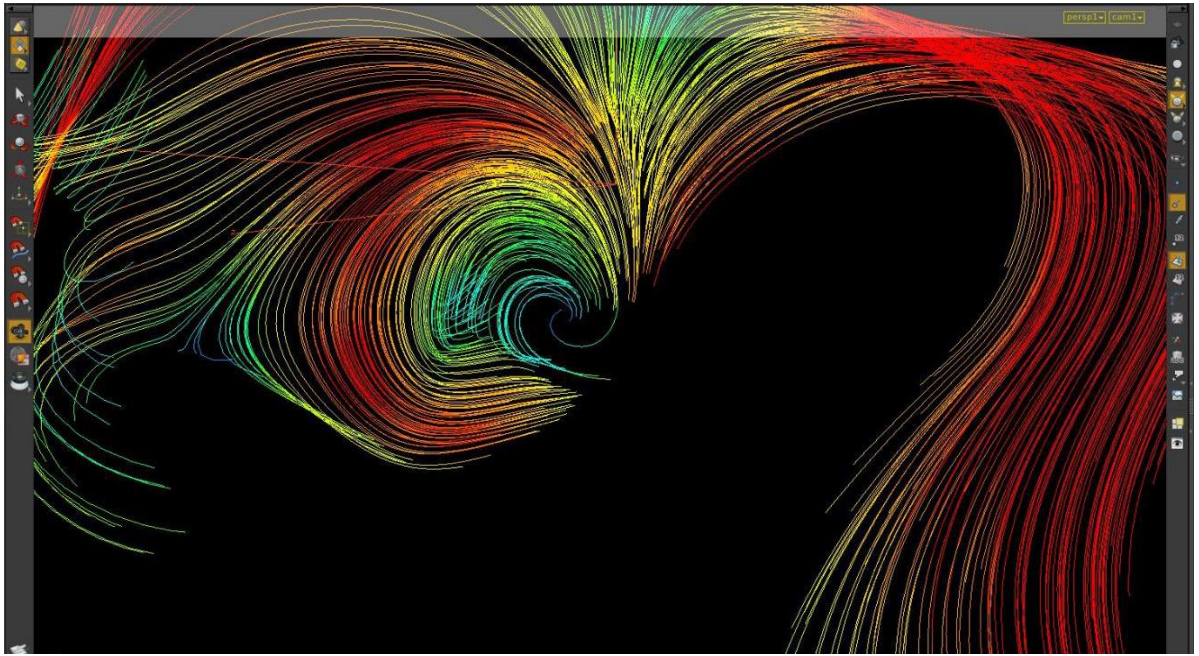
Set-based System Behavioral Verification: The Geometric Approach

2D Case

Time-Series View



Phase Portraits View

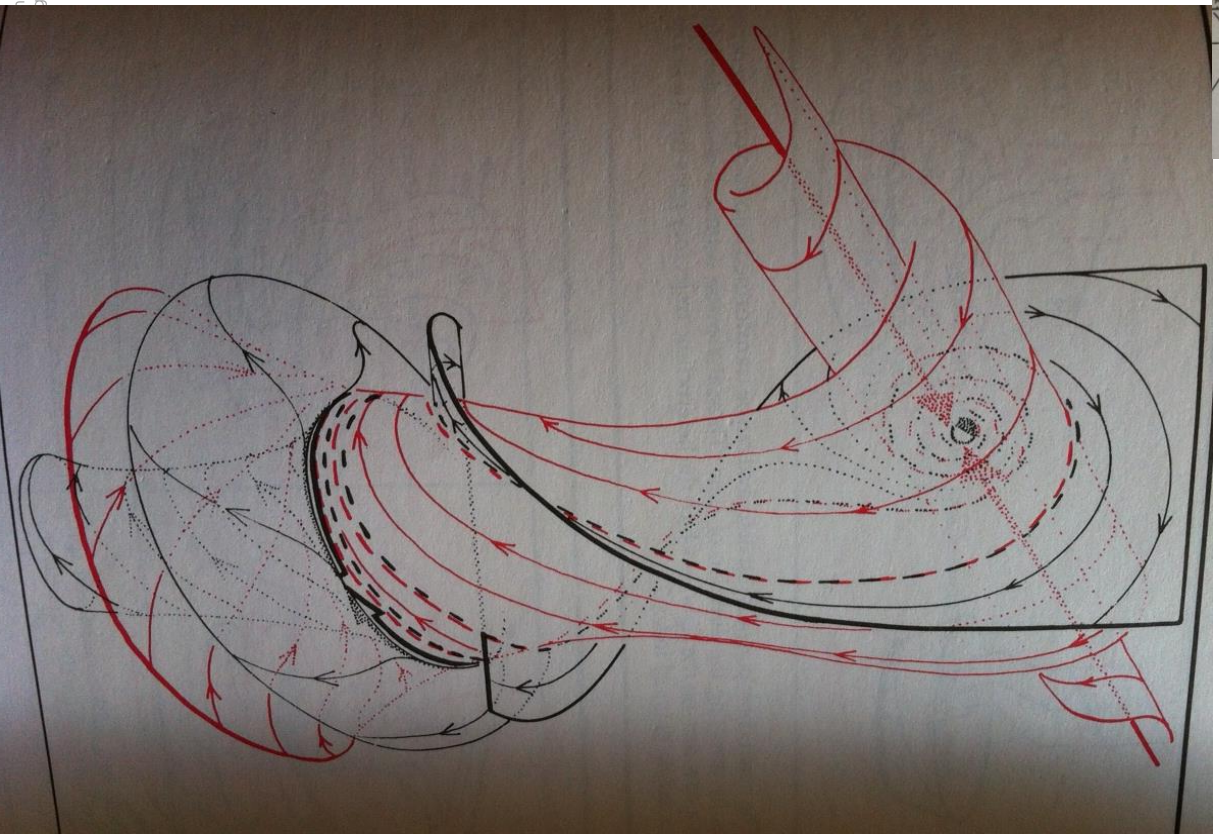


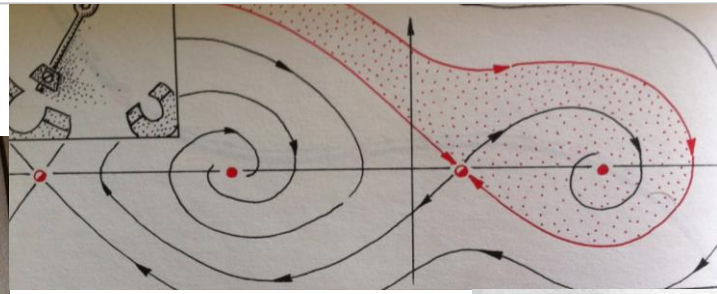
THALES

Geometry of Dynamics

R. Abraham & C. Shaw « **Dynamics, The Geometry of Behavior** » 1992

E. Ghys & J. Leys **«Chaos et Dimensions »** (2x DVDs)





NEW

1890

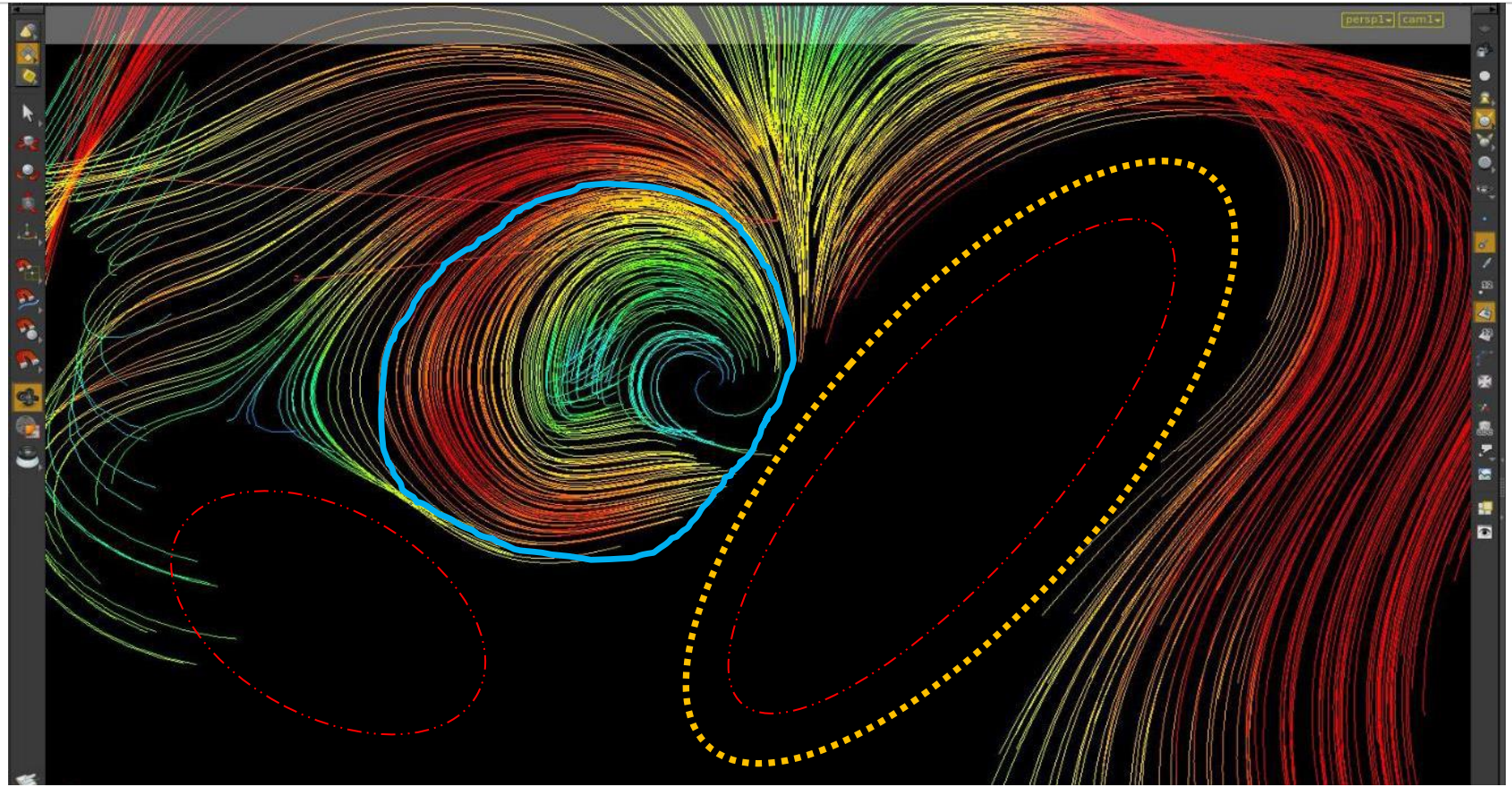
… But 201x for

D > 3

Computational Geometry Libraries

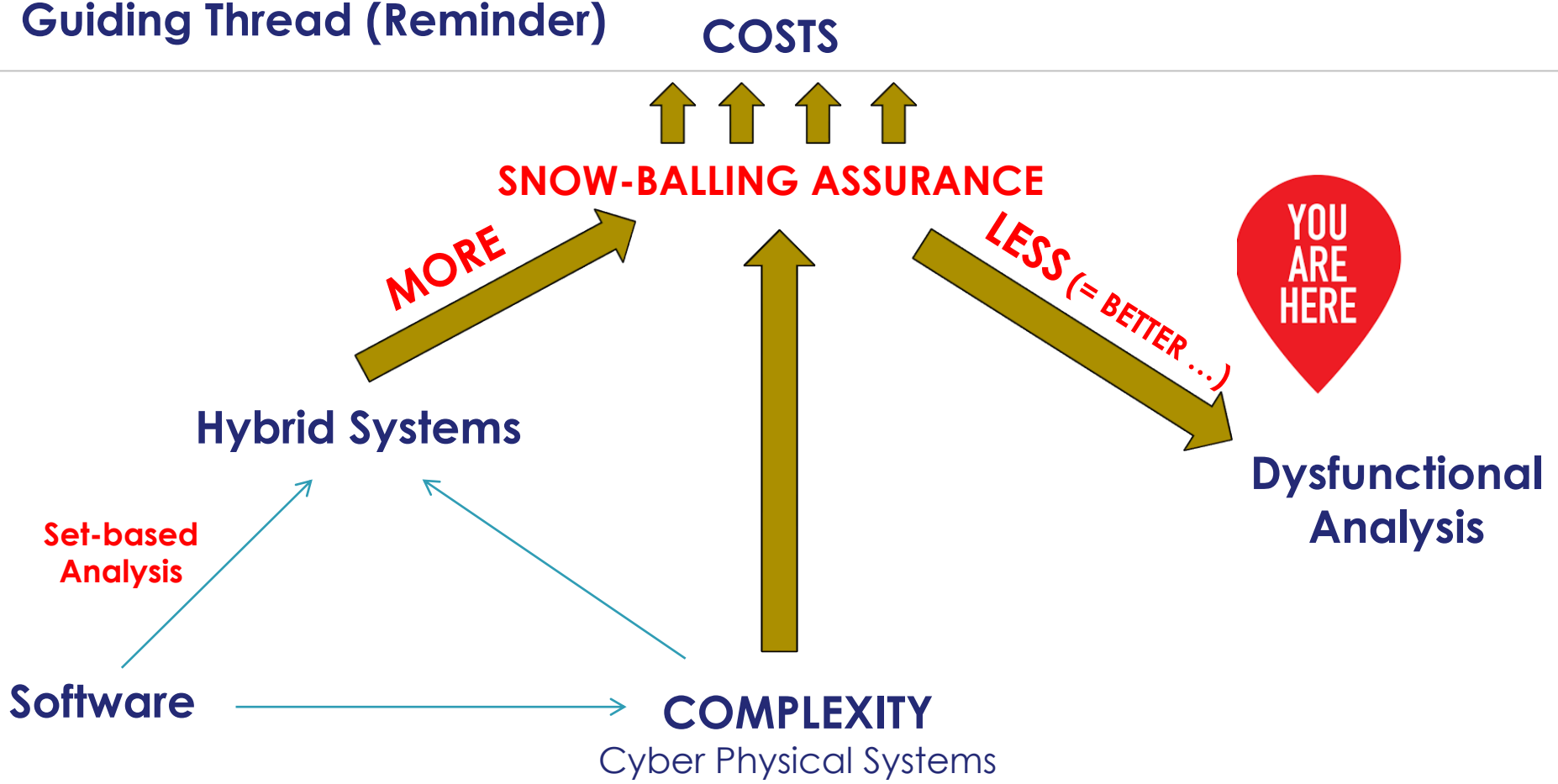
THALES

« Thinking The Unthinkable » (Bret Victor)



THALES

Guiding Thread (Reminder)



THALES

Inverse Dysfunctional Analysis

- From the Global to the Local
- From some Effects to *All* Possible Causes (Complete Inverse Causality)
- When some Faults lie in the System

- Claim: Too Complicated on Software-intensive Parts to be Trustworthy
- Applicability: FTA on Control-intensive of Physics-intensive Systems

THALES

Dysfunctional Analysis (Deterministic part) for Green Engineering

- Functional Safety Specification (e.g. STPA)
- Function & Resource Containment Regions
- Fault/Failure Detectors
- Recovery Control
- Testability
- Annunciation Logics
- Maintenance Design

FAULT TOLERANCE Implemented In The Product

Effort Saving Opportunity on Red Engineering

- "Exhaustive Inventories" of **Banned Behaviors** (FMEAs, FTAs)

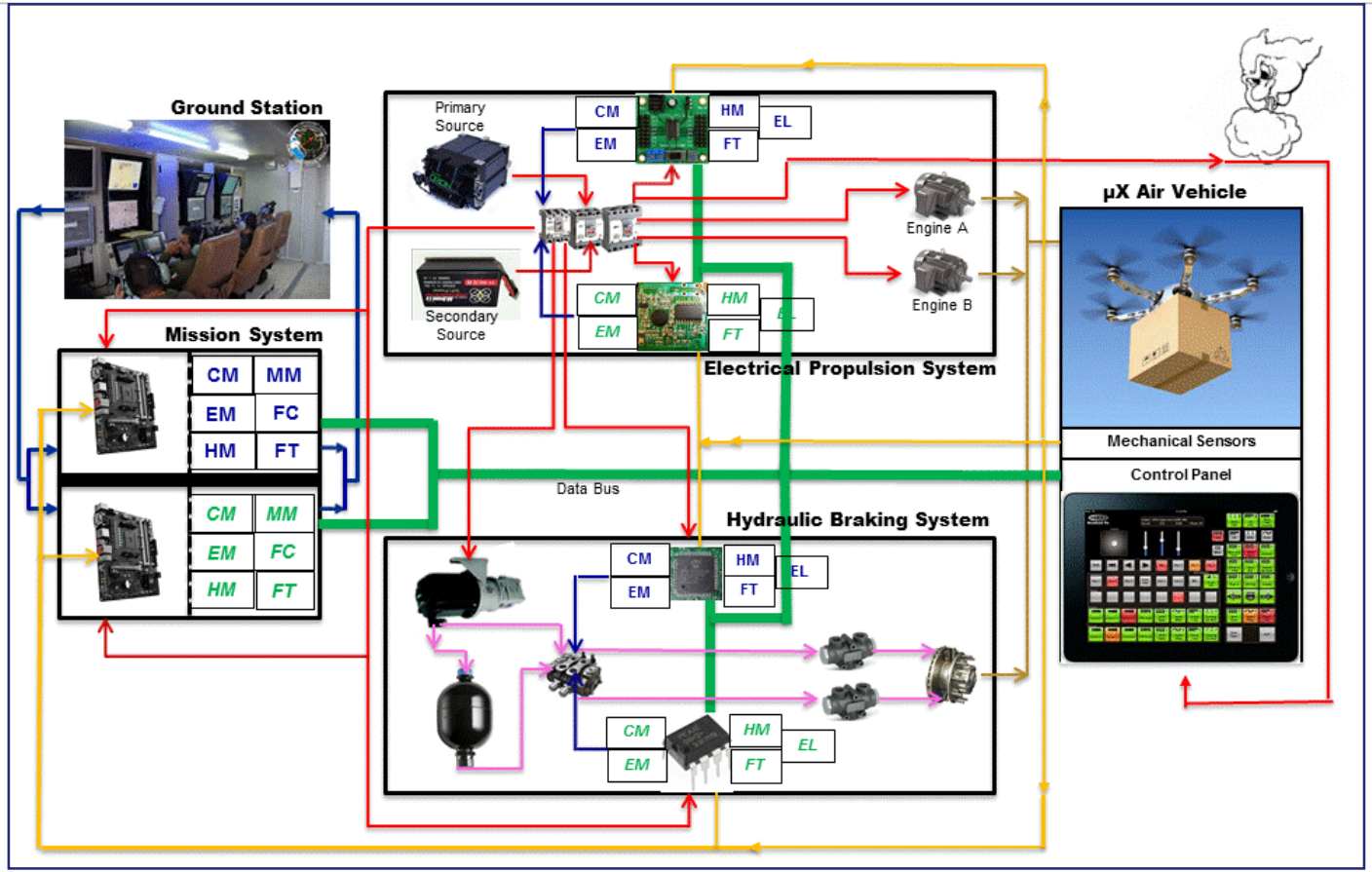
THALES

Mind-Map Proposal

	IMPOSSIBILITY Engineering		**RARITY** Engineering
	Structural	**Behavioral**	**Probabilistic**
Green Engineering **Controllability**	Influence Networks Containment Regions Replication Policies	**'Stay-in' Regions** Safety Controls Safety Monitors **STPA**	Estimation Failures Signal processing, **AI Machine Learning**.
Disturbance Analysis **Red Engineering**	**FMEA** **FTA** **Common Cause** Analysis	**STPA** **FMEA, MBSA** FTAs (***inverse mode***) **'Stay-out' Regions**	**Availability** **Reliability** Quantification of ***all*** the '**Controllability Escapes**'

THALES

Bridging the Gap Between Two SotAs : A Public Domain Use Case



RESSAC Project (2016-2018)
Follow-up

« Toy » CPS

- Multi-Physics,
- Multi-System
- Duplex & Simplex
- 12 Functions
- 36 Component Failures
- 6 Safety Properties
- Formal **System** Verification
- Assurance Processes

THALES

Objectives of The Use Case: Towards Stronger Assurance

- STPA-based Safety Specification
- Invariant-based Design
- Contract-based Refinement

- Structural Analysis for Independence
- Hybrid System Formal Verification
- Geometric Approach to Physical Dynamics

- Argument-based Assurance
- Probabilistic Calculation on High Fidelity Models

THALES

Conclusion (1/3)

Two Gaps are Widening Between the States of the Art of

- **Products** and **Engineering**
- **Engineering** and **Assurance**

THALES

Conclusion (2/3)

Rebalancing Assurance with More

- At *Constant* Overall Cost on **Control** and **Fault-Tolerance**
- "Green-oriented Red Engineering": Failure inventories **to design**
  - The "Stay-in" Regions,
  - The Detectors,
  - The Containment Regions,
  - The Replicates,
  - The Recovery Controls

THALES

Conclusion (3/3)

Rebalancing with **Less**

- **FM Inventories:** illusory complete identification of the initiators
- **Backward Dysfunctional** Analysis on Software-intensive parts
- **FTA:** limited to structural *structure functions*

THALES