Model Checking at Scale: Automated Air Traffic Control Design Space Exploration

M. Gario*, A. Cimatti*, C. Mattarei*, S. Tonetta*,
K. Y. Rozier†

gario@fbk.eu

Fondazione Bruno Kessler*
Iowa State University†

2016-07-22


Minneapolis
Milwaukee
Chicago
Toronto
Vermont
Massach
New York
Illinois
Indiana
West
District of
Columbia
Delaware
Mississippi

Increase the **capacity** of Air Traffic Control

NextGen Air Traffic Control

NASA needs to **evaluate multiple issues** and points of view: Realizability, **Safety**, Cost, Social and Political Impact ...

Our scope: Function Allocation for Separation Assurance

- **Separation Assurance**: "avoid aircraft getting too close to each other" (Loss of Separation)
- **Function Allocation**: Which functions should be on-board and which ones on-ground?

Problem

NASA had some initial ideas of **possible** designs:

- Some were **quite different** from each other
- Each had several **open choices**

$\Rightarrow$ **Large design space**: thousands of designs

Problem

NASA had some initial ideas of **possible** designs:

- Some were **quite different** from each other
- Each had several **open choices**

$\Rightarrow$ **Large design space**: thousands of designs

Compare different designs considering:

- How good they are, i.e., what do they **guarantee**;
- Resilience to **faults**.

$\Rightarrow$ Apply **formal methods** to exhaustively analyze **1620** designs.

Contributions

Automatically **generate**, **validate**, and **analyze** the **entire design space** of 1620 configurations

Contributions

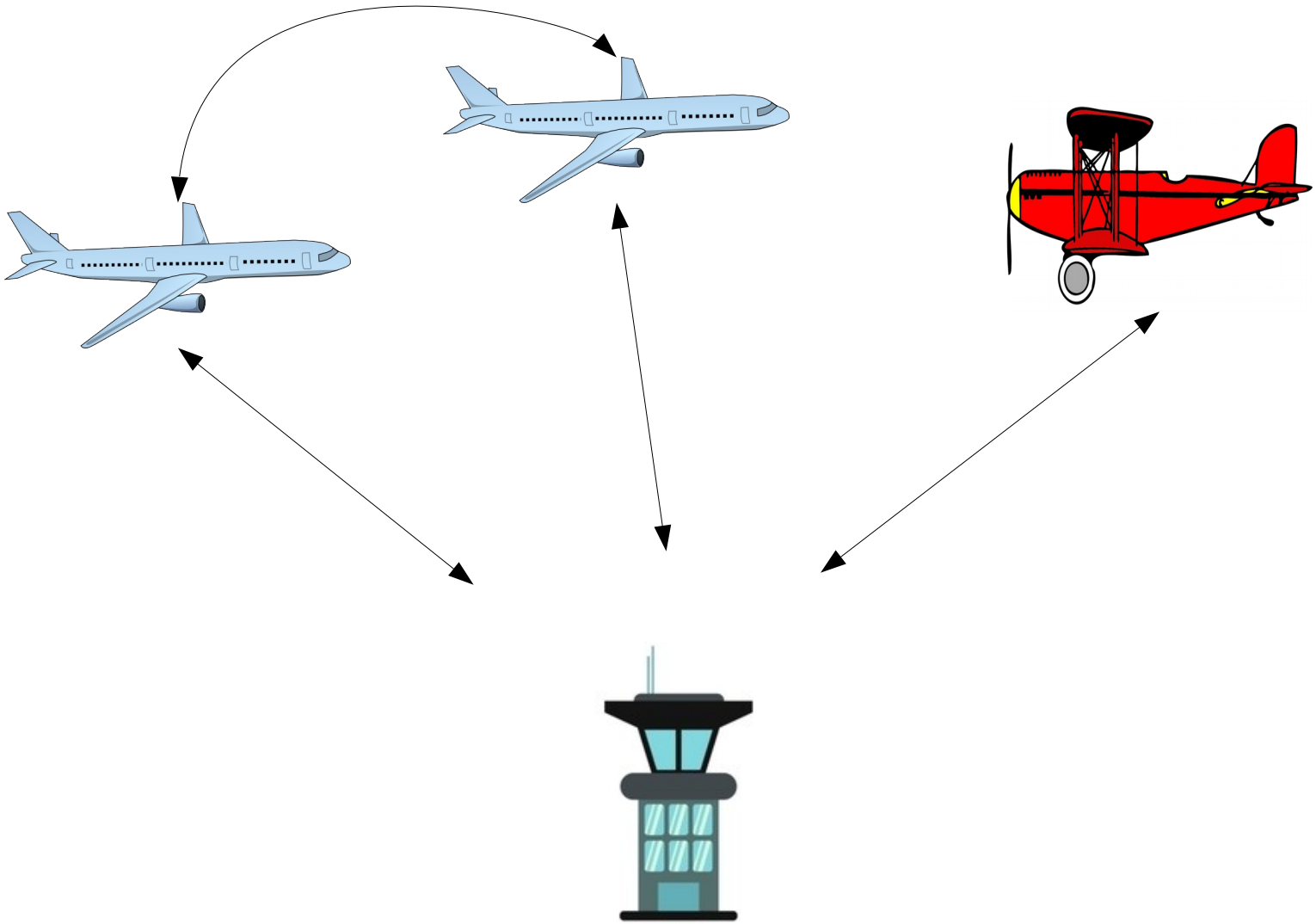
Automatically **generate**, **validate**, and **analyze** the **entire design space** of 1620 configurations

Industrial:

- **Rich dataset** of results that **characterize each configuration**
- Results were **validated by NASA** system designers:
  $\Rightarrow$ identify **novel and known** problems

Technical:

- Novel **process** combining existing technologies for **Compositional** + **contract** + **parameteric** design
- Publicly **release** a complex case-study of industrial interest (Artifact Eval)
- Proposals for analyzing the **big amount** of results



Related Work

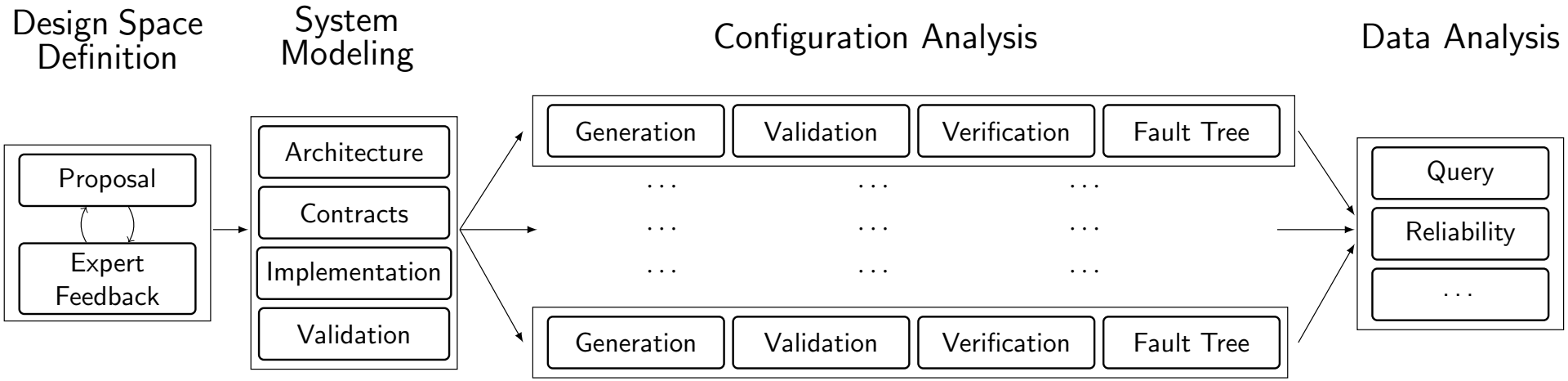
Air Traffic Control and Formal Methods:

- Many works focusing on the **implementation** of a component (e.g., ACAS-X)
- Previous works limited to a few designs (e.g., Zhao-Rozier'15, Mattarei et al.'15)

Design Space Exploration:

- Mostly **combinational**: no **memory**
- Driven by a clearly defined **cost function**
- Software Product Lines: **Not comparative** and **no faults**

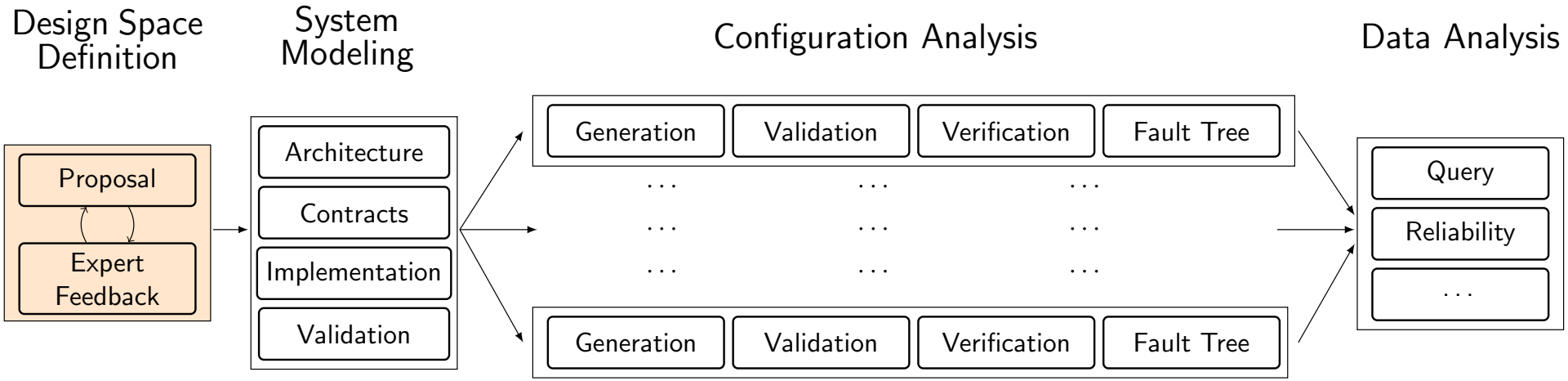
Process Overview



4 Phases:

1. Design Space Definition
2. System Modeling
3. Configuration Analysis
4. Data Analysis

Process Overview



4 Phases:

1. **Design Space Definition**
2. System Modeling
3. Configuration Analysis
4. Data Analysis

Design Space

Name	Possible Values	Size of Dimension
SSEP TS SA	ATC, SELF, SATC	3
SSEP SS SA	ATC, SELF, SATC	3
Aircraft Mix	$\langle 4,0\rangle$, $\langle 3,1\rangle$, $\langle 2,2\rangle$, $\langle 1,3\rangle$, $\langle 0,4\rangle$	5
Info Sharing (GSEP-to-SSEP)	None, Current, Near, Mid, Far	5
Info Sharing (SSEP-to-ATC)	None, Current, Near, Mid, Far	5
Burdening Rules	Undef, *GSEP*, *SSEP*	3
Com Steps	1, 2, ...	2
ACDR Implementations	Simple, Asymmetric, Non-Receptive	3
TOTAL	-	20250

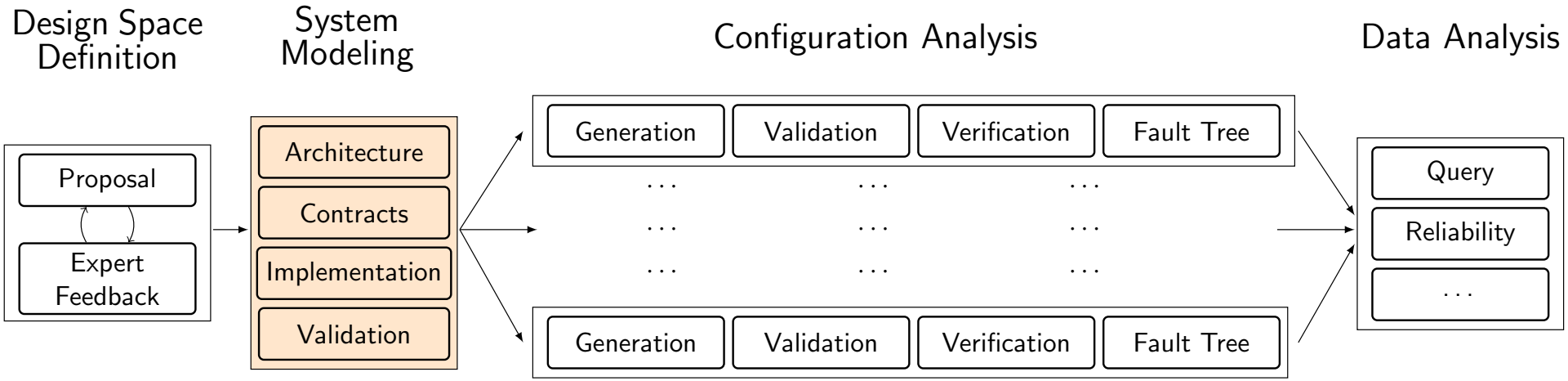
- **20250** Possible configurations
- NASA suggested to **focus on a subset**

Design Space

Name	Possible Values	Size of Dimension
SSEP TS SA	ATC, SELF, SATC	3
SSEP SS SA	ATC, SELF, SATC	3
Aircraft Mix	$\langle 4,0\rangle$, $\langle 3,1\rangle$, $\langle 2,2\rangle$, $\langle 1,3\rangle$, $\langle 0,4\rangle$	5
Info Sharing (GSEP-to-SSEP)	~~None~~, Current, ~~Near, Mid~~, Far	~~5~~ 2
Info Sharing (SSEP-to-ATC)	None, ~~Current, Near, Mid,~~ Far	~~5~~ 2
Burdening Rules	Undef, *GSEP*, *SSEP*	3
Com Steps	1, 2, ...	2
ACDR Implementations	Simple, Asymmetric, Non-Receptive	3
TOTAL	-	~~20250~~ **1620**

- **20250** Possible configurations
- NASA suggested to **focus on a subset**
- **1620** Configurations to analyze!

Process Overview



4 Phases:

1. Design Space Definition
2. **System Modeling**
3. Configuration Analysis
4. Data Analysis

Modeling

Impossible to **manually** model 1.6k configurations!

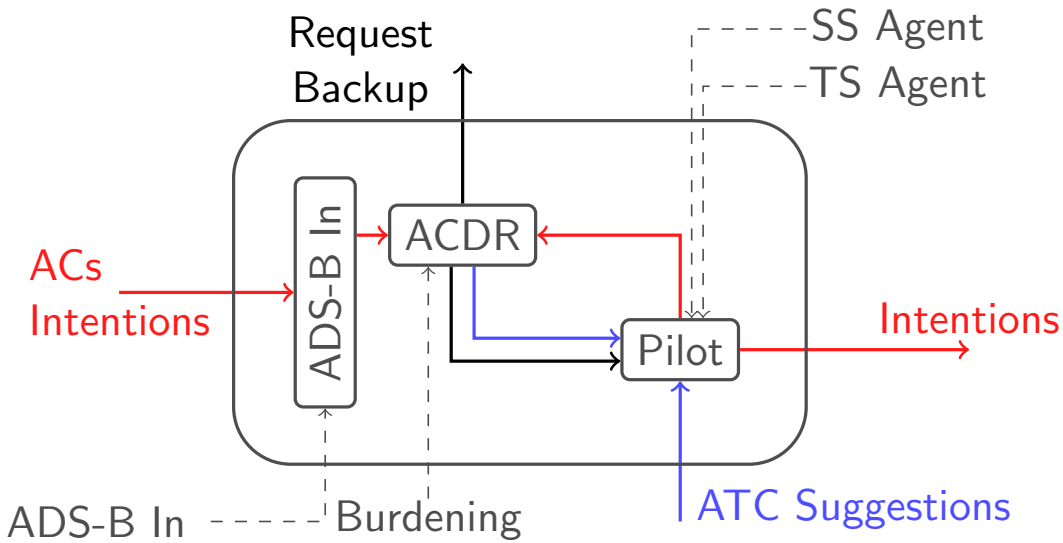
$$\Downarrow$$

Compositional + **Parametric** Model

Modeling: Components and Parameters

Use components to capture relevant aspects in isolation:

- **Different** implementations; or
- Tweak behavior with **parameters**



$\Rightarrow$ No need to modify the other components!

Validation

Increase **confidence in auto-generated** models

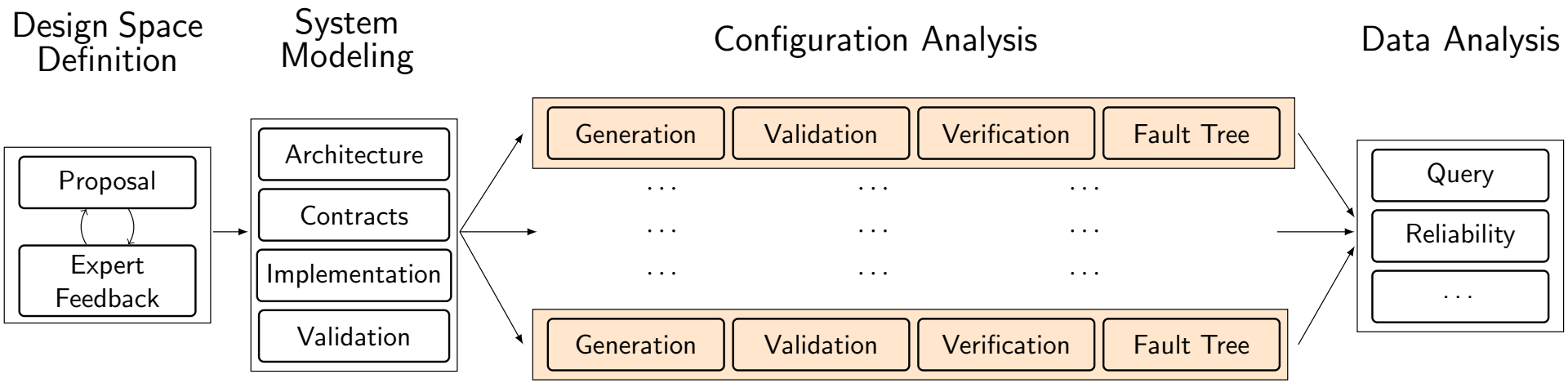
Validation of the components using **Contracts**:

- Contract of, e.g., Aircraft is **decomposed** into its components
- Focus on the implementation of the **component in isolation**

$\Rightarrow$ **Smaller** model to verify

$\Rightarrow$ **Speed-up** design loop

Process Overview



4 Phases:

1. Design Space Definition
2. System Modeling
3. **Configuration Analysis**
4. Data Analysis

Configuration Analysis

All steps of the **analysis** are performed
automatically

Scalable and **reproducible** process!

Tooling and Stats

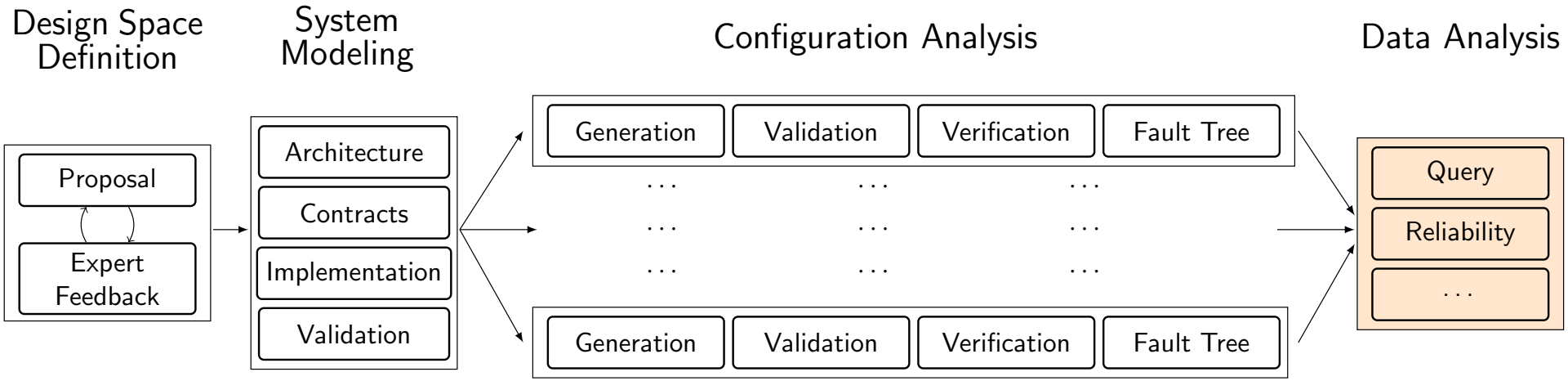
Tools:

- OCRA: **contract-based** reasoning; **mapping** of implementation to components; **instance generation**.
- nuXmv: **validation** and **verification** of instances.
- xSAP: **fault tree** and **reliability** computation.

Statistical Info:

- **1620 Models**
- **346 Properties** per model (LTL/CTL/INVAR)
- 10^{107} **State-Space** (Avg. per model)
- ≤ 5 **minutes** total verification time per model: efficient **SAT-based** algorithms
- $\geq 90\%$ of the models ≤ 1 **hour** for Validation (BDD-Based) and Fault Tree Computation.

Process Overview



4 Phases:

1. Design Space Definition
2. System Modeling
3. Configuration Analysis
4. **Data Analysis**

Data Analysis

Outcome of process:

- **Big table** linking each configuration to satisfied properties
- Set of **fault trees** for each configuration

	A	B	C	D	E	F	G	H	I	J
1	ID	AC_MIX	SSEP_SA	GSEP_SSE	SSEP_AT	BURD	COM_	MAP	NO-LOS	NO-LOS-Near
2	1	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	2	nominal_simple_cdr	True	True
3	2	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	2	nominal	True	True
4	3	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	2	nominal_nr_cdr	True	True
5	4	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	1	nominal_simple_cdr	True	True
6	5	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	1	nominal	True	True
7	6	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	UNDEF	1	nominal_nr_cdr	True	True
8	7	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	SSEP	2	nominal_simple_cdr	True	True
9	8	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	SSEP	2	nominal	True	True
10	9	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	SSEP	2	nominal_nr_cdr	True	True
11	10	4_GSEP_0_SSEP	ATC_ATC	CURRENT	FAR	SSEP	1	nominal_simple_cdr	True	True

How to get **insights** from this data?

Data Analysis: Summarizing results

- **How many** configurations satisfy the given property?

  E.g., 1251 out of 1620 satisfy the **No Loss of Separation** (NO-LOS) property

Data Analysis: Summarizing results

- **How many** configurations satisfy the given property?

  E.g., 1251 out of 1620 satisfy the **No Loss of Separation** (NO-LOS) property

- How **common** are the X most common **Single Point of Failure**?

  The **5 most common** single point of failure are shared by **more than 1000** configurations!

Data Analysis: Summarizing results

- **How many** configurations satisfy the given property?

  E.g., 1251 out of 1620 satisfy the **No Loss of Separation** (NO-LOS) property

- How **common** are the X most common **Single Point of Failure**?

  The **5 most common** single point of failure are shared by **more than 1000** configurations!

- Synthesize **region of parameters** that satisfy a given property:

  E.g., For cardinality 1, NO-LOS:

$$(MIX = (4, 0)) \vee (SSEP\_TS\_SA = ATC) \vee (SSEP\_SS\_SA = ATC)$$

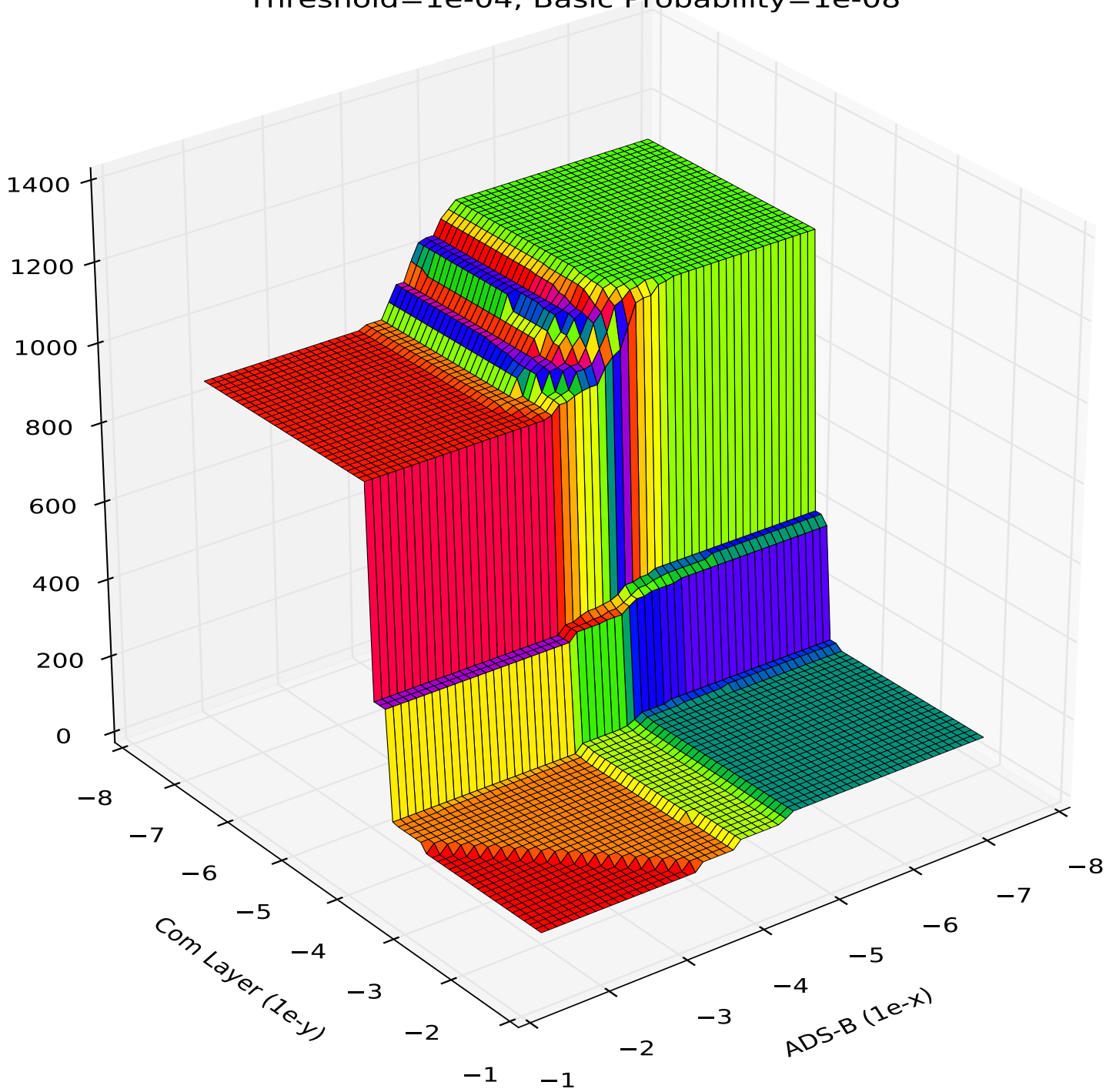
Data Analysis: Reliability + Sensitivity

Divide faults in **3 groups**:

- x (e.g., ADS-B Network – all components)
- y (e.g., Communication Layer)
- θ (e.g., all other faults)

Fix a failure probability for θ and a threshold τ,
how many configurations have a reliability above τ
for a given probability of x and y?

What happens when we **change** the probability of x and y?


Threshold=1e-04, Basic Probability=1e-08
1400
1200
1000
800
600
400
200
0
−8
−7
−6
−5
−4
−3
−2
−1
Com Layer (1e-y)
−1
−2
−3
−4
−5
−6
−7
−8
ADS-B (1e-x)

Results Validation

- Selection of configuration **validated by NASA** experts
- Independently **reproduced two known issues**: side-walk and coincidental conflicts
- Discovered a problematic configuration, due to **missing assumptions**, when dealing with **backup from ground**

Conclusions

Automatically **generate**, **validate**, and **analyze** the **entire design space** of 1620 configurations

- Novel **process** combining existing technologies for **Compositional** + **contract** + **parameteric** design
- Publicly **release** a complex case-study of industrial interest
- **Rich dataset** of results that **characterize each configuration** + Techniques to **analyze it**
- Results were **validated by NASA** system designers:
  $\Rightarrow$ identify **novel and known** problems

Thank You! Questions?

- Models, tools and detailed results are available online:
  `https://es-static.fbk.eu/projects/nasa-aac/`

M. Gario, A. Cimatti, C. Mattarei, S. Tonetta, K. Y. Rozier - gario@fbk.eu

Model Checking at Scale:
Automated Air Traffic Control
Design Space Exploration