Fraunhofer IKS

SAFE INTELLIGENCE

COGNITIVE SYSTEMS | ARTIFICIAL INTELLIGENCE & MACHINE LEARNING | AUTONOMOUS SYSTEMS | AUTONOMOUS DRIVING | INDUSTRY 4.0 | IOT

TOWARDS COMPREHENSIVE SAFETY ASSURANCE IN CLOUD-BASED SYSTEMS

VISION PAPER

OLEG OLEINICHENKO, CHRISTIAN DRABEK, ANNA KOSMALSKA

PRESENTER: OLEG OLEINICHENKO

AFFILIATION: FRAUNHOFER INSTITUTE FOR COGNITIVE SYSTEMS IKS

EMAIL: OLEG.OLEINICHENKO@IKS.FRAUNHOFER.DE

BRIEF RESUME

Oleg Oleinichenko

Position: Research engineer at Fraunhofer IKS
Department: Safety, Reliability, Availability (since 2019)
Education: RWTH Aachen University (MSc ’16, Communications engineering)

Current research area:

Development and verification of new processes and algorithms for the safety analysis of flexible cloud-based E2E architectures.

AGENDA

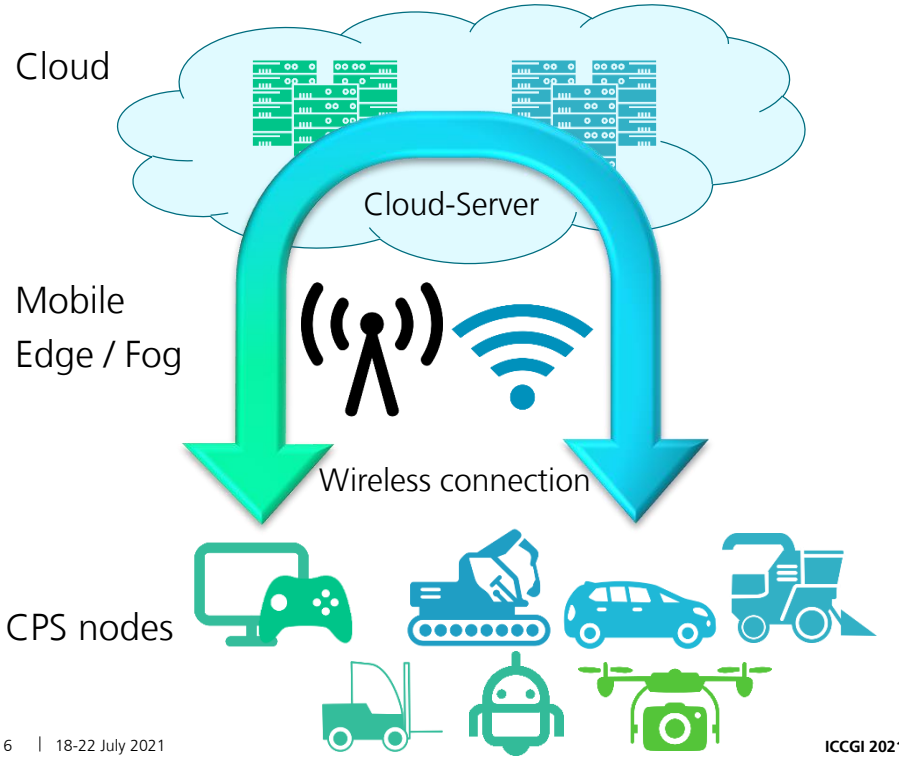
I. Motivation and goals

II. Considered approach

III. Conclusions and future outlook

MOTIVATION AND GOALS

CLOUD-BASED CYBER-PHYSICAL SYSTEMS



In the current digital transformation CPS are becoming increasingly pervasive

Many CPS rely on cloud-based services (functional offloading), e.g. in: smart cities, agricultural domains, vehicular systems, industrial automation, health-care, robotics, etc.

Cloud-offloaded functions exhibit dynamic and composite context of operation (highly virtualized, shared and often constrained resources within unrestricted evolving environment (fog), intermittent connectivity in RTS-environment, dynamic end nodes etc.)

PROBLEM DEFINITION

Cloud-based CPS system, to satisfy design goals and timeliness of operation, must be dependable and able to avoid service failures that are more frequent and more severe than is acceptable.

For off-loading of services / functions into cloud / fog / edge within fluent system borders, provisioning of safety guarantees is utmost important task.

Many standards dictate safety assurance in different domains:

- ISO 26262
- ISO 21448
- IEC 61508
- ARP 4761
- …

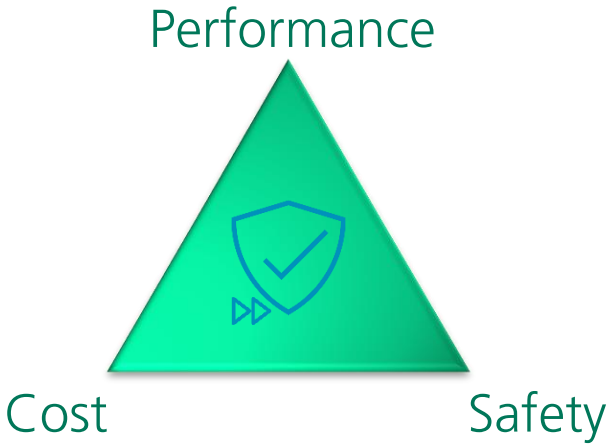
PROBLEM DEFINITION

In a dynamic cloud-based environment application of one of the existing standard might be highly inefficient:

- Insufficient safety coverage for a flexible architecture (complex forecasting - transient or unforeseen failures)
- Unstudied/Unknown effects of complex failure modes
- Implementation excessive (conflicting) redundancy solutions
- System instability due to poor handling of error propagation (complex dynamic error containment)
- Scalability problem (complex coordination in presence of faults)

PROBLEM DEFINITION

- Lack of effective mechanisms to foresee or handle / contain errors resulting from complex interactions –> insufficient safety coverage
- Excessive and burdening redundancy solutions within resource-constrained nodes with restrained scalability –> suboptimal performance
- Applying safety analysis posteriorly and in insufficient way –> increased costs / downtime during operation



Redundancy is neither cheap nor always realizable. In the end, the system must be performant, whilst providing sufficient level of safety. Satisfying these requirements in a dependable manner remains largely underexplored.

MAIN GOALS

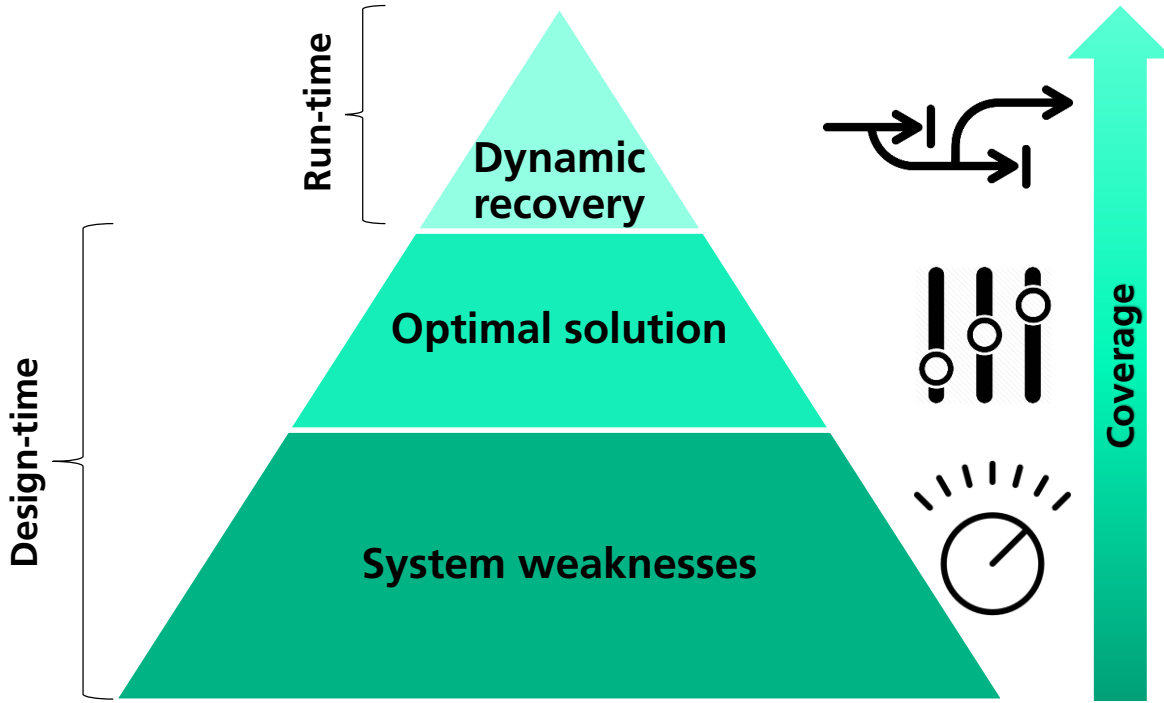
- Find applicability and the right composition of methods that will be best suited for cloud context
- Find expected yield of each applied method within the process
- Identify preferable countermeasures types for a cloud use-case of interest

CONSIDERED APPROACH

DEPENDABLE CLOUD SYSTEM ARCHITECTURE DEVELOPMENT

Targeting different scale of the dependability problems starting from the most fundamental at the bottom and ending with more sophisticated and research intense at the top.

The lower two levels are proactive and confined within design-time domain methods, whereas the third is reactive and consists of run-time domain methods.

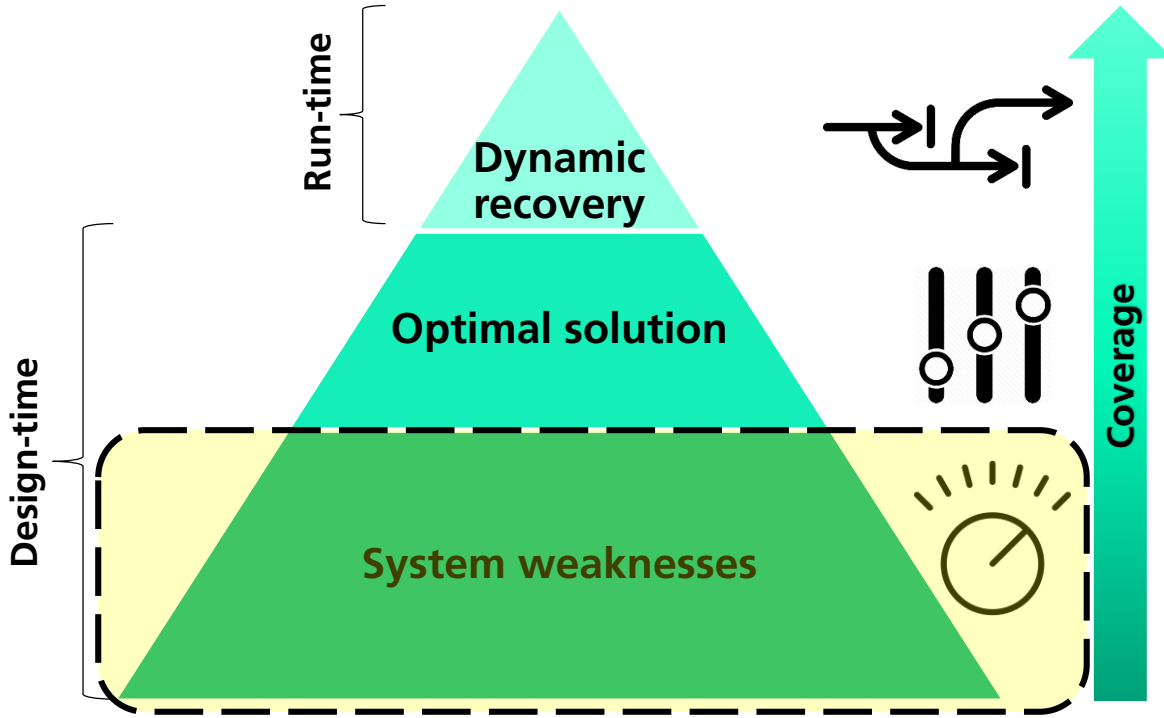


LEVEL 1 - SYSTEM WEAKNESSES

- Assuring safety process first steps
- Covering up top weaknesses
- Provision of a basic level of safety
- Elaboration of the set of a coarse and fundamental countermeasures (backbone of the system)

Methods:

- Guide-phrases
- HAZOP
- STAMP/STPA
- FMEA
- …

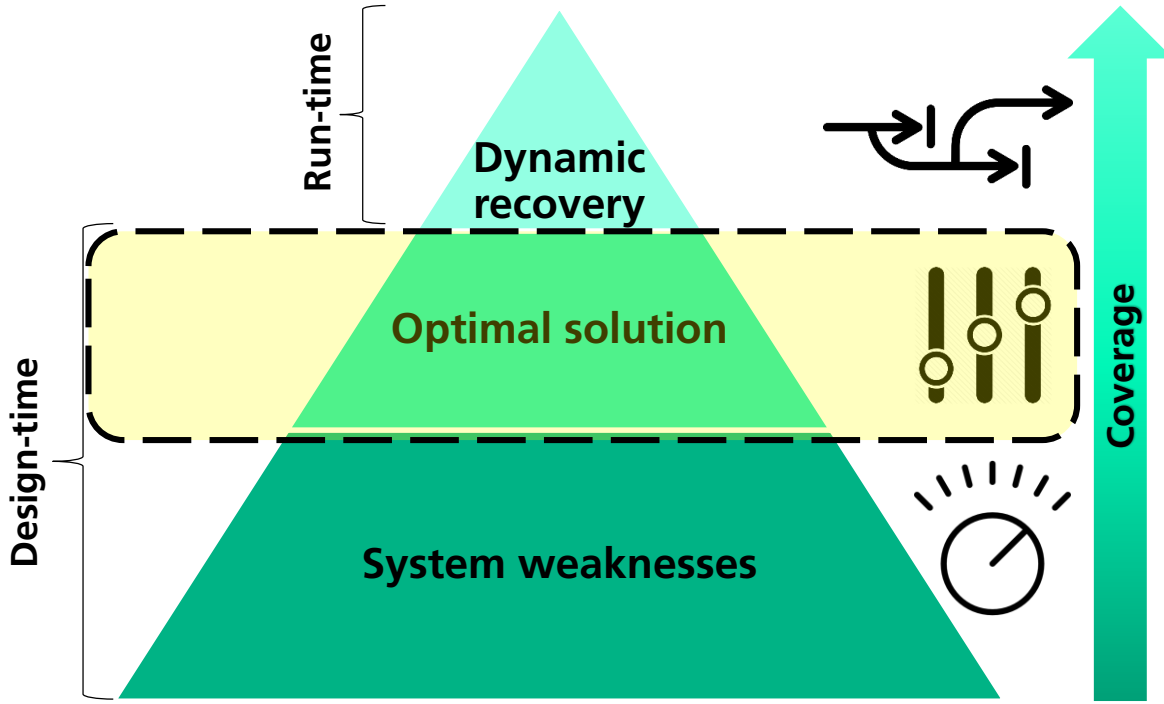


LEVEL 2 – OPTIMAL SOLUTION

- Assuring optimization of system operation
- Finding the most optimal utilization pattern using various physical and virtual realizations
- Provision of an extended level of safety
- Adjusting system configuration and selecting most suitable countermeasures (functional allocations, resource utilization and connectivity scenarios)

Methods:

- MBDA
- Simulation tooling
- …

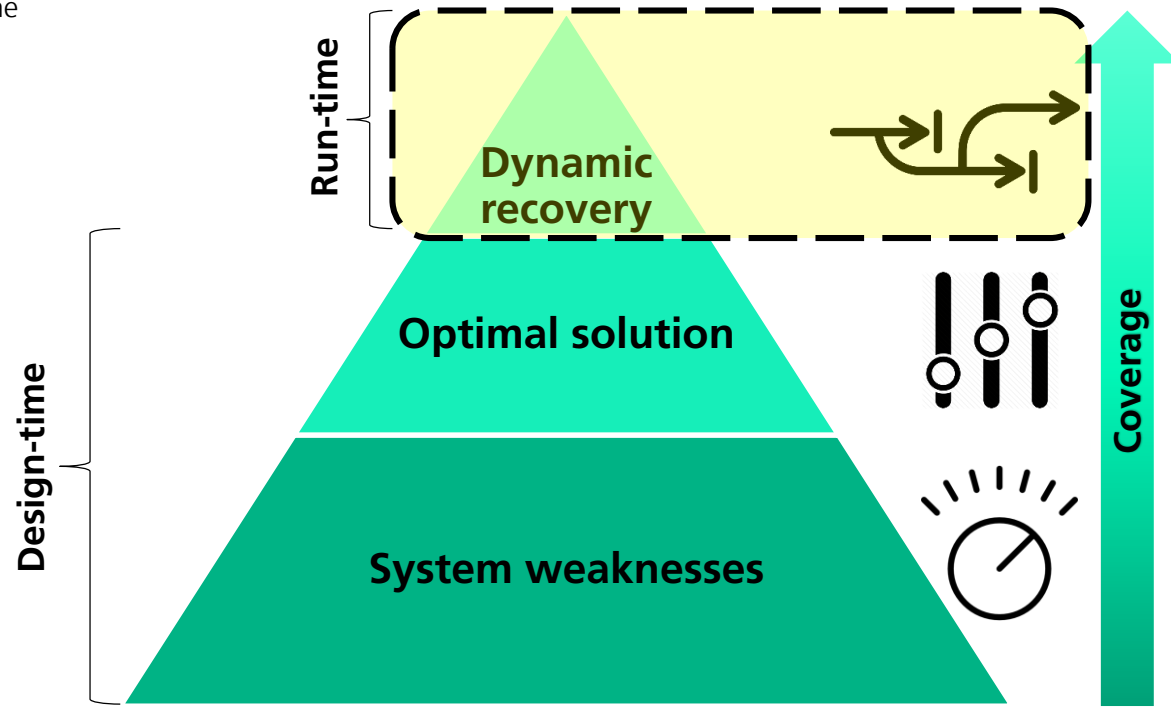


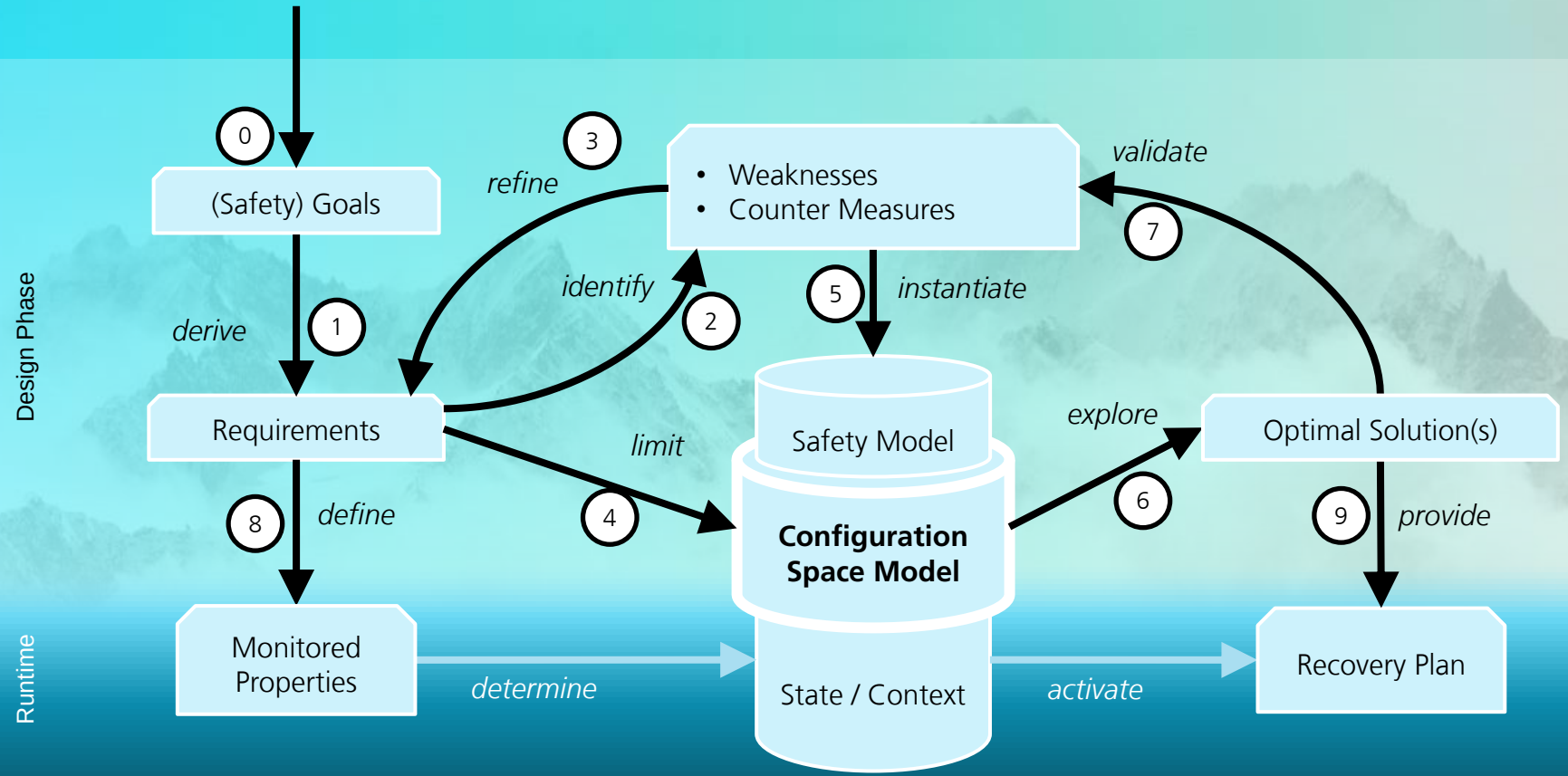
LEVEL 3 – DYNAMIC RECOVERY

- Assuring system resilience and adaptation in run-time
- Thorough investigation of system operation environment for its attribution and monitoring
- Provision of an advanced level of safety
- Developing an adaptive detection and recovery counter-reaction against foreseeable and unforeseeable events (monitoring attributes across the system)

Methods:

- Simulation tooling
- Cloud-system testbeds
- …




Design Phase
Runtime
0
(Safety) Goals
1
derive
Requirements
2
identify
3
refine
• Weaknesses
• Counter Measures
4
limit
5
instantiate
6
explore
7
validate
8
define
Monitored Properties
determine
Safety Model
Configuration Space Model
State / Context
Optimal Solution(s)
9
provide
activate
Recovery Plan

DESIGN OF SAFE AND EFFICIENT CPS CLOUD-BASED SYSTEM

Safe System

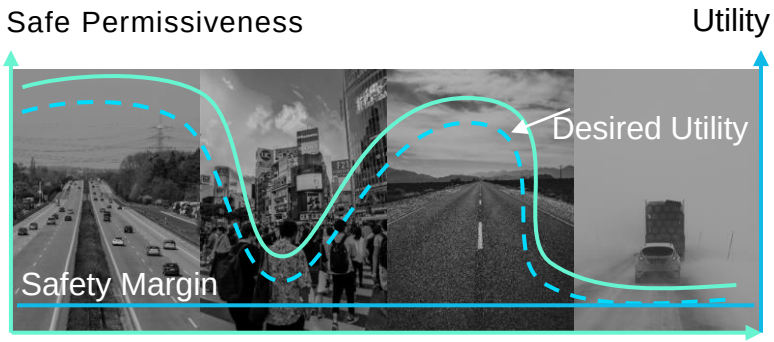
- Requires holistic approach to ensure no safety requirements are missed
- Might neglect performance
- Results in simple safety mechanisms (e.g., stop or worst case)

Efficient System

- Adapts to the current situation
- Avoids conditions that trigger safety stops
- Operates close to the edge of the safety-to-performance envelope

Validation

- Definition of safety-to-performance ratios for variety relevant KPIs pairs
- Strike the desired magnitude in the operation envelope –> right balance between design-time and run-time methods
- Explore significance and applicability of selected safety methods for a given use-case -> track the progress gain of each safety level successively



CONCLUSIONS AND FUTURE OUTLOOK

CONCLUSIONS AND FUTURE OUTLOOK

- Architecture design process must be accompanied by appropriate safety activities aforehand -> built-in resilience
- The ultimate system to be safe must incorporate measures covering foreseeable events and unforeseeable events (performance and safety ones)
- Leveraging traditional methods with sophisticated simulation practices within one process in a right proportion and selection
- Tack a safety-to-performance ratios for optimal decision making when choosing the alternative countermeasures compositions balancing design and run-time mechanisms
- Adapt the process to particular use-case by exploring applicability and gain of each of its levels' methods
- Future work will encompass discussions on the application of the proposed process and suitability of diverse countermeasures in cloud context

Image retrieved from https://humanecontrol.com/rats-mice-and-squirrels , Accessed 15 Jul. 2021.

THANK YOU

I WILL BE GLAD TO ANSWER YOUR QUESTIONS