

SAFE INTELLIGENCE

WHY MODELS REALLY MATTER FOR SAFETY ASSURANCE

Mario Trapp
mario.trapp@iks.fraunhofer.de

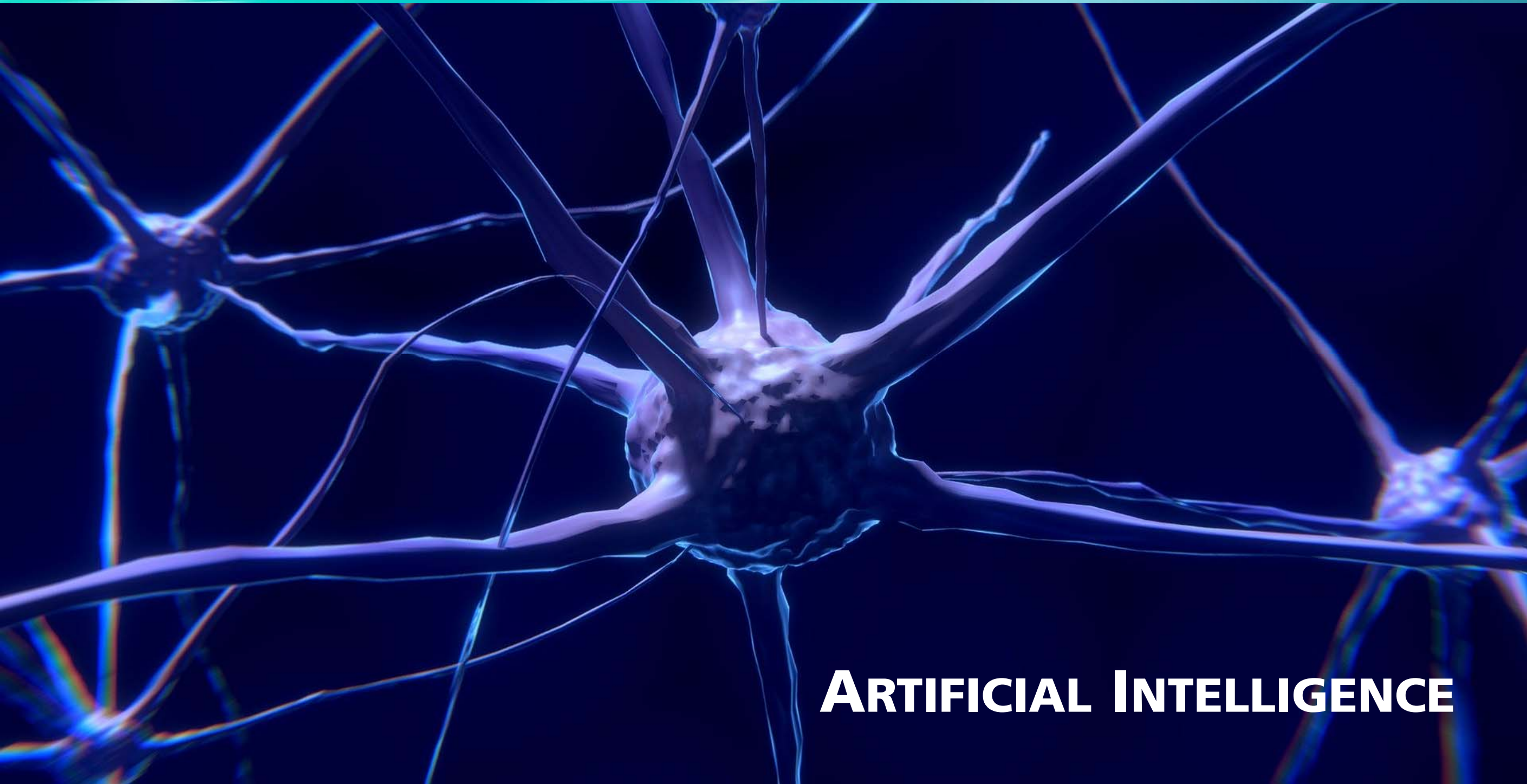


THE FUTURE



AUTONOMY

THE FUTURE



ARTIFICIAL INTELLIGENCE

THE FUTURE

SAFETY-CRITICAL APPS & SERVICES



THE FUTURE

CONNECTIVITY



THE FUTURE

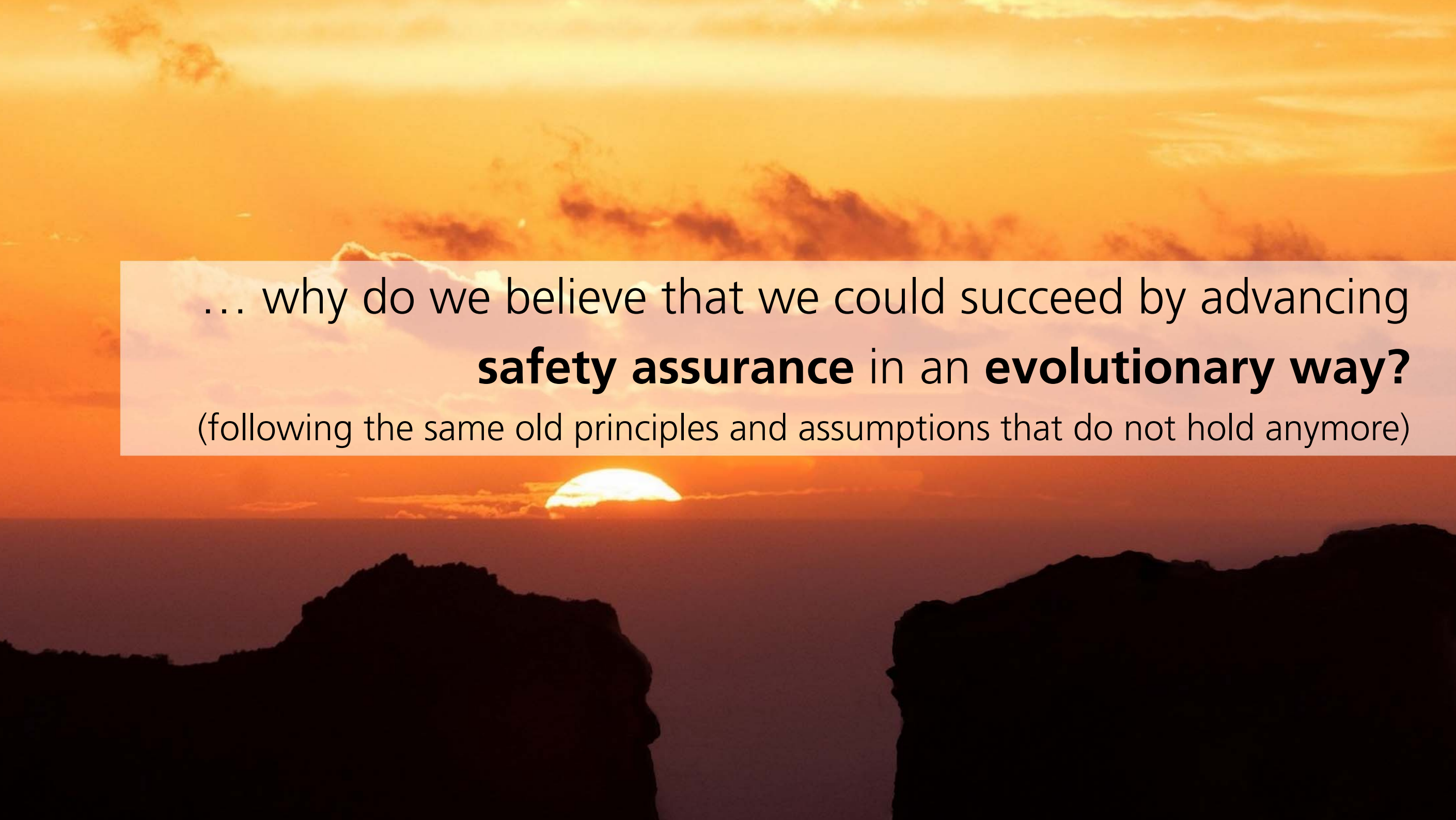
SYSTEM COLLABORATION





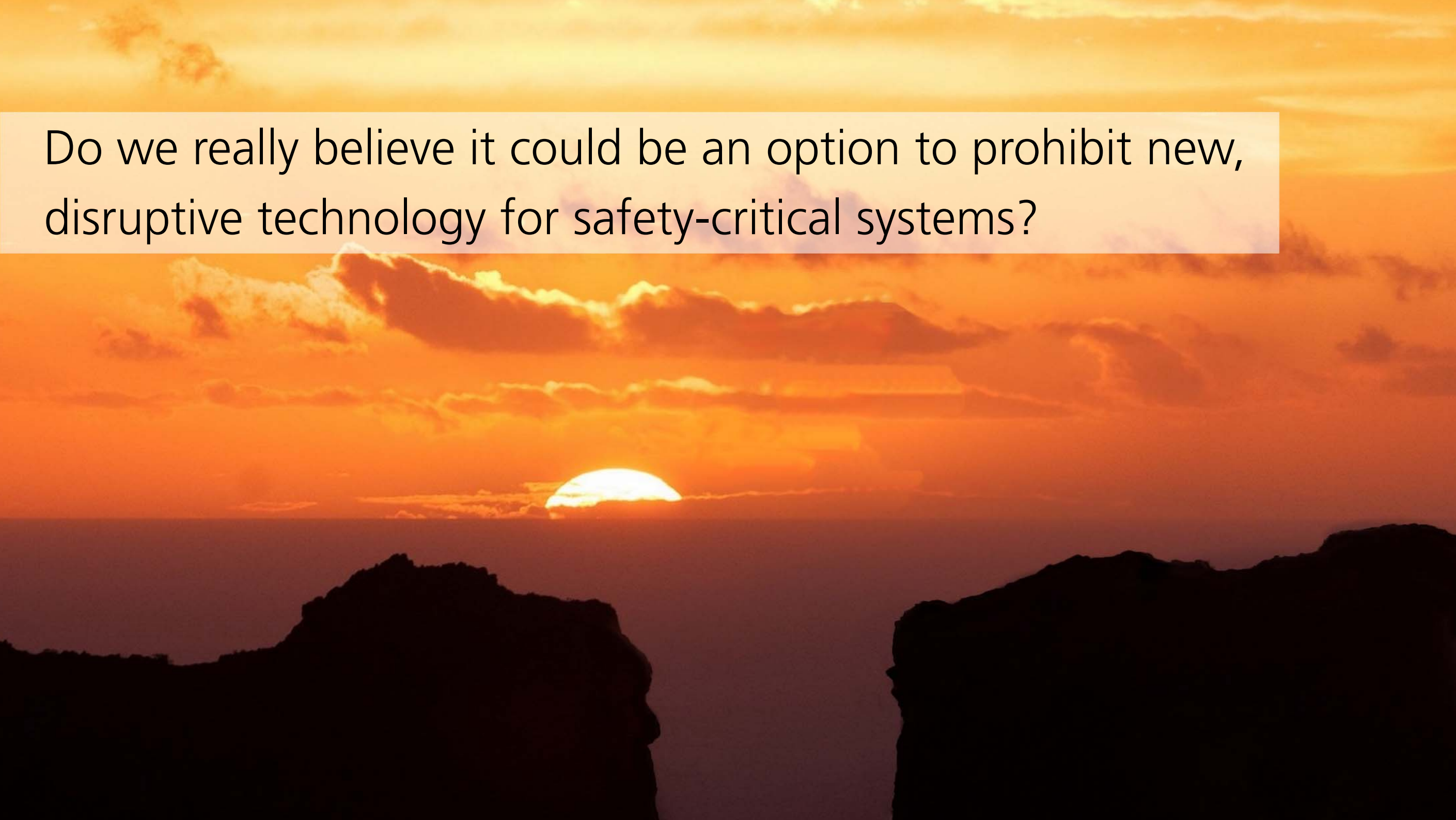
If products, business models, and the underlying software **technology change in a disruptive way, ...**




A sunset scene with a semi-transparent white text box. The sun is a bright yellow semi-circle on the horizon, partially obscured by a thin layer of clouds. The sky is a gradient of orange and yellow. In the foreground, the dark silhouettes of mountain peaks are visible against the sunset.

... why do we believe that we could succeed by advancing
safety assurance in an **evolutionary way?**
(following the same old principles and assumptions that do not hold anymore)

Do we really believe it could be an option to prohibit new, disruptive technology for safety-critical systems?



A sunset scene with a semi-transparent white text box. The sun is a bright yellow semi-circle on the horizon, partially obscured by a thin layer of clouds. The sky is a gradient of orange and yellow, with some wispy clouds. In the foreground, the dark silhouettes of mountain peaks are visible against the lower part of the sky.

Or should we be courageous enough for
new, innovative, disruptive ways of safety assurance?
(finding new, sound principles and assumptions for next generation technology)



SAFETY NOW

Assumptions

static systems & context
technology-driven failure models
determinism & predictability

Methodology & Technology

(monolithic) a-priori assurance
conservative worst case assumptions
inflexible, “stupid” mechanisms



SAFETY NEXT

Presumption

open systems & context
behavior-driven failure models
uncertainties

Methodology & Technology

modular and **dynamic** assurance
dynamic **actual case** assumptions
intelligent, adaptive resilience



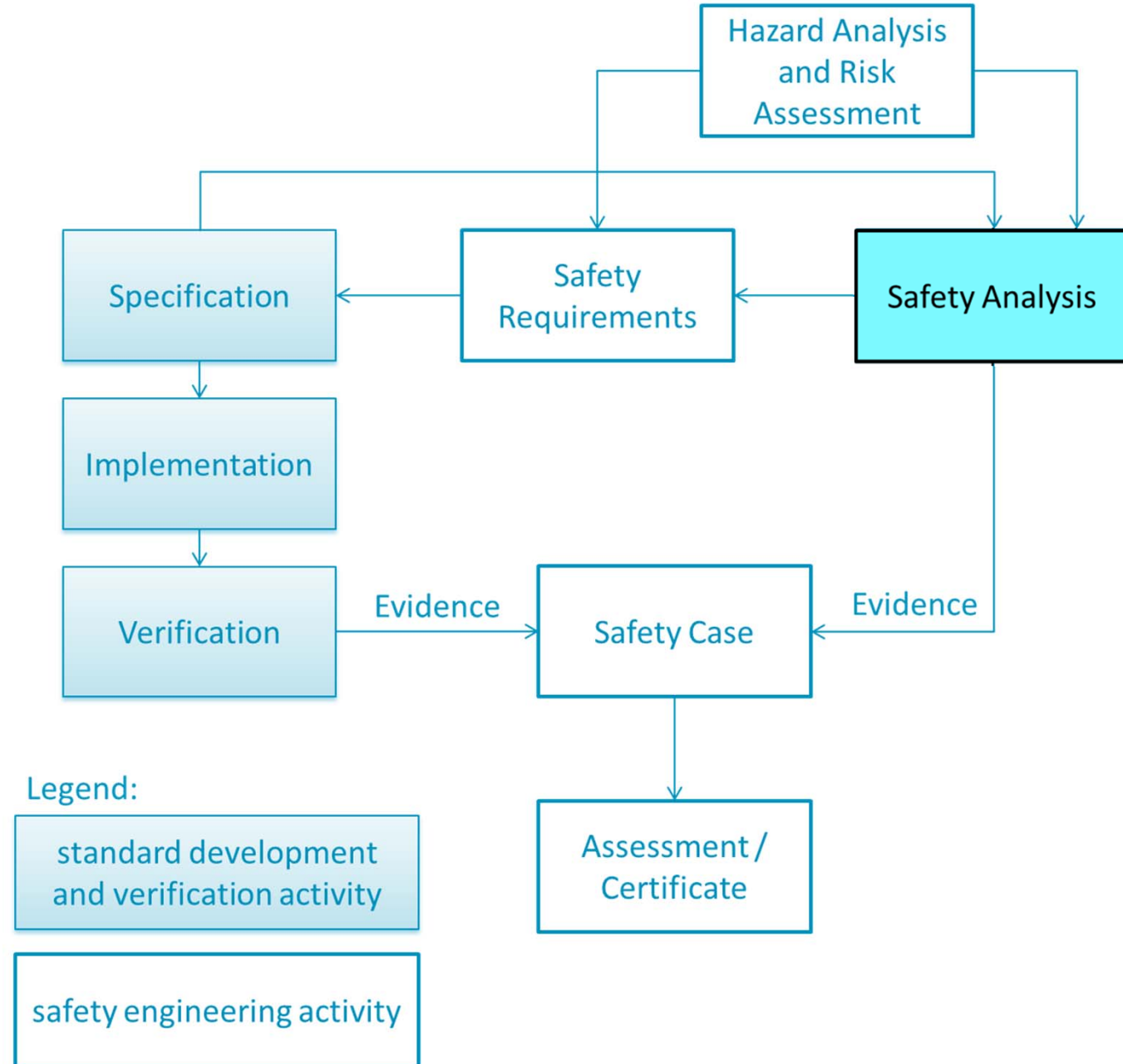
THE KEY: MODEL-BASED SAFETY ASSURANCE



MODEL-BASED SAFETY MANAGEMENT



MODEL-BASED SAFETY ENGINEERING



IDEAL CASE

One integrated model with different diagrams and viewpoints

A LONG-LASTING PRINCIPLE NEEDS TO BE CHANGED



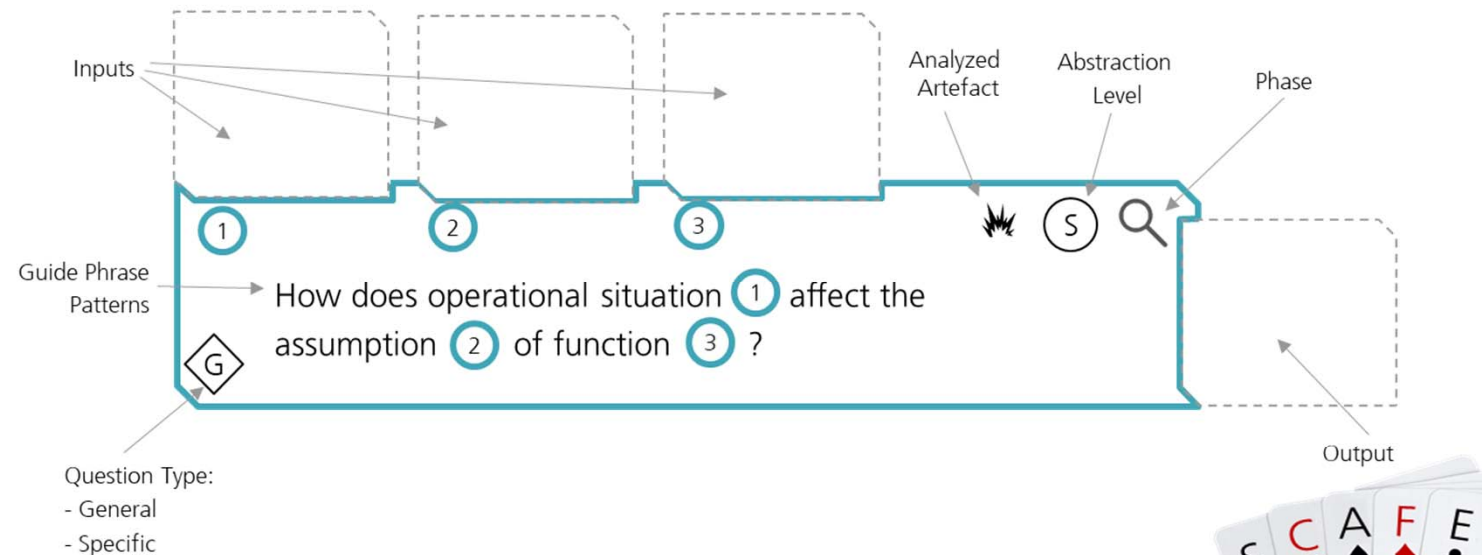
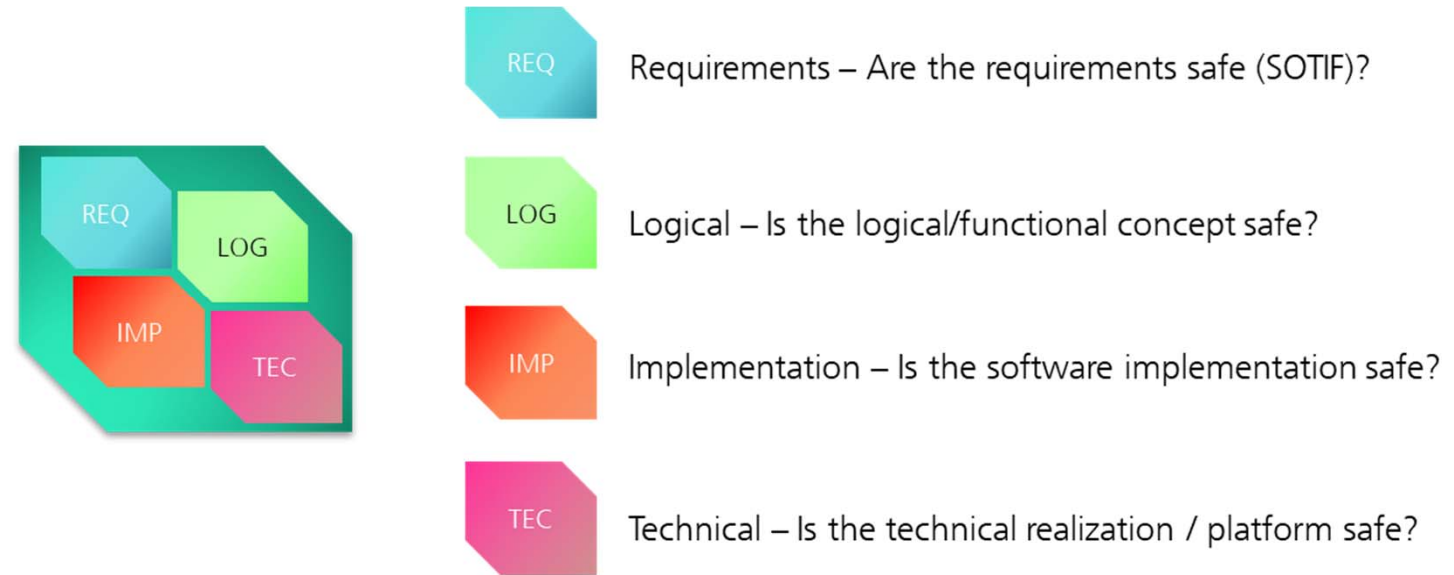
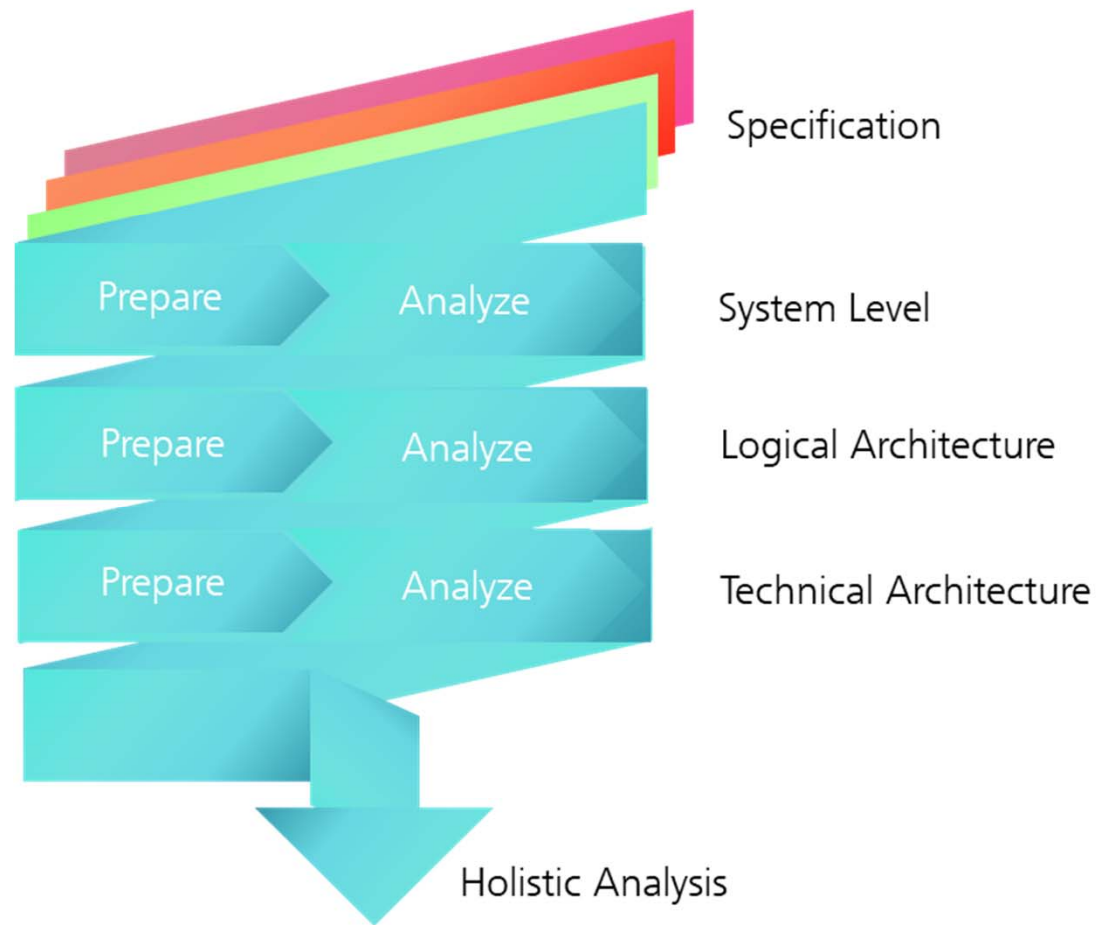
Broad-spectrum counter-measures



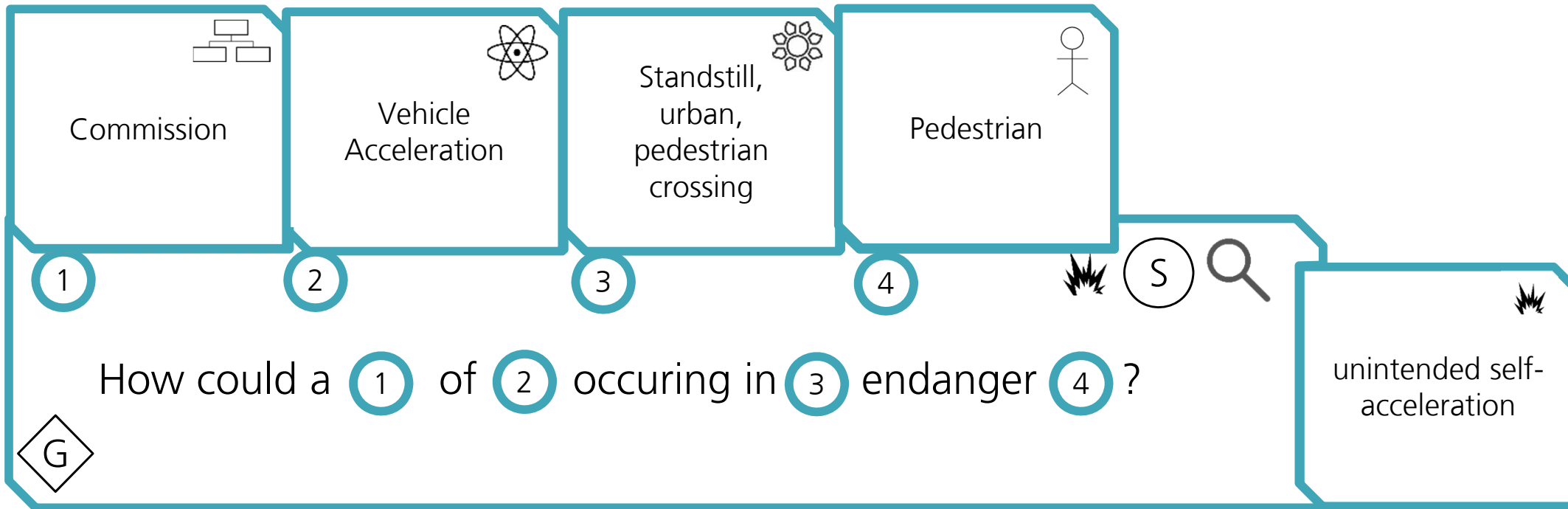
Specific counter-measures



EXAMPLE: SERIOUS CARD PLAY FOR SAFETY ANALYSIS - SSAFE



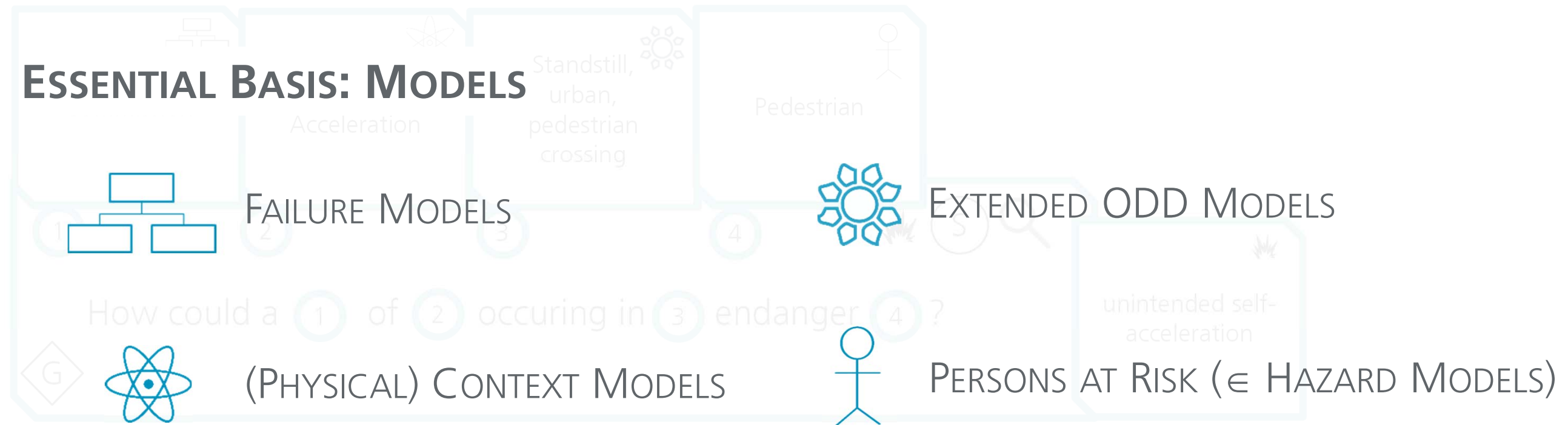
GUIDE PHRASES - EXAMPLE



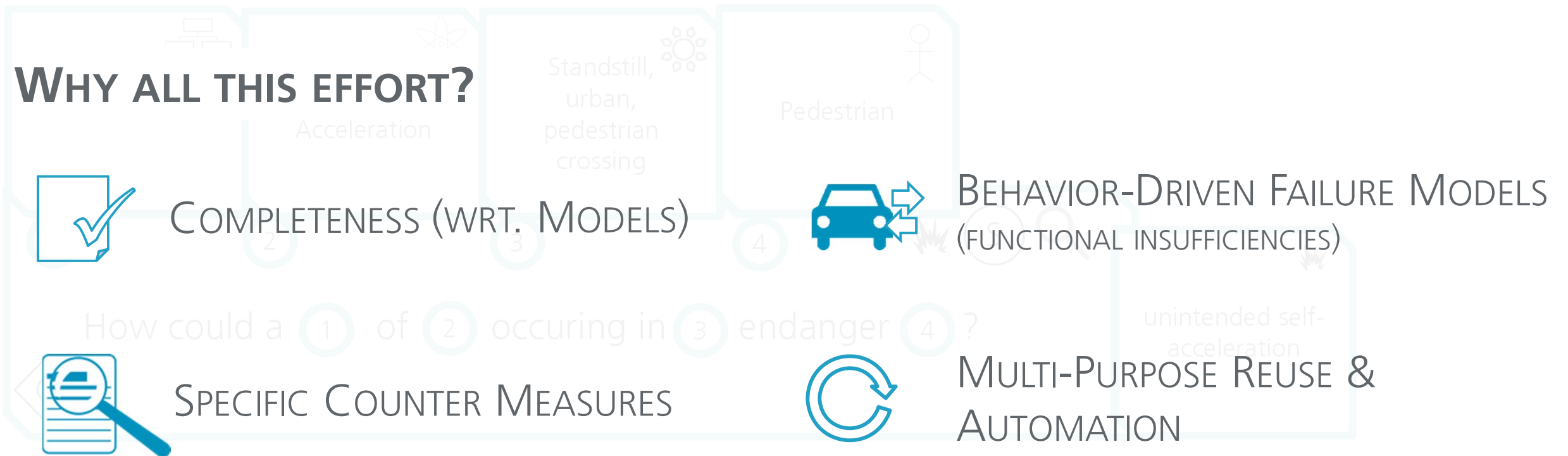
Read as: How could an unintended vehicle acceleration during a standstill in front of a pedestrian crossing in an urban traffic situation endanger pedestrians?

4

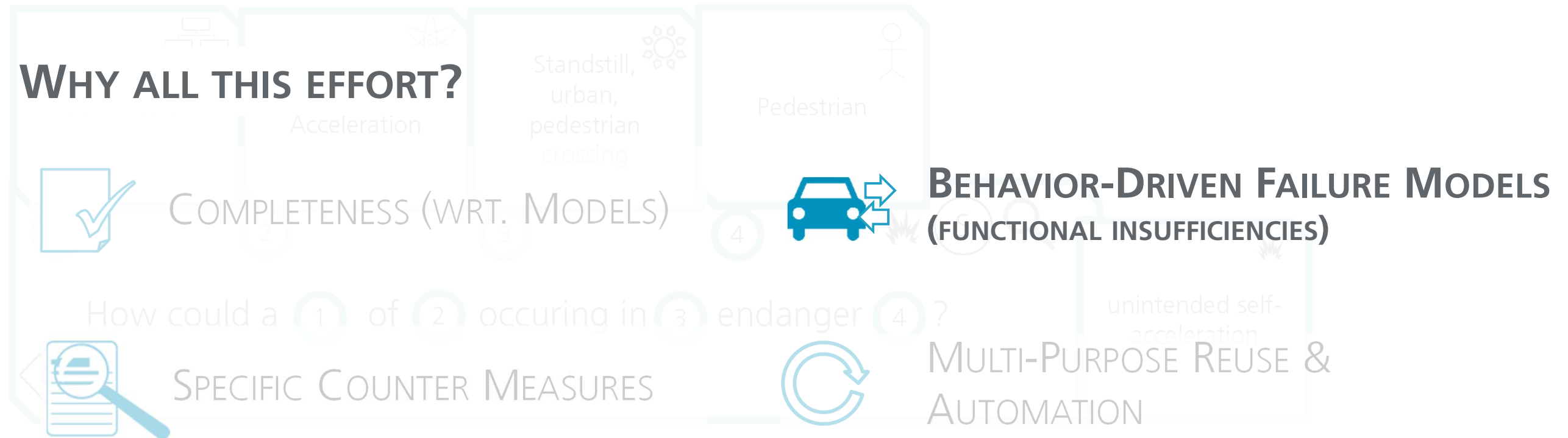
GUIDE PHRASES - EXAMPLE



GUIDE PHRASES - EXAMPLE

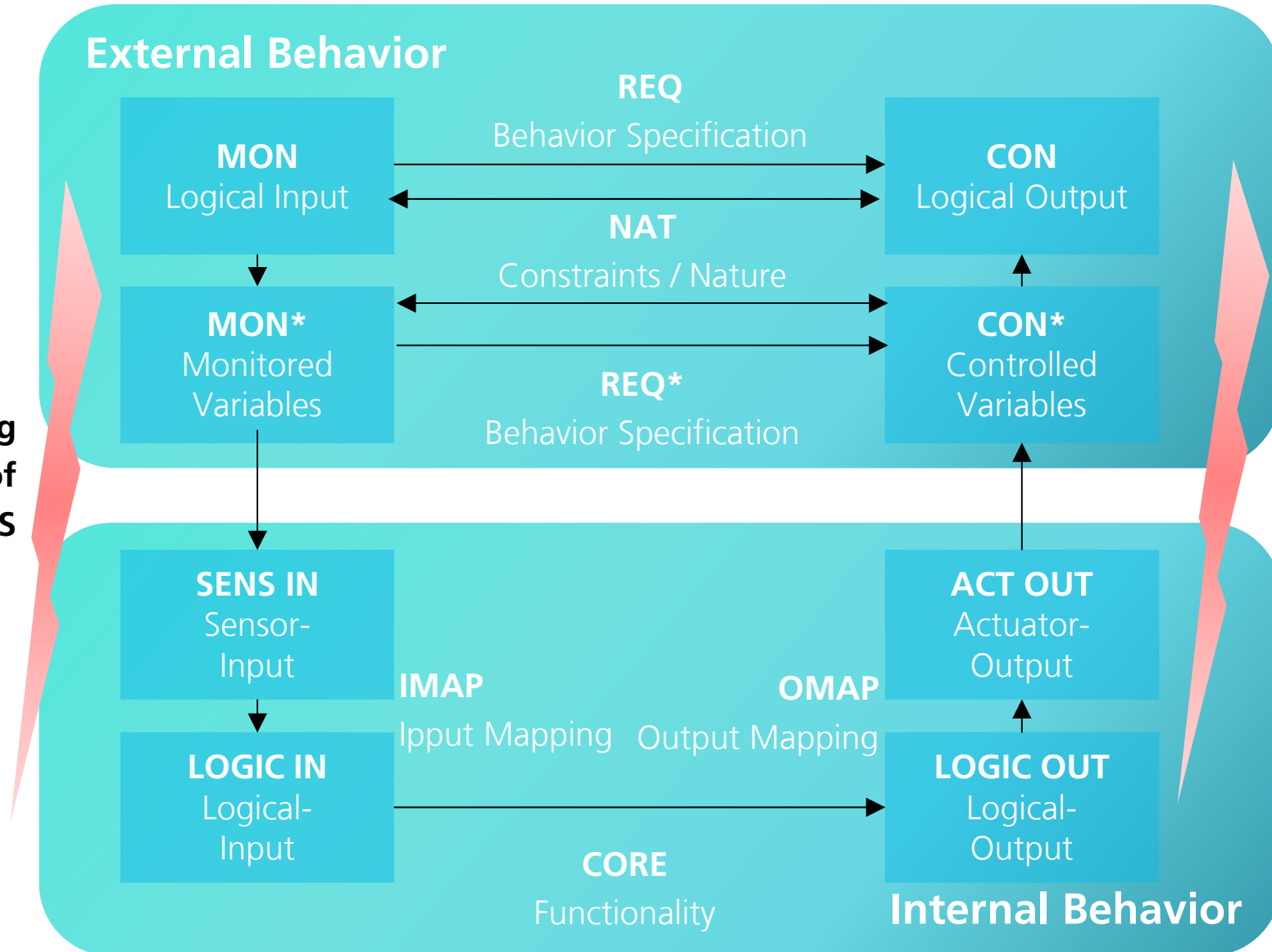


GUIDE PHRASES - EXAMPLE



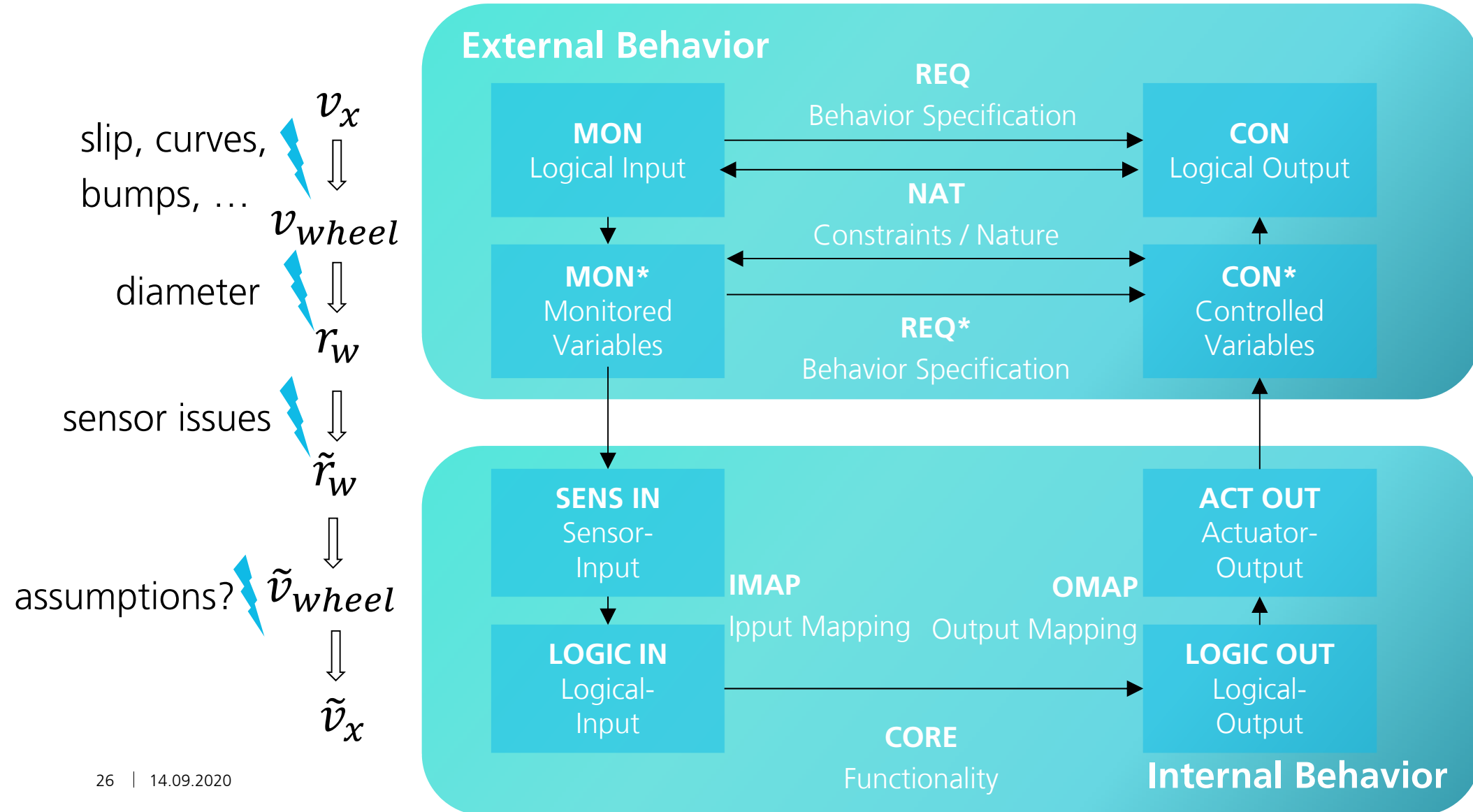
SOME BACKGROUND: THE EIGHT-VARIABLE-MODEL [BASED ON PARNAS' 4-VARIABLE MODEL]

Input and output mapping defines major part of behavior of CPS

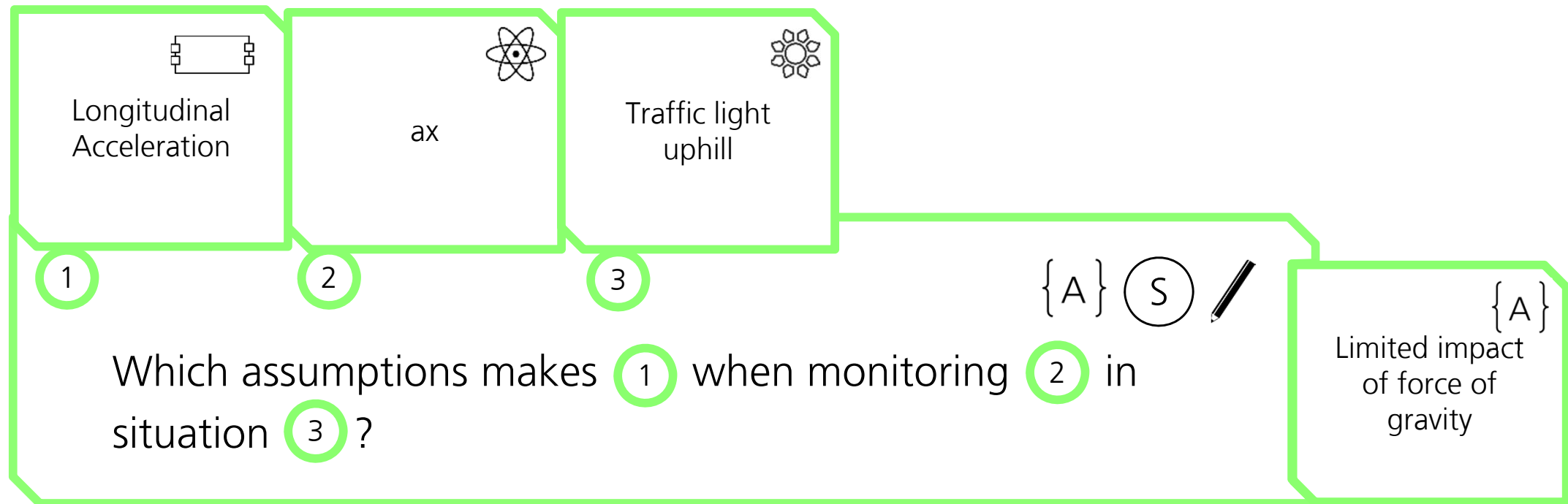


Tremendous, often neglected potential for critical systematic faults!

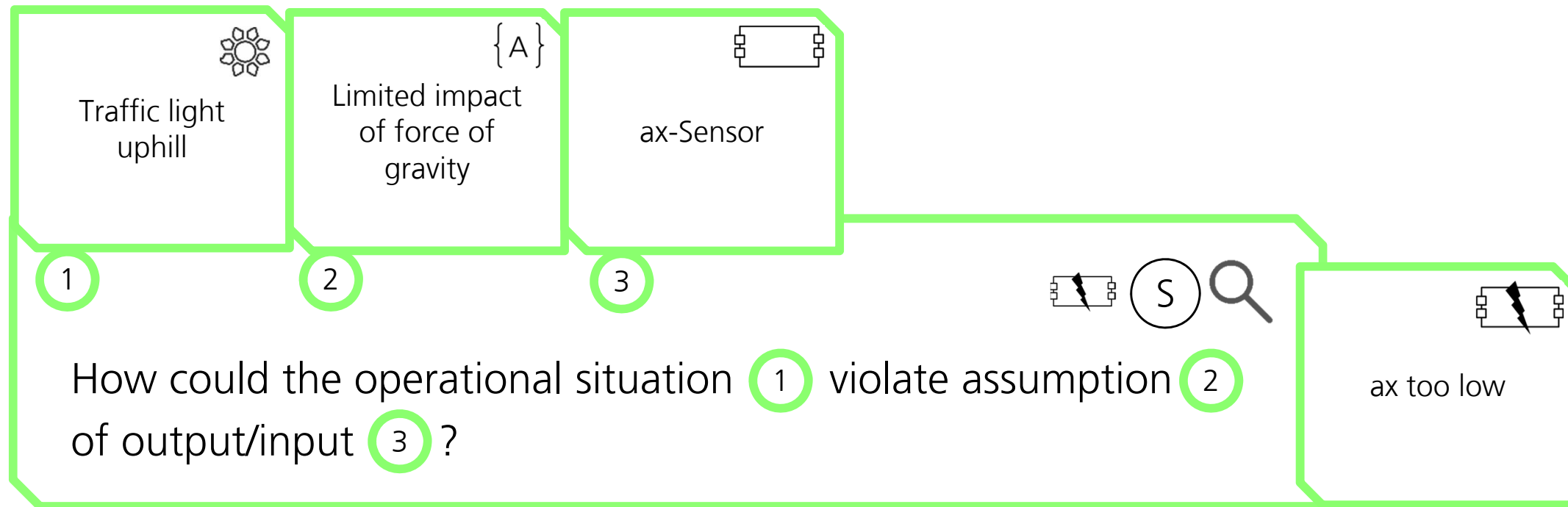
SOME BACKGROUND: THE EIGHT-VARIABLE-MODEL [BASED ON PARNAS' 4-VARIABLE MODEL]



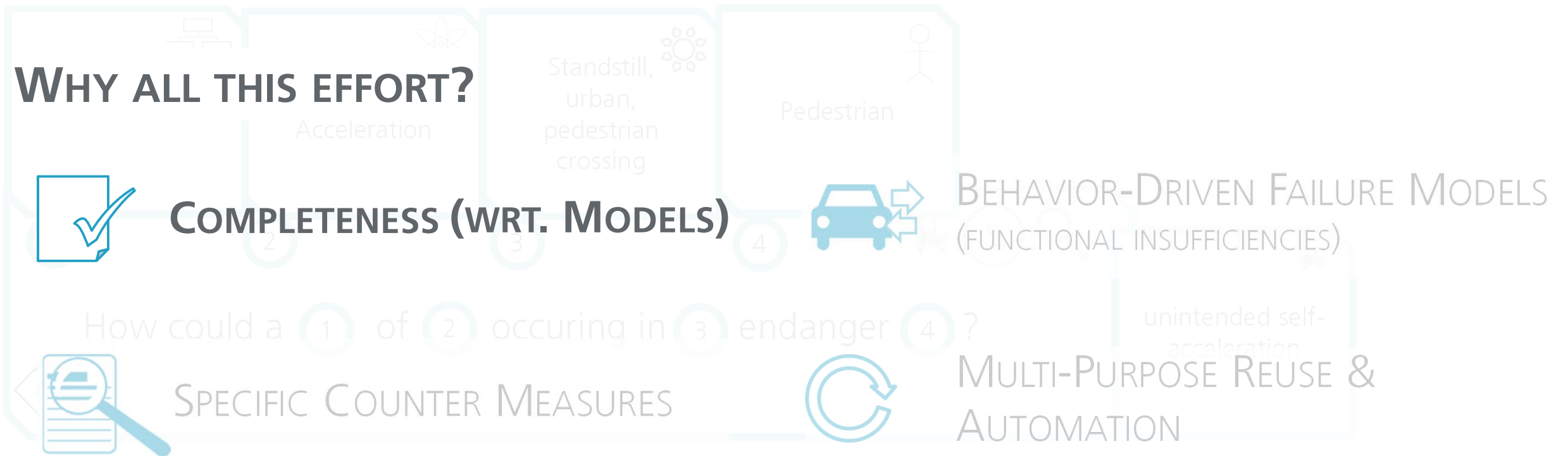
IDENTIFY ASSUMPTIONS



IDENTIFY FAILURE MODES

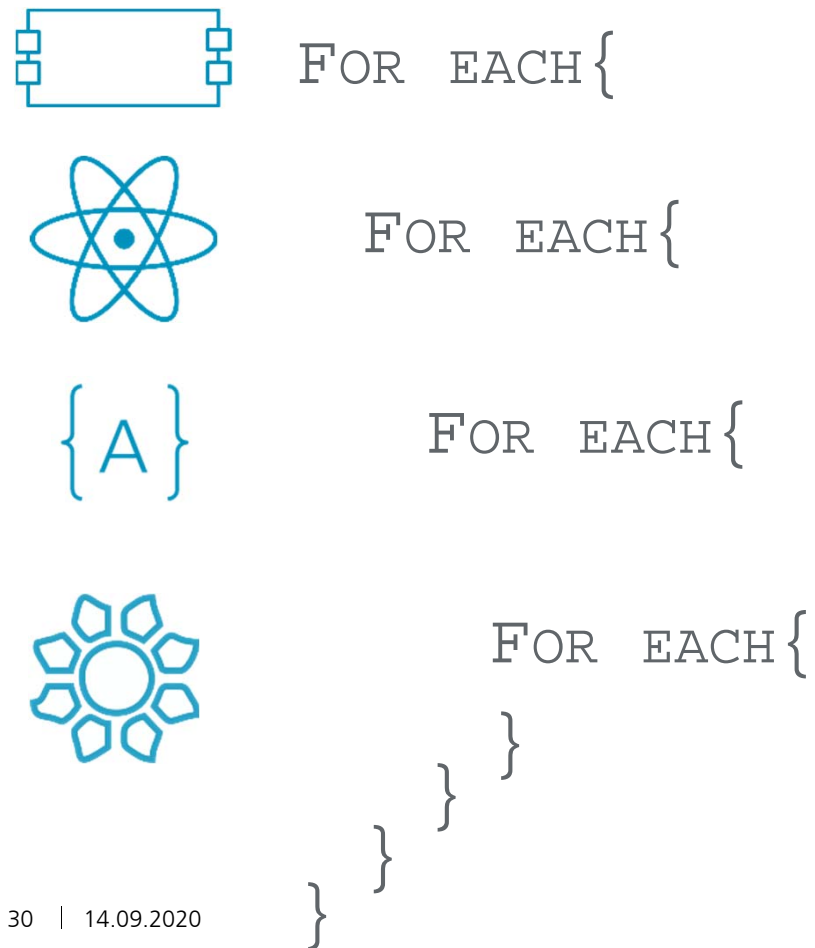


GUIDE PHRASES - EXAMPLE

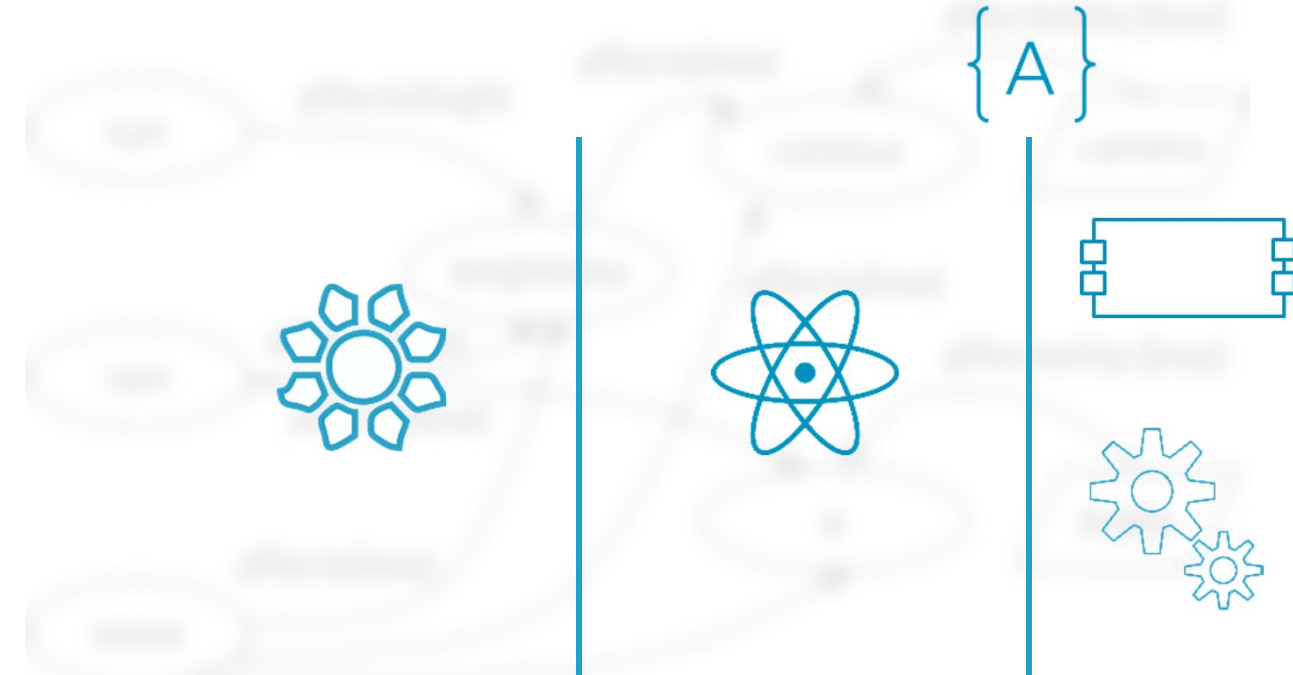


MODEL-BASED COVERAGE

THE BRUTE FORCE APPROACH



THE INTELLIGENT APPROACH



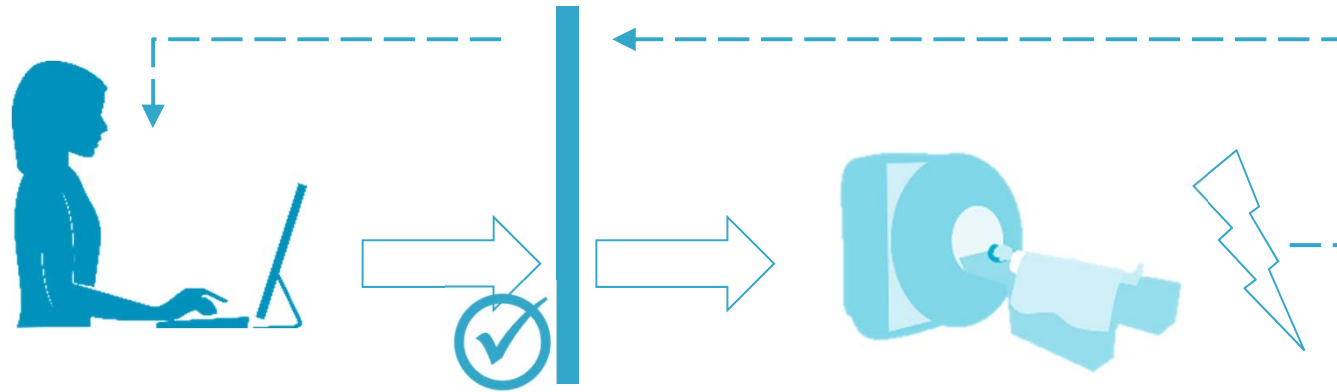
EXTENDED ONTOLOGIES FACILITATE INTELLIGENT SELECTION USING INFERENCE

CONTINUOUS SAFETY MANAGEMENT

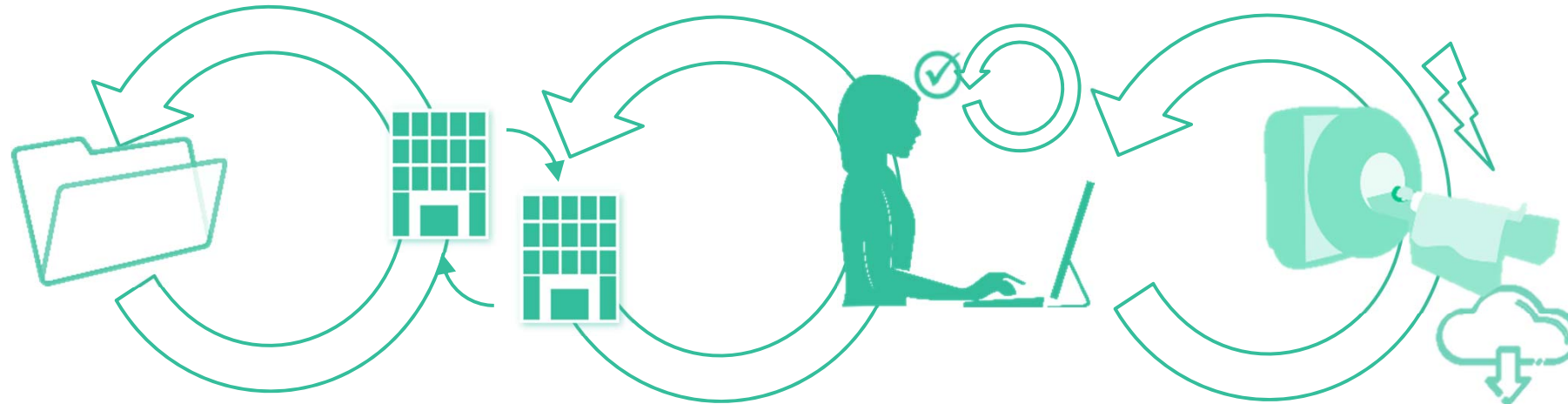


SAFETY MEETS DEVOPS - CONTINUOUS SAFETY MANAGEMENT

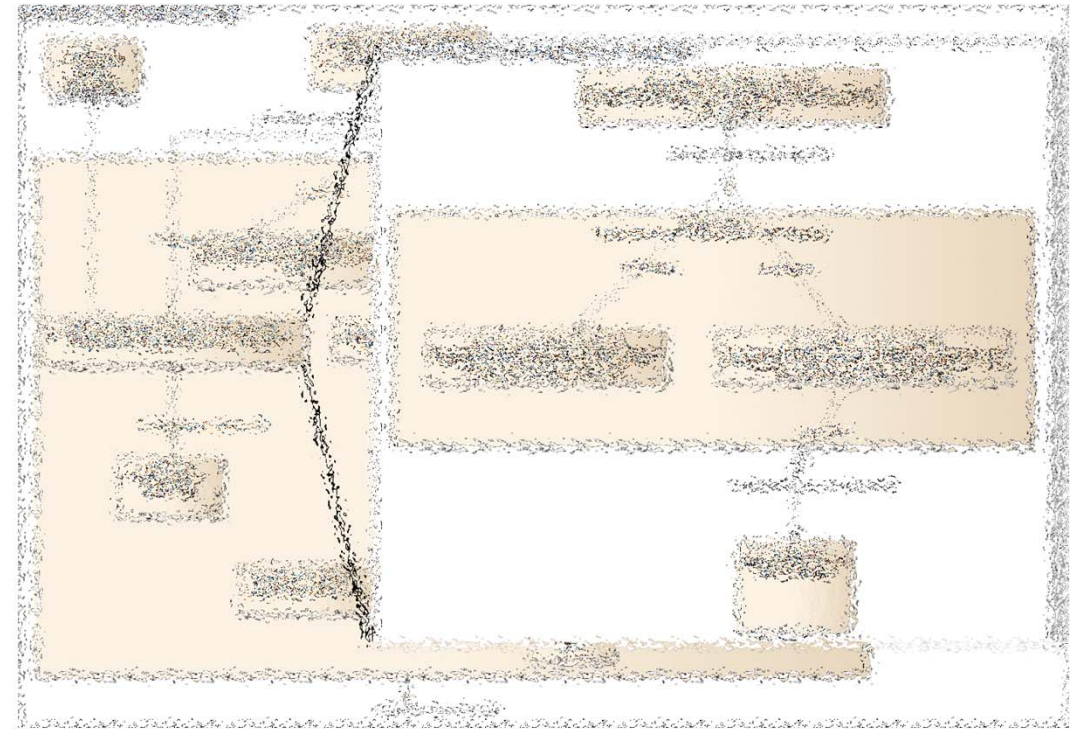
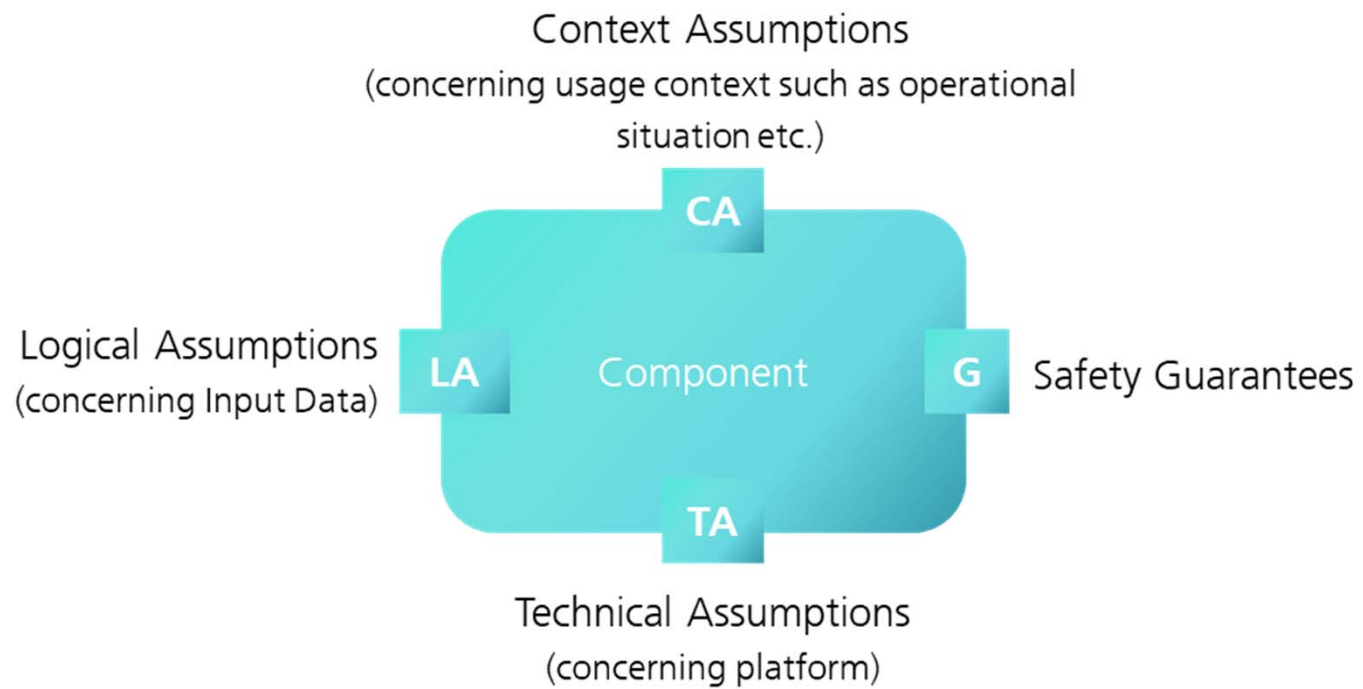
Today



Next



KEY TO SUCCESS: MODULARITY & MODEL-BASED AUTOMATION

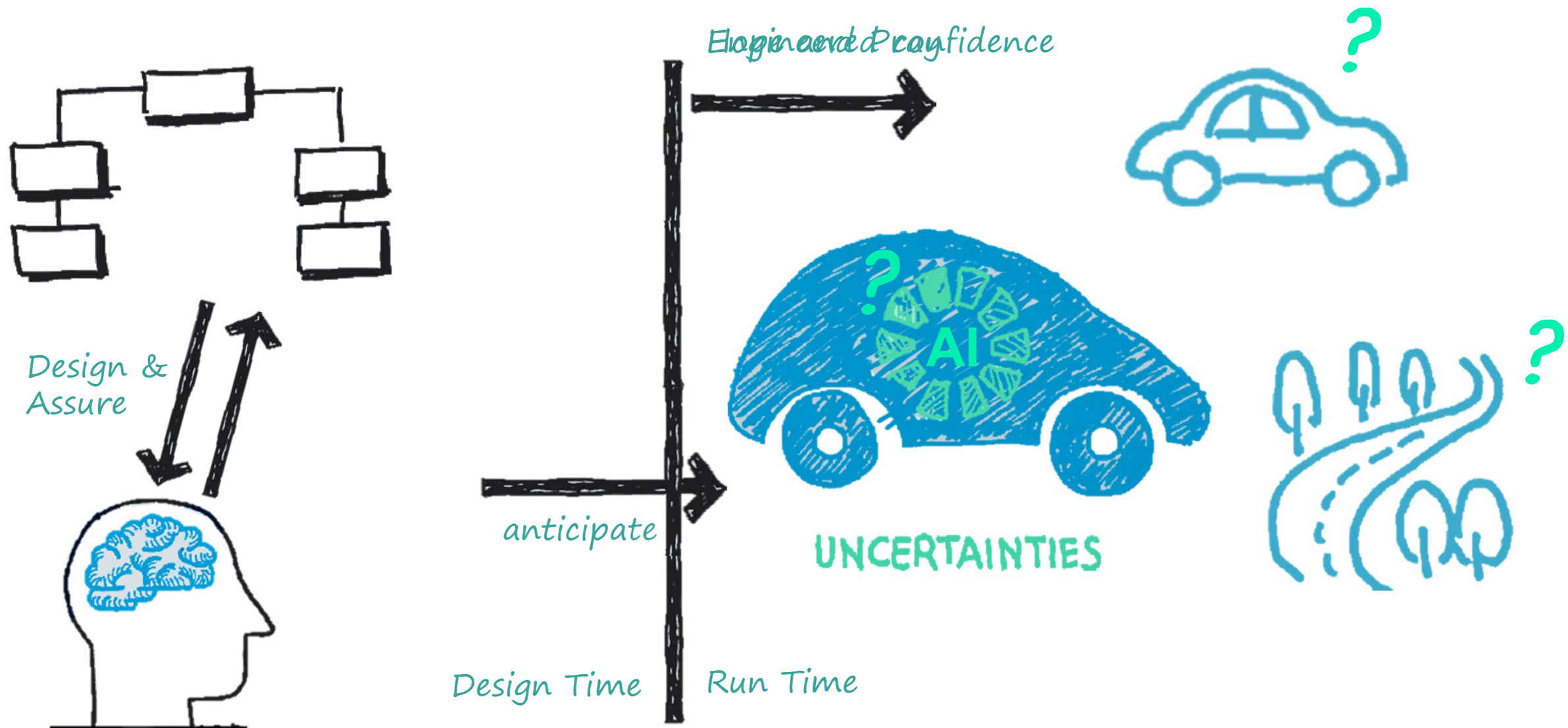


[SafeTBox – Fraunhofer IESE]

ADAPTIVE SAFETY MANAGEMENT

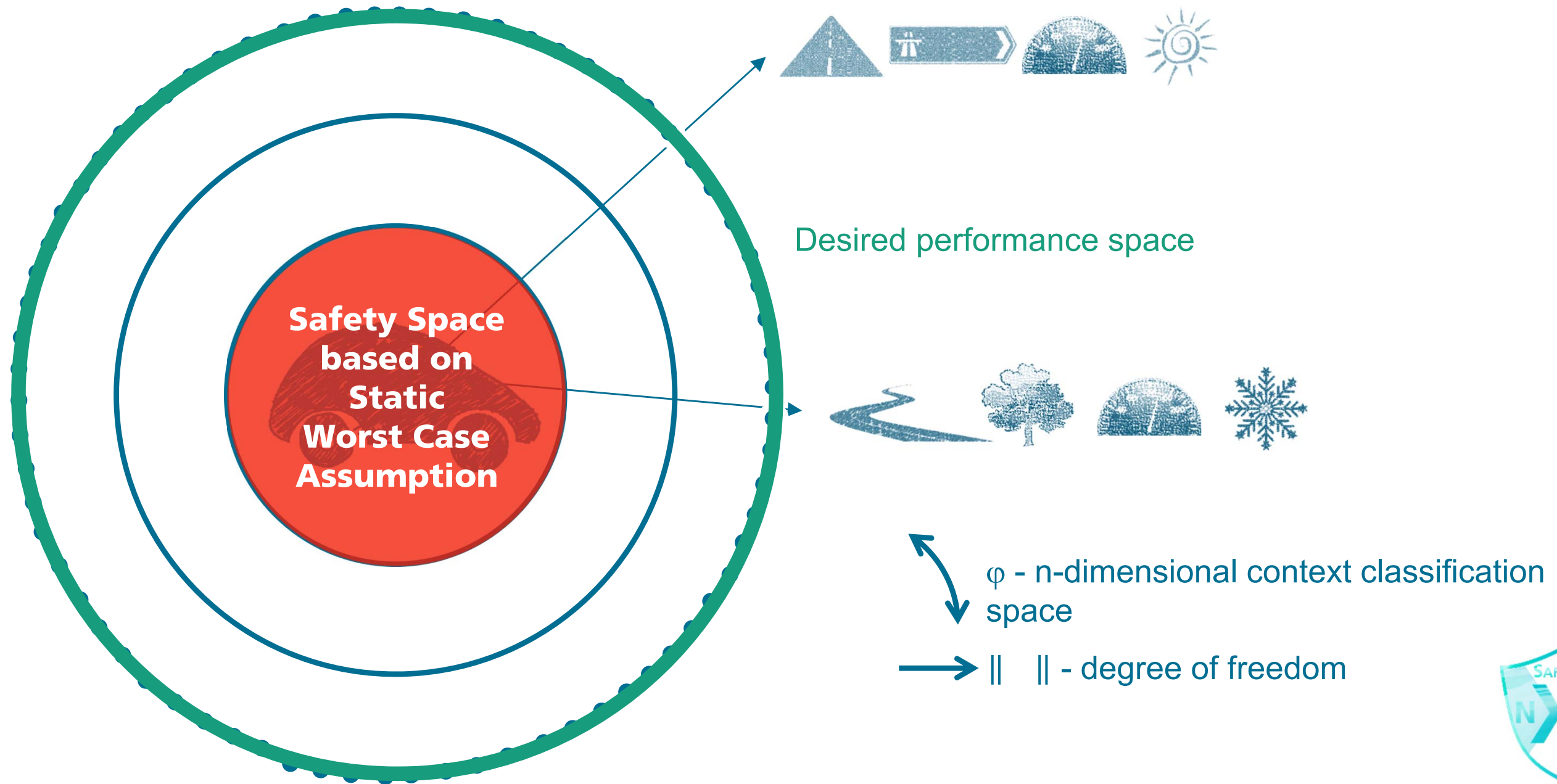


FROM STATIC TO DYNAMIC SAFETY MANAGEMENT

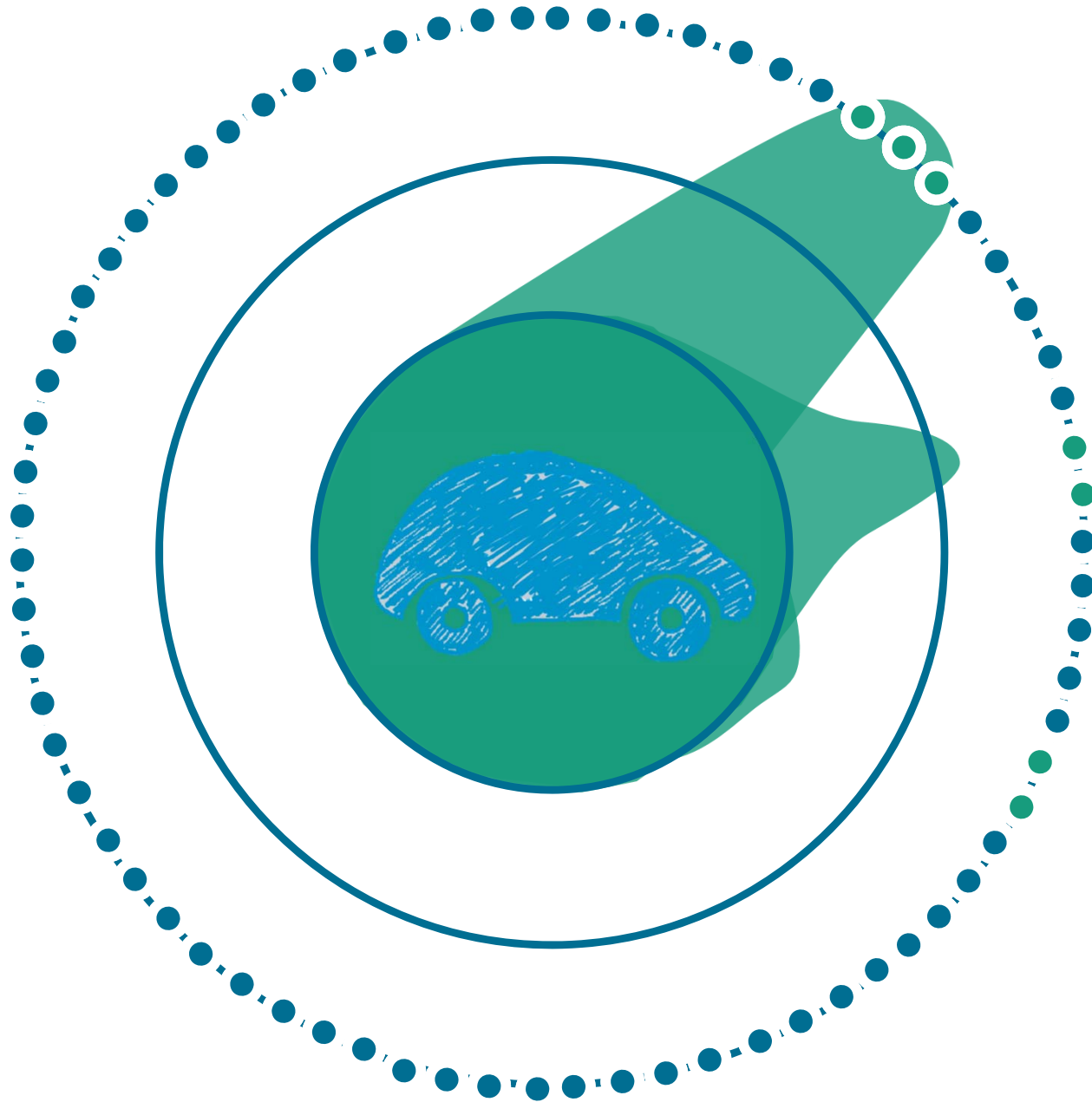


Intelligent Functionality requires Safety Intelligence

MORE FREEDOM BASED ON SITUATIONAL AWARENESS



ADAPTIVE SAFETY SPACE



Dynamic Is-Situation

Dynamic Safety-Space → Adaptive Safety-Space

Adaptive Safety Management

Data/Information



External Context

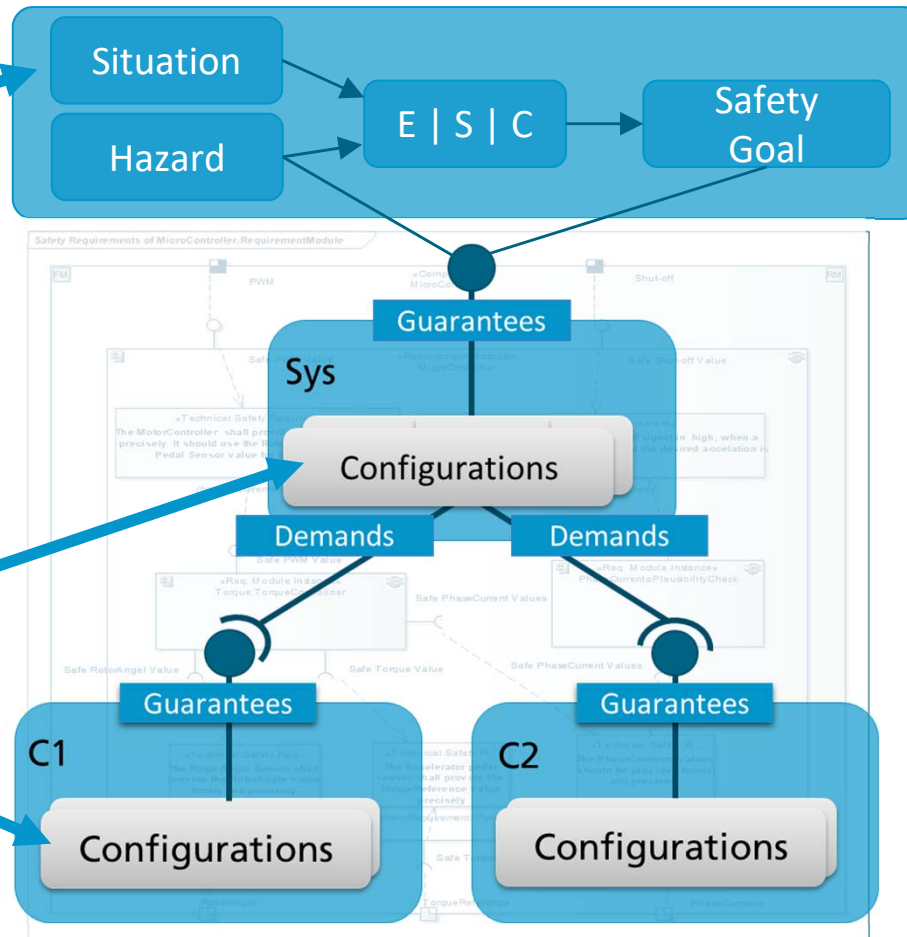


Monitoring

Safety Awareness

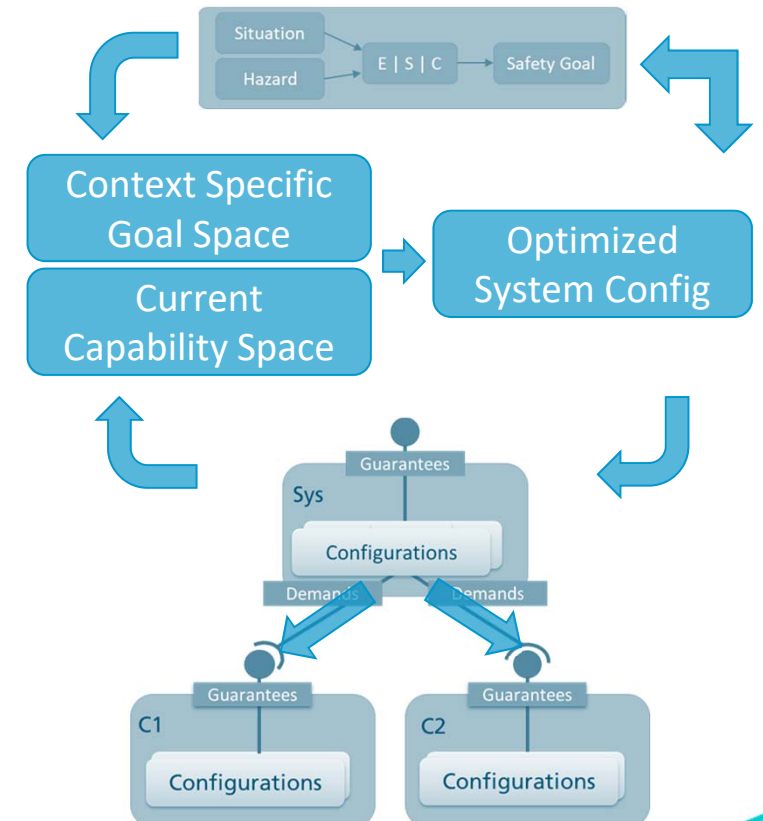
Context-Awareness

Self-Awareness

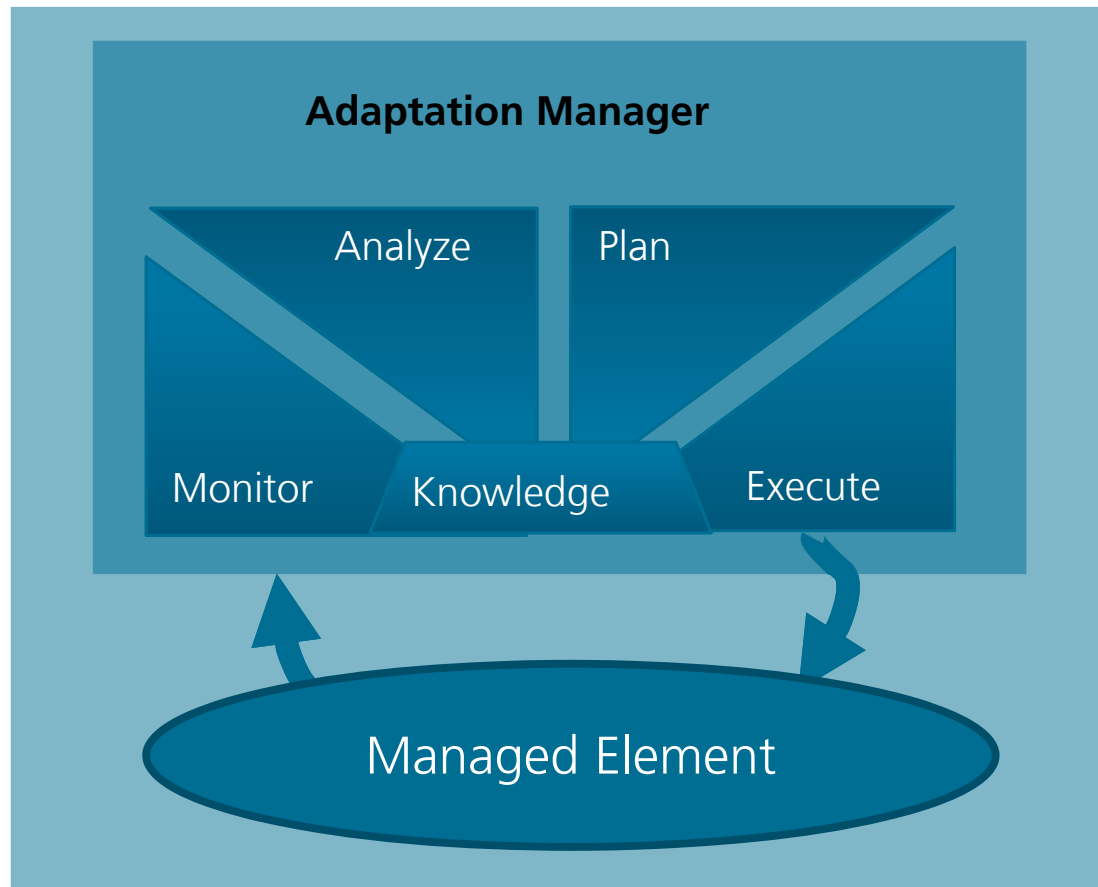


Safety Model @ Runtime

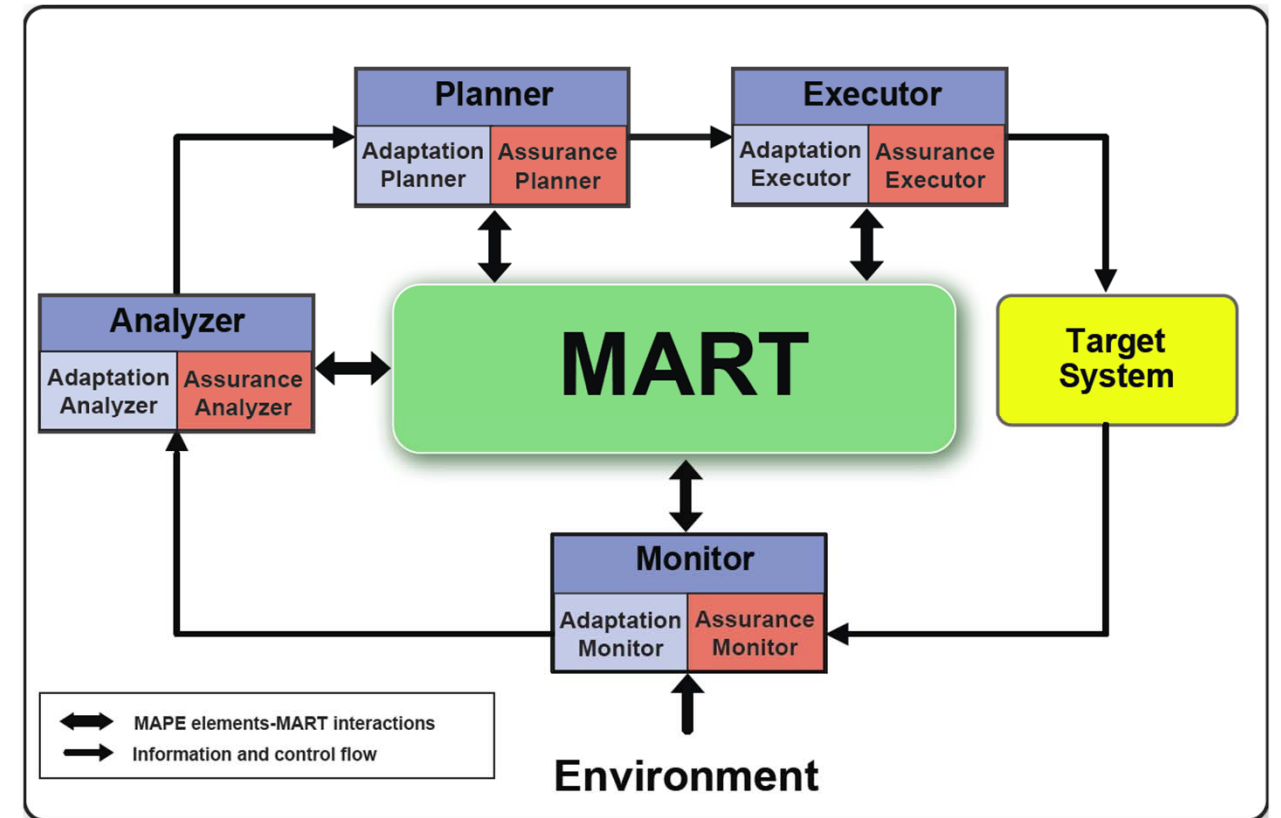
Adaptive Safety Management



BACKGROUND: FOUNDATIONS FROM SELF-ADAPTIVE SYSTEMS

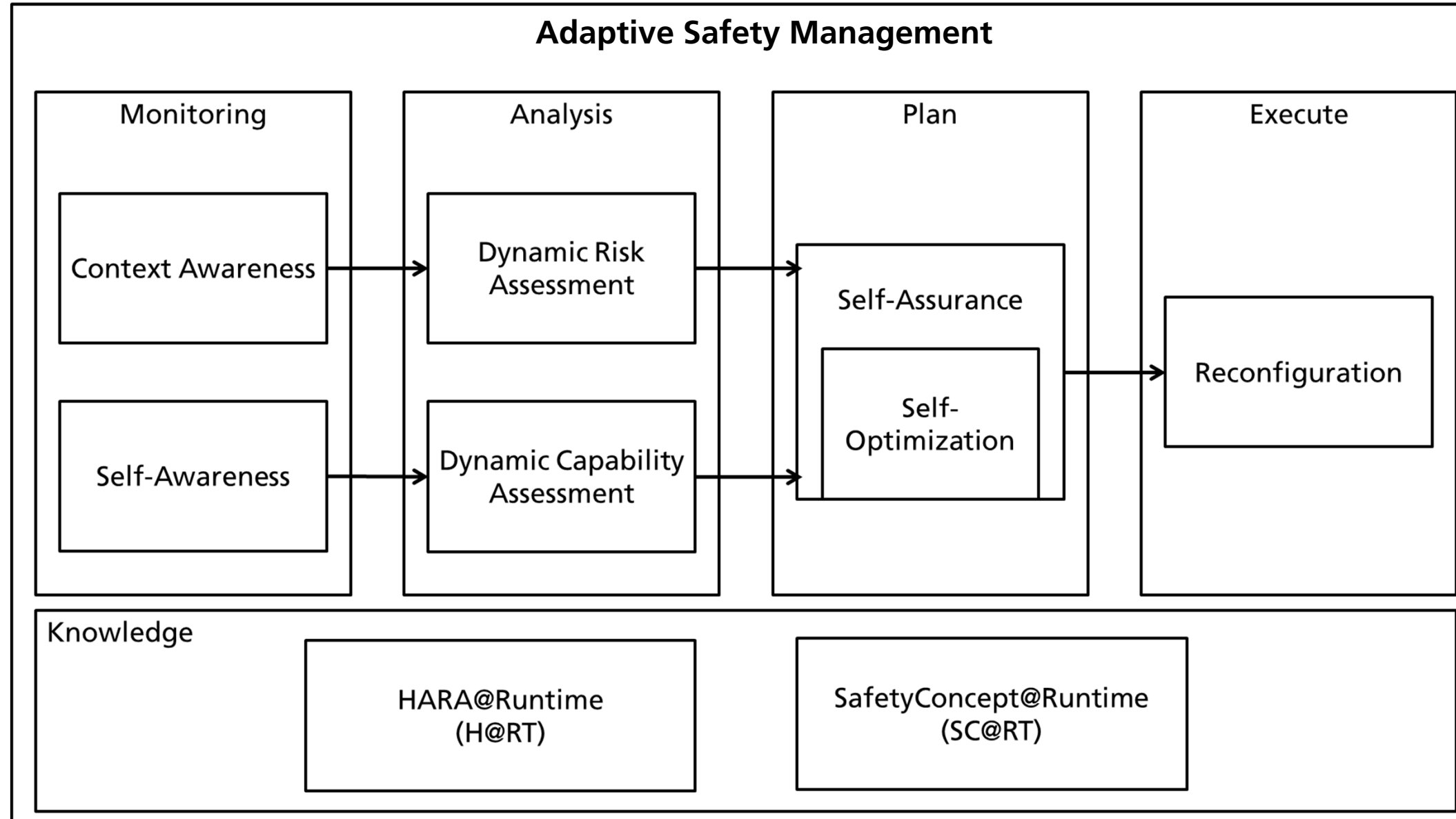


[Kephart, Chess]



[Cheng et. al] (MART = Model@Run.Time)

ADAPTIVE SAFETY MANAGEMENT CYCLE



COGNITIVE SAFETY MANAGEMENT



FROM ADAPTIVE TO COGNITIVE SAFETY MANAGEMENT

ADAPTIVE SAFETY-MANAGEMENT

primarily rule-based

adaptation by dynamic reconfiguration

deterministic & predictable

modular pre-assured

COGNITIVE SAFETY MANAGEMENT

goal-based

self-adaptivity including AI

emerging and adaptive strategies

runtime assurance



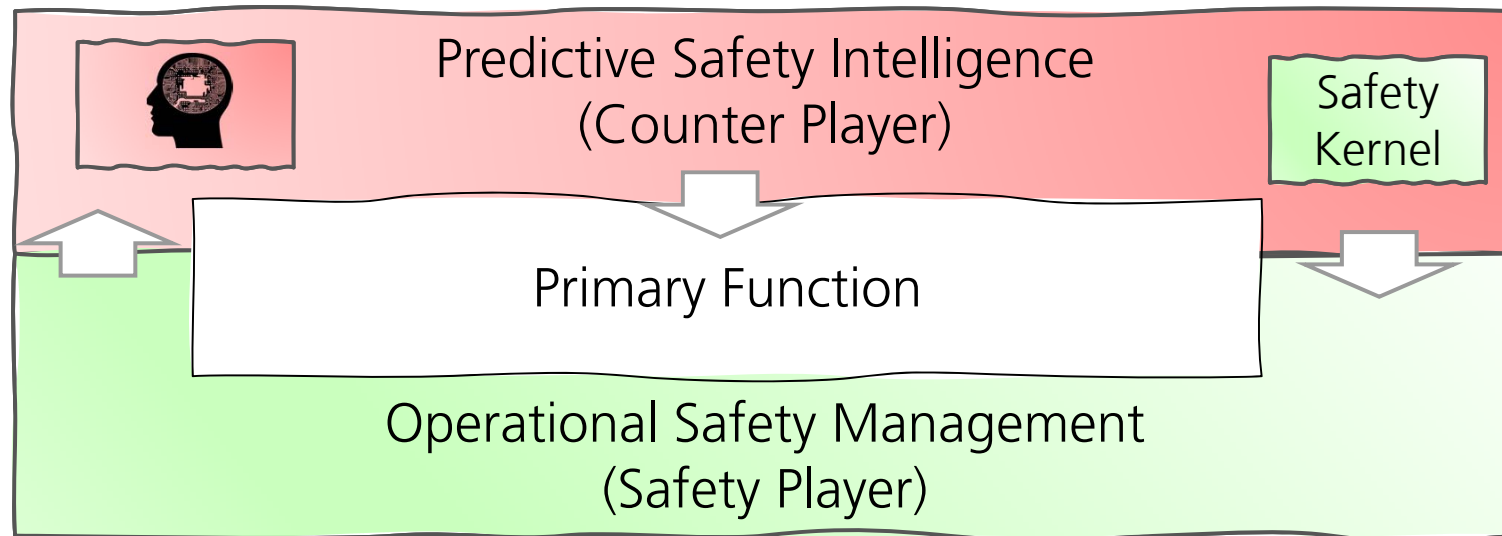
EXAMPLE: INTELLIGENT COUNTER PLAYER ARCHITECTURE

Problem: Safeguards intervene too often (false positive error detection)

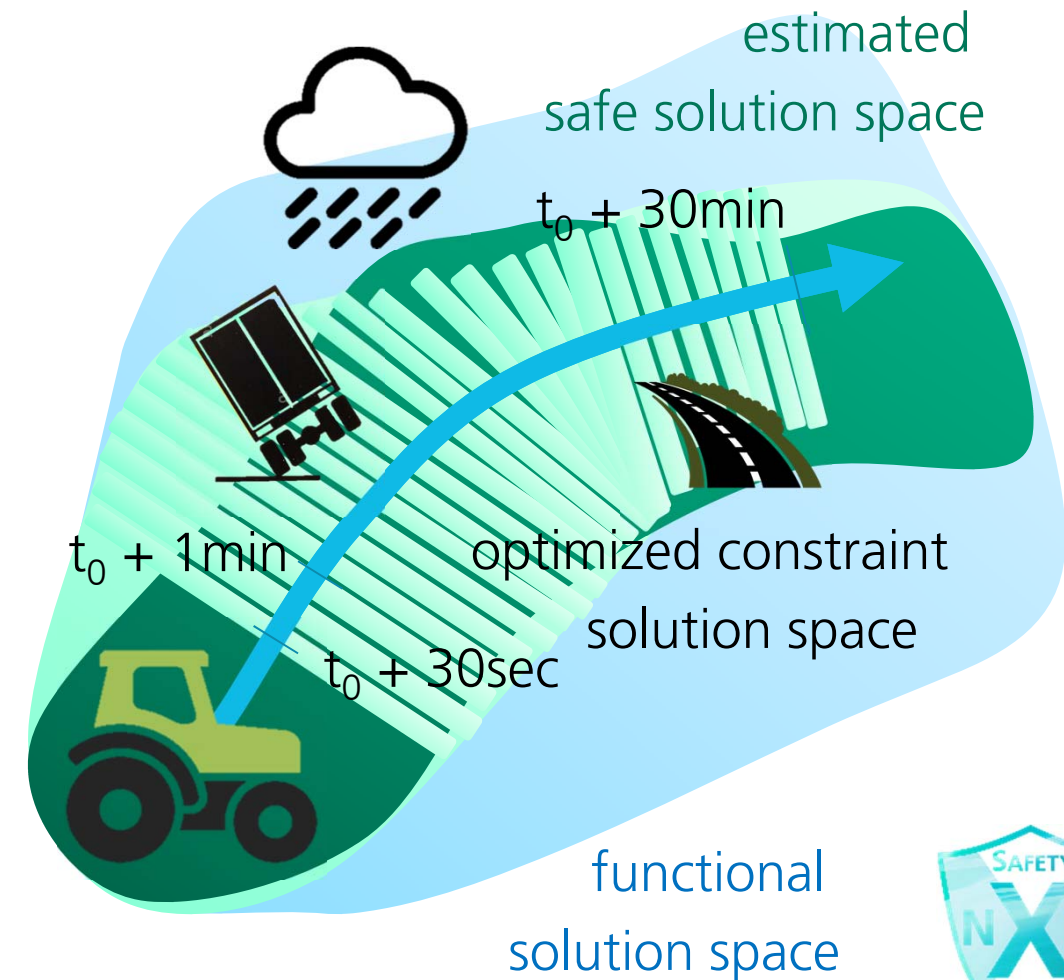
Solution: Make safety measures more intelligent and active at the strategic / tactical level



adapt functionality following goal-based optimization
(avoid safe guard interventions)

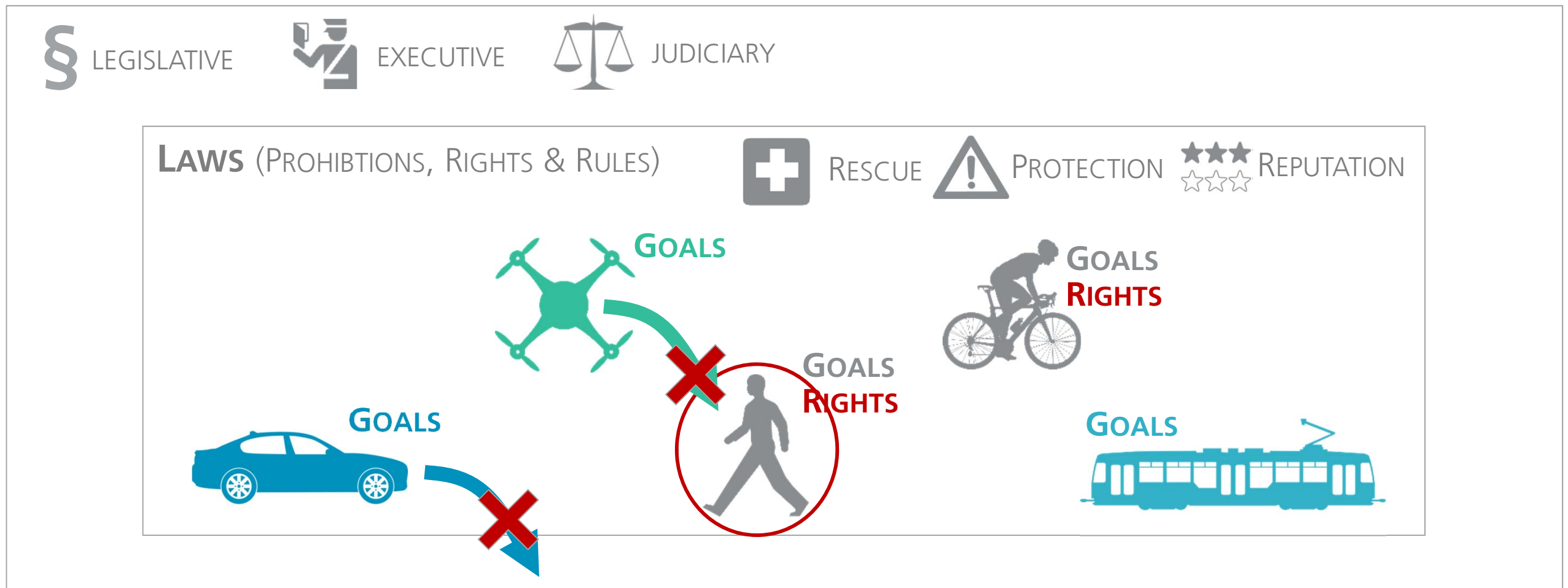


keep system safe



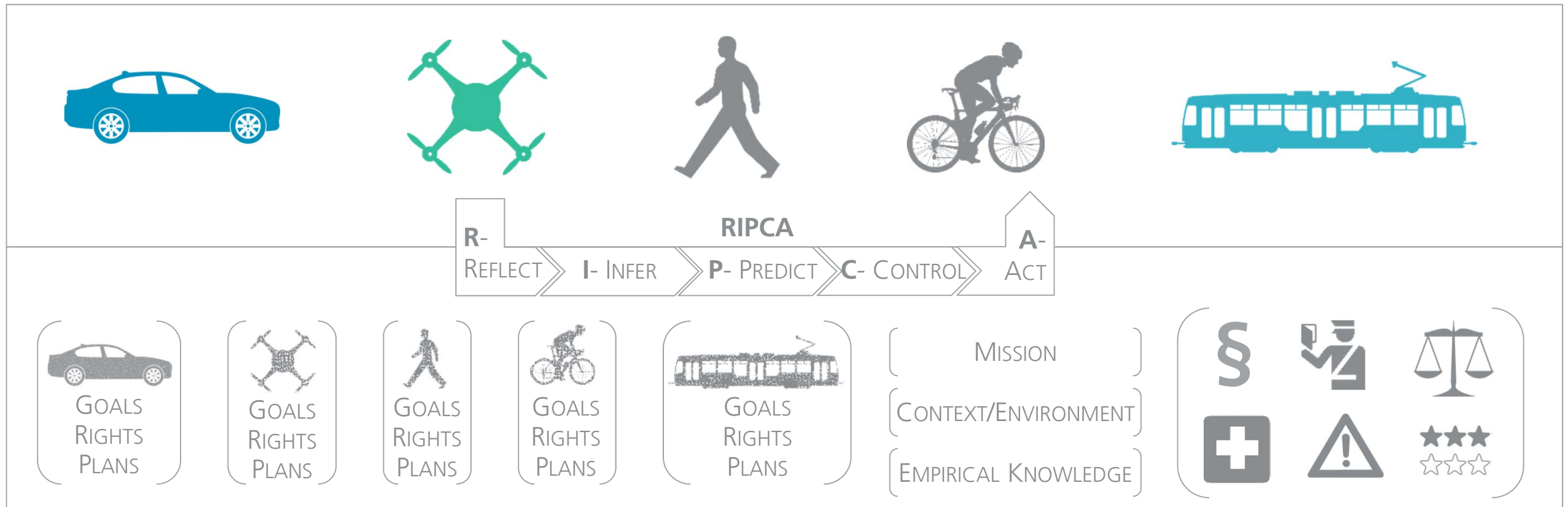
EXAMPLE: CONSTITUTIONAL SAFETY ASSURANCE

CONSTITUTION



CONSTITUTIONAL SAFETY ASSURANCE USING B-SPACES

A-SPACE (REALITY)



B-SPACE (VIRTUALITY)

SUMMARY



Whatever challenge safety assurance will have to face in the future



Model-Based Safety Assurance will be *the* key to success

SAFE INTELLIGENCE