

Operation Design in the 5th Industrial Revolution

Avi Harel, Ergolight Consulting, Haifa, Israel

An extended version of the SERC AI4SE 2025 presentation



The focus of operation design is on
interaction control.

The theme of this presentation is:
AI is essential for enabling **safe operation**
of **complicated systems.**



About Avi Har'el - Ergolight Consulting

- Mathematician (M.Sc.)
- Practice: SW, System, HF, HSI, Integration engineering
- Focus: understanding and preventing human errors
- Affiliates: Technion, Rafael, UPA, HFE, SII, INCOSE, Ergolight
- Projects: Artificial FO, FFA, emergency control, war alarms
- Positions: Head of Usability TC of the SII, FC C2 Intelligence

The **About** info may be found here (<https://avi.har-el.com>).
Please, Email me to get a free copy of the **full presentation**.



Sep. 18, 2025

AI-System Integration (AISi) - Ergolight Consulting: ergolight@gmail.com




What is new in the 5th Industrial Revolution?

The five Industrial Revolutions

Revolution	Timeframe	Challenges
1st	Late 18th – Mid-19th century	Steam and water power
2nd	Late 19th – Early 20th century	Electrification and mass production
3rd	Mid-20th – Early 21st century	Electronics and computing
4th	Early 21st century – Present	Cyber-physical integration
5th (emerging)	2020s onward (projected)	Human-machine synergy, sustainability

<https://www.symestic.com/en-us/what-is/industry-1.0-to-5.0>

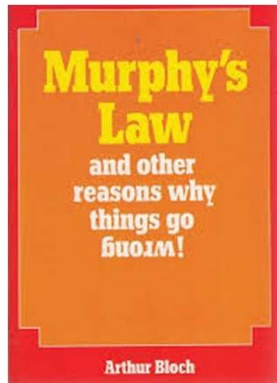


In the 5th IR, systems engineering is **human centric**.
AI offers new opportunities for **sustainability assurance**.
Sustainability is also a hot topic of **operation design**.



Case study: the origin of Murphy's Law

A simple design mistake: enabling an assembly error



The project
MX981 Experiment:
Testing human tolerance
to extreme G force



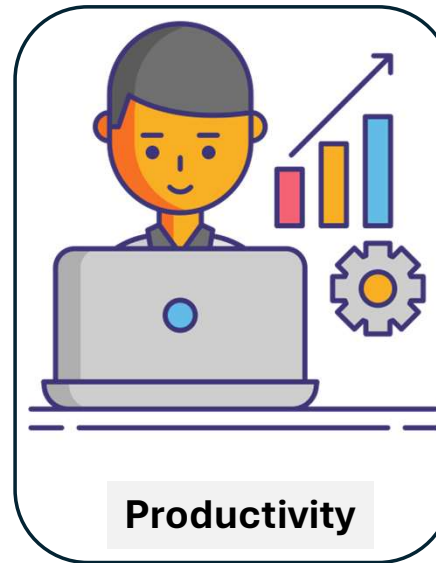
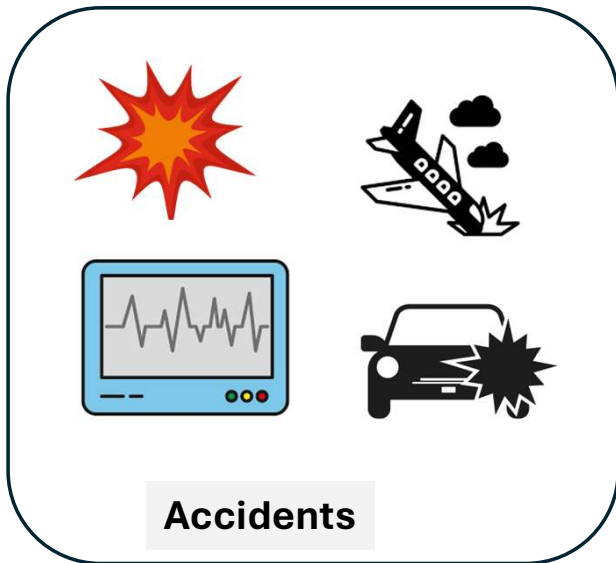
Engineer: Edward Murphy
1949 - Pre-test of MX 981.
Test subjects - chimpanzees
<https://code7700.com/murphy.htm>

Oops ...
Accelerometer
problem.
Assembly error
Poka (error)
due to ...
A design mistake,
...
Enabling the error,
Demonstrating ...

Sustainability **challenge**: protect from errors.
Lesson: we need to **enforce proper assembly** by design.
Methods: Poka **Yoke** (prevention) and **proactive detection**.



The industry need: poka yoke



Exceptions result in **accidents** ...,
hamper **productivity** ..., and the
experience of using everyday things.



Coordination failure

Examples: friendly fire accidents (FFA)



1990 - Zeelim A
Artillery support
Control error



1992 - Zeelim B
Special forces
Ammunition error
https://en.wikipedia.org/wiki/Operation_Bramble_Bush



Kandahar 2001
Air support
GPS mode error
<https://uxdesign.cc/bad-design-kills-eight-300f9623cb61>

Different weapons, similar results
Same failure mode: scenario confusion
Same protection: **scenario-driven coordination**
Challenge: enforce **cross-branch learning** from accidents



Sep. 18, 2025

AI-System Integration (AIS) - Ergolight Consulting: ergolight@gmail.com



Topics of this presentation

- Modeling **normal and exceptional operation**
- Modeling **discipline maturity**
- Integration = human behavior + **inter-unit coordination + HSI**
- System vars: from assembly error to **troubleshooting**
- Antifragility: sampling and **learning** from incident
- Protection **layers**: proactive (preventing) and reactive (alerting)
- Coping with **complexity by scenario-centered design (SCD)**



Engineering challenge: reduce sustainability loss

70% to 90% of operational failures are due to human error.

Industry	% Attributed to Human Error	Key Source(s)
Aviation	70%–90%	Boeing Safety Reports, FAA Human Factors Division
Healthcare	~70%–80%	WHO Patient Safety Reports, BMJ (Makary & Daniel, 2016)
Manufacturing / Industrial	60%–80%	OSHA Guidelines, National Safety Council
Information Technology	75%–95%	IBM Cybersecurity Report (2020), Gartner Cloud Security Forecast
Nuclear / Energy	70%–80%	U.S. NRC Human Factors Reports, IAEA Chernobyl Analysis
Cross-Industry / General	70%–90%	James Reason (1990), Sidney Dekker (2014)

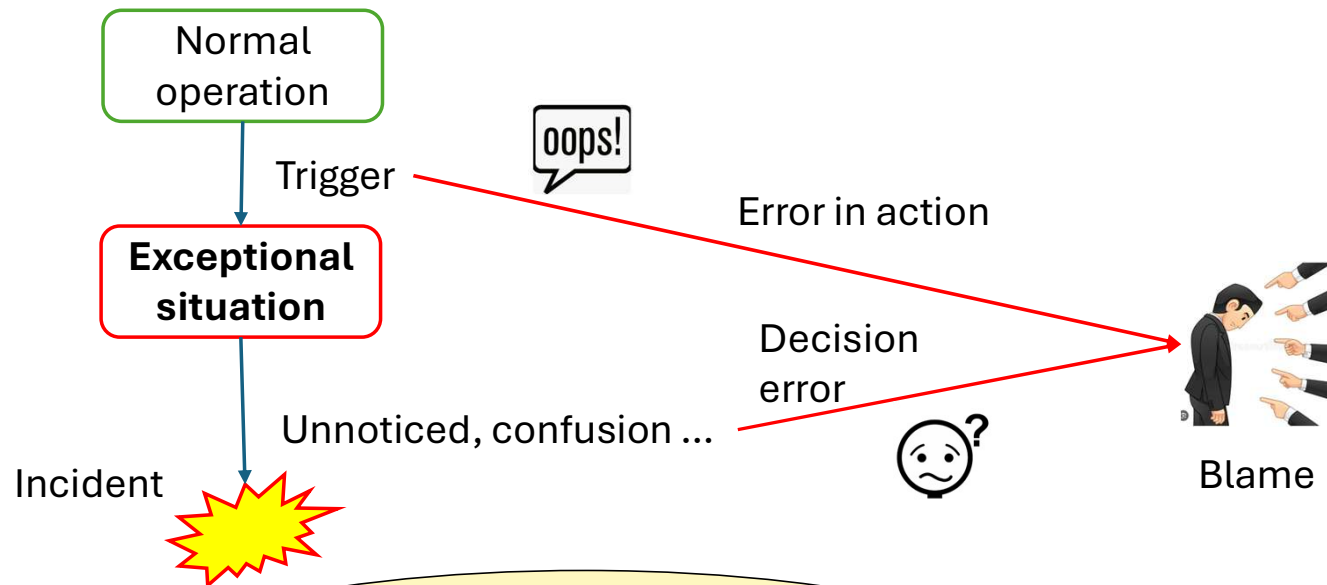


Goal: understanding errors



A naïve model of error generation

What do we mean by “error”



Design mistake:
enabling activity
diverting the situation
to **exceptional**

And/or ...

Design mistake:
enabling operation
in **exceptional**
situations

Error generation is a sequence ...
Errors are associated with blame.
Errors are associated with **exceptions**.
Discussion: Can we prevent errors?



Sep. 18, 2025

AI-System Integration (AISI) - Ergolight Consulting: ergolight@gmail.com



A model of operational risks

Flexibility, bumpers, options, exceptions ...

System operation can be **seamless**, if we know the way, and it can be difficult and risky, when in a new area with **bumpers**.



Sustainability rules:

1. The procedures for task completion should be **unique**.
2. Stay on the **paved road**. When applicable, **avoid options**, and **prevent exceptional activity**.
3. When **off track**, facilitate **resuming** operation on the paved road.



Rephrasing **Murphy's Law**,
Failure should be attributed
to operational **flexibility** .

Sep. 18, 2025

AI-System Integration (AIS) - Ergolight Consulting: ergolight@gmail.com



Views of failure

Traditional view
Focus on **performance**



Engineering view
Focus on **QA**

Explaining failure:

- Force majeure
- Blaming the operators
- Black swans (rare events)

Tackling complexity:

- Standard solutions
- Modeling
- **New: AI support**



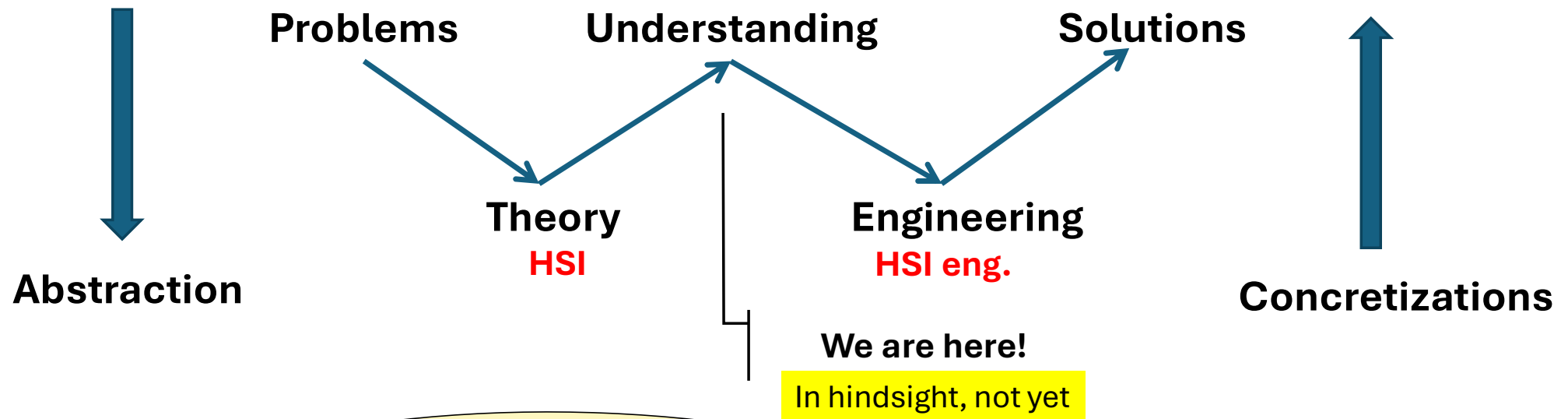
AI accelerates
cost-effective
development.

Sep. 18, 2025

AI-System Integration (AISI) - Ergolight Consulting: ergolight@gmail.com



A model of discipline maturity – HSI 2019



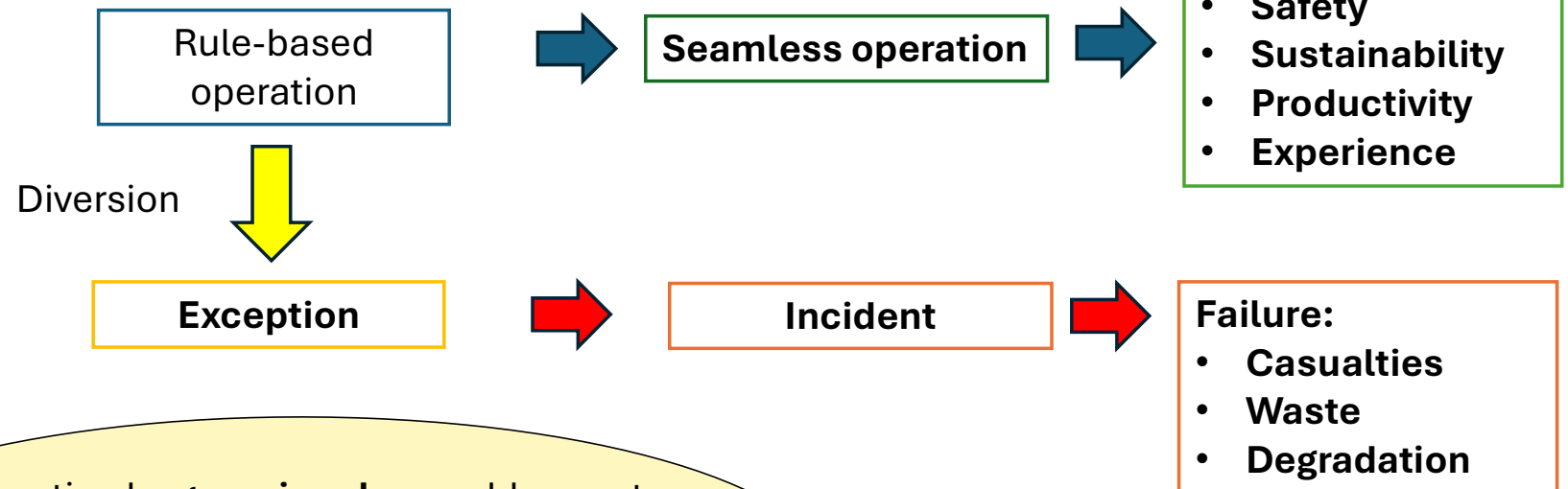
The **W model of HSI development** – Biaritz, describing typical scientific progress, from theoretical HSI to engineering. It seems that we are not there yet. With AI, we may be there shortly.



Utility-oriented approach Exception Avoidant Design (EAD)



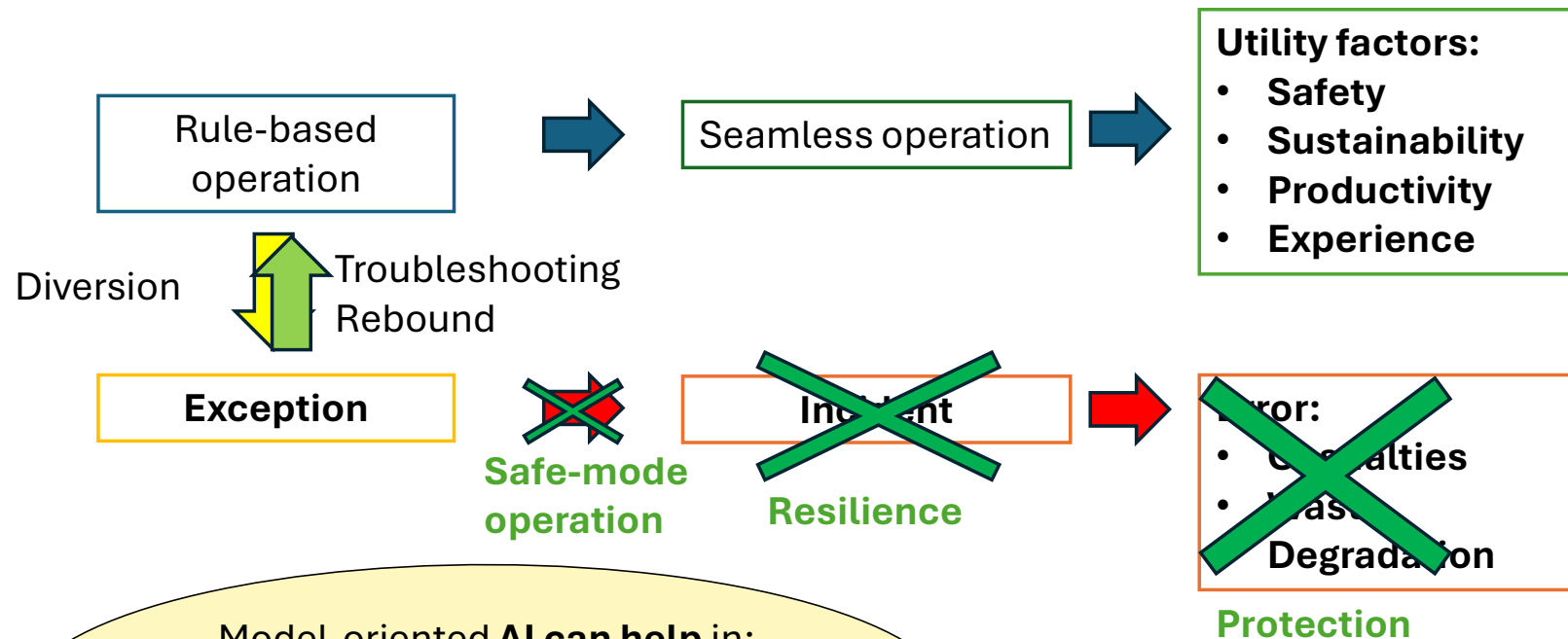
Hollnagel - 1983



Operation by **generic rules** enables cost-effective design of seamless operation. Errors are due to **exceptional operation**. Challenge of operation engineering is to **prevent diversion from the rules**.



Exception Handling

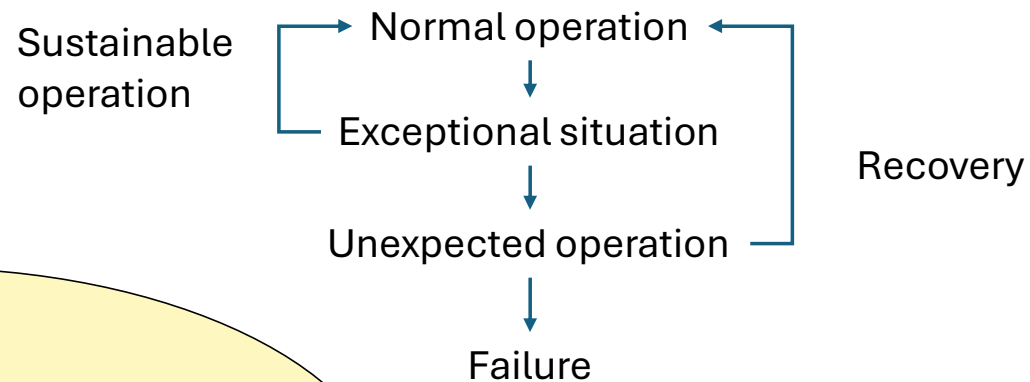


Model-oriented **AI** can help in:

1. Early **detection** of the exception
2. Fast **troubleshooting**
3. **Recovery** procedures



A model of operational sustainability



Goals:

- Sustain normal operation
- Prevent operational failure

Challenges:

- Maximize the operation according to the specifications
- Prevent and recover from operation in exceptional situations



Approaches to failure prevention

Complying with the rules defining normal operation

Proactive approach: exception prevention

- Following the operational rules: scenario-driven situational coordination

Reactive approach: exception management

- Exception detection: detecting violation of the operational rules,
- Reaction: alerting, resilience, safe-mode operation, ...



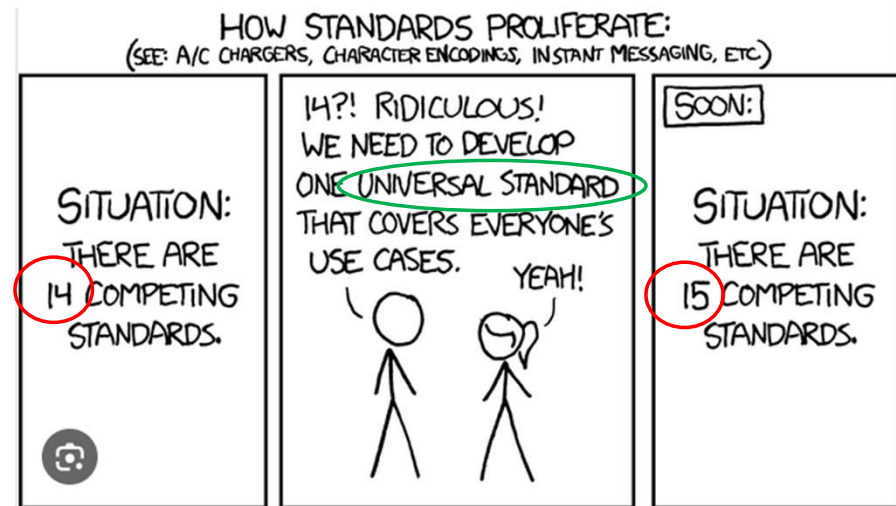
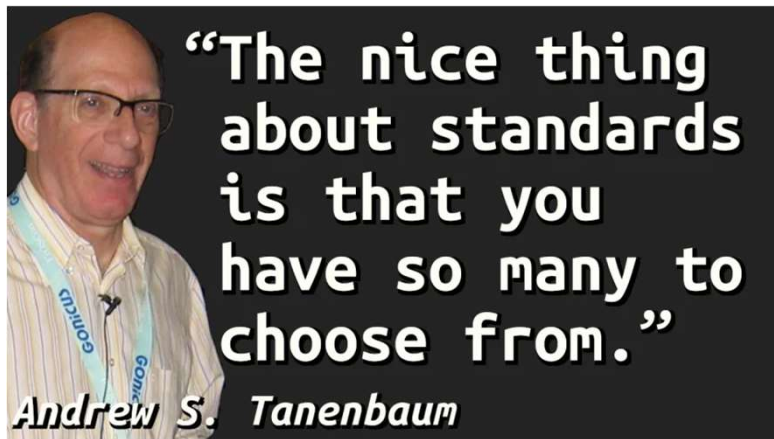
Sep. 18, 2025

Two layers of coping with exceptions:

1. Proactive: exception prevention
2. Reactive: exception management



The role of standards



We need a guide for choosing the right standard.

Oops ...

Model-oriented AI may guide us in finding the proper standard, and the topics in the guide applicable to our project.



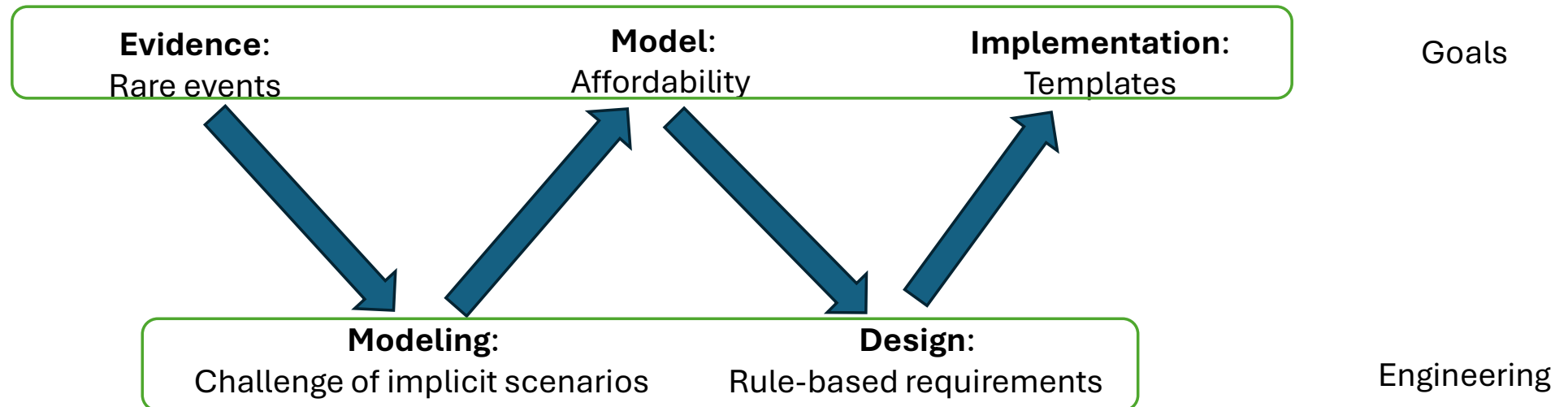
Sep. 18, 2025

AI-System Integration (AISI) - Ergolight Consulting: ergolight@gmail.com



2025 revision of the W model

From evidence to implementation



Sep. 18, 2025

Discipline development

2019: HCD → HSI; utility, outside-in, interaction, architecture, failure modes, human errors, exceptions, triggers, resilience

2025: HSI → SCD; Controller multi-service interaction, **complexity**, fuzzy situations, cost- effect, Scenario-centered design, **AI**, rule-based coordination, generic models and rules



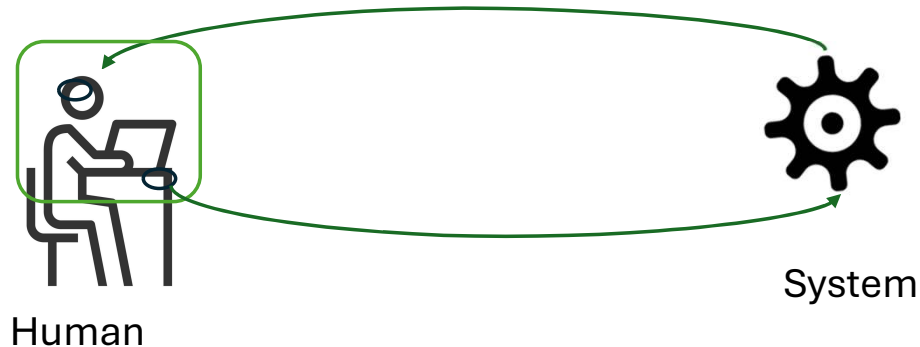
A naïve model of Human-System Integration

A basic architecture for operational sustainability

HCD approach

Human failures:


- Perception
- Decision
- Action



SE approach

System failures:

- functional
 - Installation error
 - Unit failure
- Scenario confusion
 - AF 296
 - Mode mismatch (FFA)
- Synchronization
 - Therac 25
- Spec mistakes
 - consistency
 - Completeness
- Implementation
 - Reverse engineering
 - Bugs.



In the first HSI workshop – Biaritz, 2019:
HSI vs. HCD: Is it the same old bess
in a new dress?




Errors in the 5th Industrial Revolution

Old view

- Errors are due to limitations of human capability
- We cannot protect from the unexpected
- Errors are due to complexity
- Errors can be mitigated by training
- Errors may be prevented by standards

New view

- Errors are due to **design mistakes**
- We can learn from prior **unexpected**
- Errors are due to operating in **exceptional situations**
- Errors can be eliminated by **rule-based operation**
- There is a problem with current use of **standards**. AI may help.



The new view: Enabling **seamless operation**
It is important to shift from the old to the new view.
AI may help to support the new view



Coping with operational complexity

Guidelines based on model-oriented RCA

Motivation: cost-effective development

- A solution is applicable only if it is affordable
- Key requirement f is minimal complexity

Challenge: operational complexity

- Rule-based models
- Generic modeling, cross-domain, cross-industry

Benefit of scenario-centered design: rule complexity, by # of state machines

- Common design practices: exponentially dependent on the size of the situational space
- Scenario-based design: linearly dependent on the size of scenario space


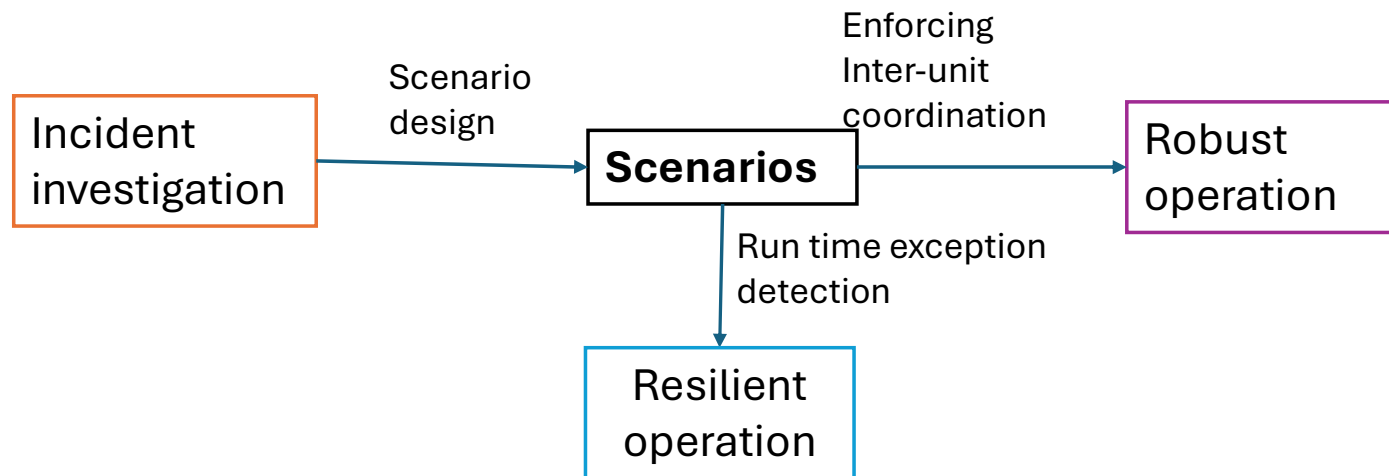


A situational space consists of all the situational array.

A situational array is a set of value of the system state machines



Affordable control of complicated situations by Scenario-centered design (SCD)



Scenarios enable exception prevention
And are required for exception detection.
The goal is to enforce situational coordination.
AI can help.



Situational coordination

Challenge of situational coordination

- Exception control in complicated situations

Scenario-driven situation setting

- Explicit scenarios are essential for the coordination.
- Primary rules defining mapping: scenario → {state machines}
- enabling to reduce the complexity: exponential → linear

Enforcing coordination

- Scenario-driven situation transition

Reacting to exceptions

- Proactive troubleshooting: early detection of rule violation
- Alarm, notification, auto-stop.



This is a list of key topics
considered in coordination design.



Challenges of sustainability models

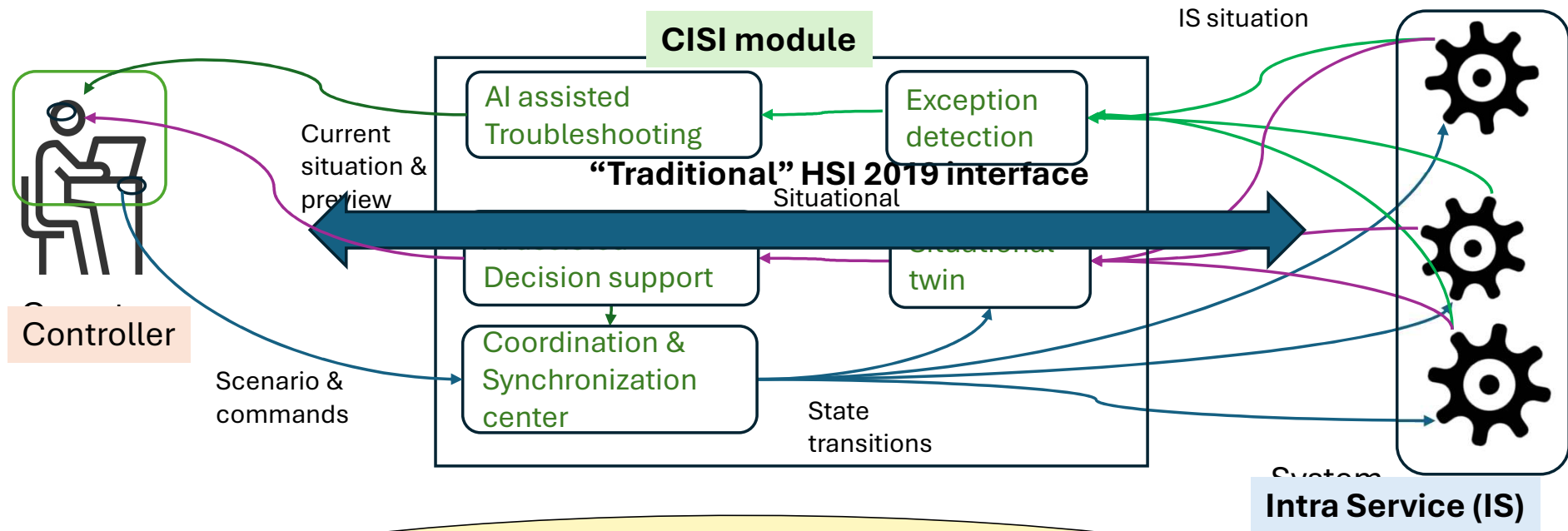
- Enforce system coordination
- Enforce human-system coordination
- Exception detection
- Diversion detection
- Coping with the unexpected
- Troubleshooting support
- Operational decision support



These are topics that should be handled
in sustainability-oriented models.

Controller **Intra-Service** Integration (CISI)

Architecture for operational sustainability



The CISI model is an **extension** of the 2019 HSI paradigm. Operational sustainability may rely on a **CISI module**, enabling **AI-driven** troubleshooting and decision support.



Case studies demonstrating the new architecture

- The Coordination & Synchronization (C&S) center
 - 1990, 1992, 2001 FFA – dynamic, fuzzy scenario-driven situation setting
 - Therac 25 – the synchronization challenge and solution.
 - TMI backup pump – detecting the exceptional pump state
- AI assisted decision support
 - 1990, 1992, 2001 FFA – proactive situation verification, by situational preview
 - TMI backup pump – preview the risks of ignoring the exception
 - AF296, AF447, PL603 – situational preview
- AI assisted troubleshooter
 - Therac 25, AF296, AF447, PL603 – hazard detection and resolution.



<https://avi.har-el.com/eng/Articles/>



Further Modeling Requirements

- Normal operation should be expressed in terms of **operational rules**
 - **Exceptions** are diversion from the rules
 - Inform operators about crossing **alarm thresholds**
 - Alarm on crossing **safety limits**
- Scenario-driven intra-service coordination
 - Controller scenarios should enforce coordination of services participating in the **CIS interaction**
 - Implementation by a Coordination and Sync Center (**CSC**), a unit of the **HSI module**
- Conditional activity depends on scenarios only
 - Consistency requirement implies **scenario fine tuning**
- Proactive troubleshooting
 - **AI assisted**
- Situation **preview**
 - **AI assisted** decision support
 - Implementation by **situational twins**



These are requirements about
the way to get a better model



Generic Operational Rules

Static view

- Unit/service states are dominated by scenarios
- Scenario-driven situation coordination

Dynamic view

- Controller-dominated activity

Availability of critical features

- Tackling Loss Of Control (LOC) incidents

Preventing Oops activity


- Protecting risky features from erroneous activation

Decision support

- Controller preview of the effect of risky service

Situation awareness

- Statistical Process Control (SPC) of continuous variables



This is a list of generic operational rules defining normal, coordinated situations and activity



Meta rules (rules about rules)

Consistency of state setting


If Reaction(Condition C1) is R
And Reaction(Condition C2) is reverting R
And Scenario (C1) = Scenario (C2)
Then define new Scenario as Scenario (C1) and Scenario (C2)

Completeness of scenario definition

If Reaction is defined for a particular scenario Then it should be defined for all other scenarios.

Deterministic use cases

Avoid conflicting / competing commands
Avoid interlock
If a use case affects a service variable
Then the service should be embedded in the controller



These are requirements about rules that
apply to verification of scenario-related rules.



Secondary rules

Preparing for the unexpected

- The operational requirements may specify risk indicators, such as unit temperature, to detect unexpected situations

The system should detect failure of critical recovery units

- Components of the alarm system
- Processes used in emergency or safe-mode operation



These are rules applicable to designing the operation when the system is in exceptional situations.



Design / Engineering

Standards

- In hindsight (AI assisted): Statistical Process Control (SPC)

Universal case sampling


- Accidents → near misses → exceptions

Requirements

- Scenario-based (explicit, embedded scenarios)

Evidence used for model development

- Scenario-based event tracking



These are topics that should be examined and explored in further development of this methodology.



AI opportunities

AI for affordability

- Generic model development

Coping with complexity


- Learning from well-documented incidents
- Affordable Infrastructure
- HSI design

Requirements specification

- AI for Rule-driven SE
- Scenario-based (explicit scenarios)

AI missions per incident

- Associate the investigation with the generic model ==> custom model
- Propose a fix, described in terms of the custom model



AI can help in the RCA of specific incidents, and in the development of the methodology of operation design, Murphy's MX981 case demonstrates the need to beware the semantic hallucination.



Requirements for AI-driven Modeling

Sustainability

- Accountability → Autonomous protection

Operational situation

- Normal → Incidents

Incident RCA

- Blame → Operational complexity

Investment

- Affordability - Reducing the operational complexity

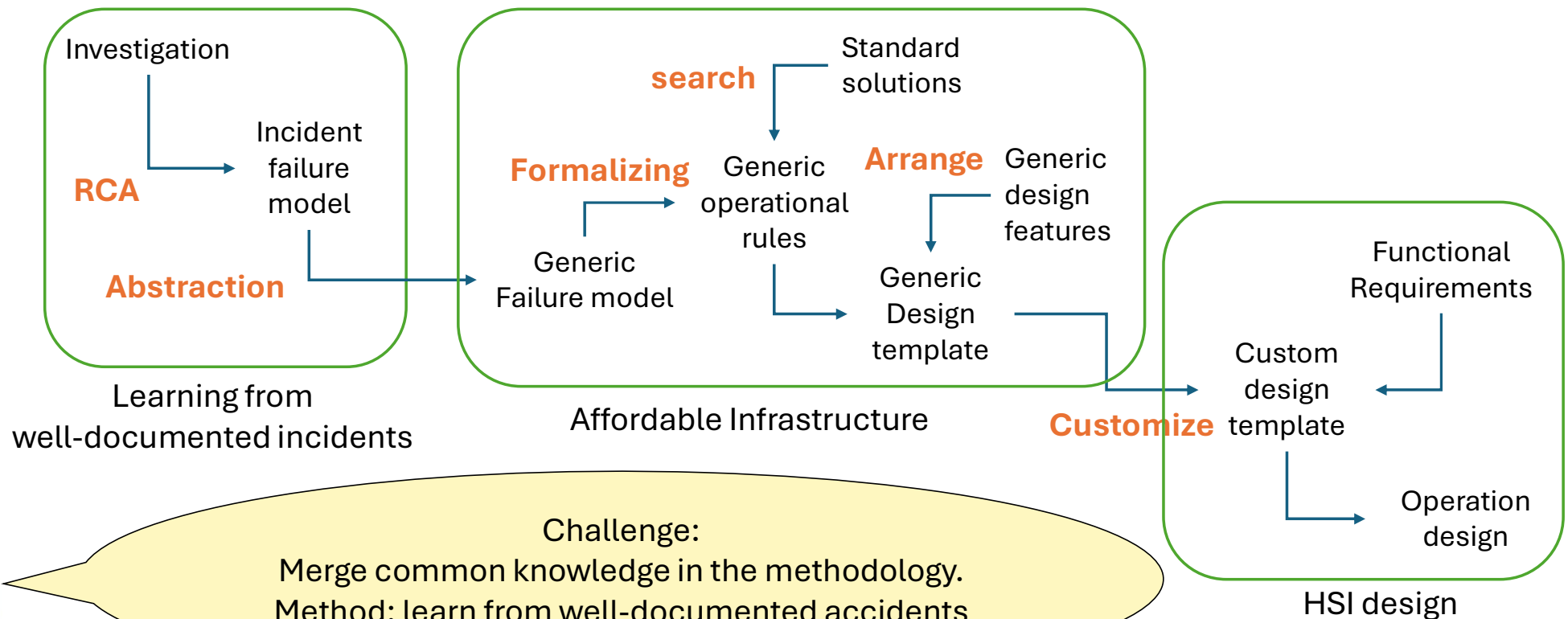


The goal is sustainability
The challenge is complexity
The objective is affordability



Crossing the complexity swamp

Infrastructure for cost-effective operation design



Challenge:
Merge common knowledge in the methodology.
Method: learn from well-documented accidents
LLM assisted activities are marked like this line



Summary

- Design goal:
 - Preventing failure
- Methods:
 - Enforcing operation by rules
 - Detecting and informing on exceptions.
- Modeling:
 - Learn from well-documented accidents
- Sampling:
 - Tracing the operation of office and everyday things
- Challenge:
 - Operational complexity
- Design principle
 - Scenario-driven coordination
- Cost-effective development
 - AI-driven model-based design



Ready for the Q&A ...



Q&A session