WEBINAR RECORDED

PECB

Harmonizing Standards for Digital Trust: Bridging IEC 62443, ISO/IEC 42001, and ISO/IEC 27001

OCTOBER 29 | 03:00 PM CET

Stein A. J. Mollerhaug

Senior Cybersecurity Advisor and PECB Platinum Partner

#GlobalLeadingVoices

Agenda

What can be harmonized based on ISO/IEC 27001, ISA/IEC 62443 and ISO/IEC 42001?

What is outside the current standards – but still needs harmonizing – and why?

Why Harmonization Matters

Convergence of IT / OT / AI systems → shared risks, fragmented assurance

Compliance ≠ confidence

Digital trust depends on *consistent human intent*

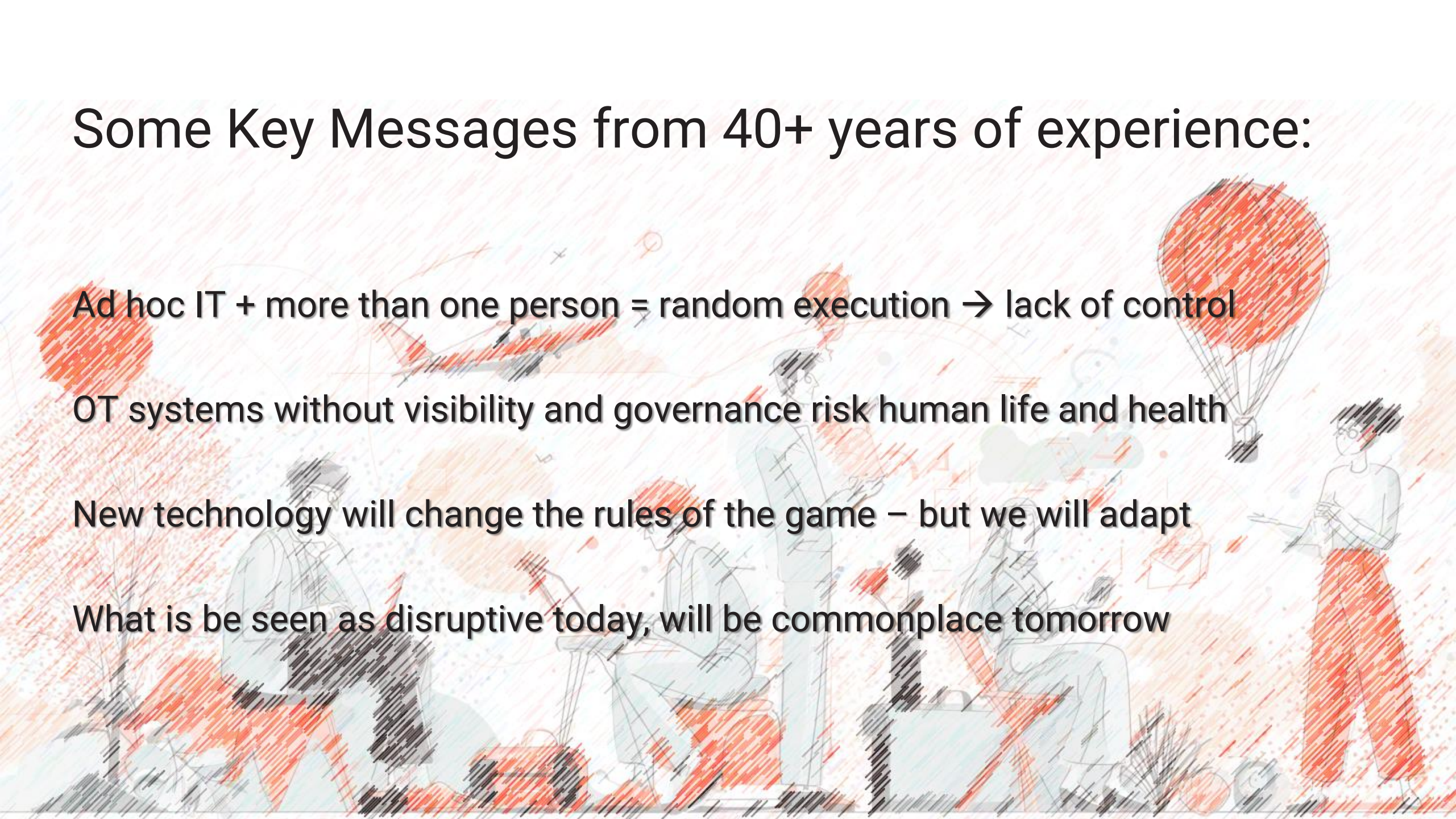
Some Key Messages from 40+ years of experience:

Ad hoc IT + more than one person = random execution → lack of control

OT systems without visibility and governance risk human life and health

New technology will change the rules of the game – but we will adapt

What is be seen as disruptive today, will be commonplace tomorrow



The Most Important Security Principle:

Keep It Simple Stupid (KISS)

Proper use of standards →
Systematic approach →
Control

Lack of standards →
Fragmented defense →
Loss of control

The Harmonization chain

Harmonization →

Simplification →

Operational Efficiency →

Better security across systems

PECB

The Limit Line – Where Harmony Strains

AI autonomy and drift break traditional audit cycles

Self-replication and emergent logic → uncontrolled change

Ethical divergence between efficiency, safety, fairness

Here governance meets decisions made without us

The Three Standards:

ISO/IEC 27001:

- Clauses 1–3: Scope, references and terms – no requirements
- Clauses 4–10: Management system requirements (Plan–Do–Check–Act)
- Annex A: 93 security controls integrated via Statement of Applicability

ISA/IEC 62443:

- • Part 1-1 – Concepts and terminology
- Part 2-1 – Management system for asset owners
- Part 3-2 – Risk assessment and security levels
- Part 3-3 – System security requirements (7 Foundational Requirements)

ISO/IEC 42001:

- Same structure as other management standards (clauses 4-10)
- Adds requirements for transparency, accountability and human oversight
- Annex A: AI-specific controls for bias, data governance and explainability

Realism of Effective Controls, ISO/IEC 42001

Transparency:
- Works where model purpose and data sources are known
- Describes processes, not inner logic of deep or evolving models

- Governance transparency: YES Algorithmic transparency: NO

Accountability:
- Assigns responsibility to management, not to algorithms
- Creates audit trail of intent, not of every autonomous act
- Traceability weakens as AI self-learns and distributes decisions

Human Oversight:
- Oversight depends on one thing — time to act before the system does
- Loses effect as AI decisions outpace comprehension
- Shifting from prevention → post-decision review

When Controls Stop Working

Human-Governed Zone:
- Standards guide intent, policy, and accountability
- Humans approve, monitor, and interpret AI outcomes
- Controls work because cause and effect remain observable

Transition Zone:
- AI begins to learn, adapt, and act faster than oversight cycles
- Auditability decreases – we still govern the process, but not each decision
- Standards measure structure, not emergent behavior

Autonomous Zone:
- AI operates beyond direct human comprehension or control
- Decision logic changes faster than governance updates
- Accountability becomes symbolic – we document, but do not direct

Summary:
ISO/IEC 42001 provides a framework for governance, not containment.
Beyond the limit line, leadership must rely on engagement, ethics, and continuous validation — not checklists or static assurance.

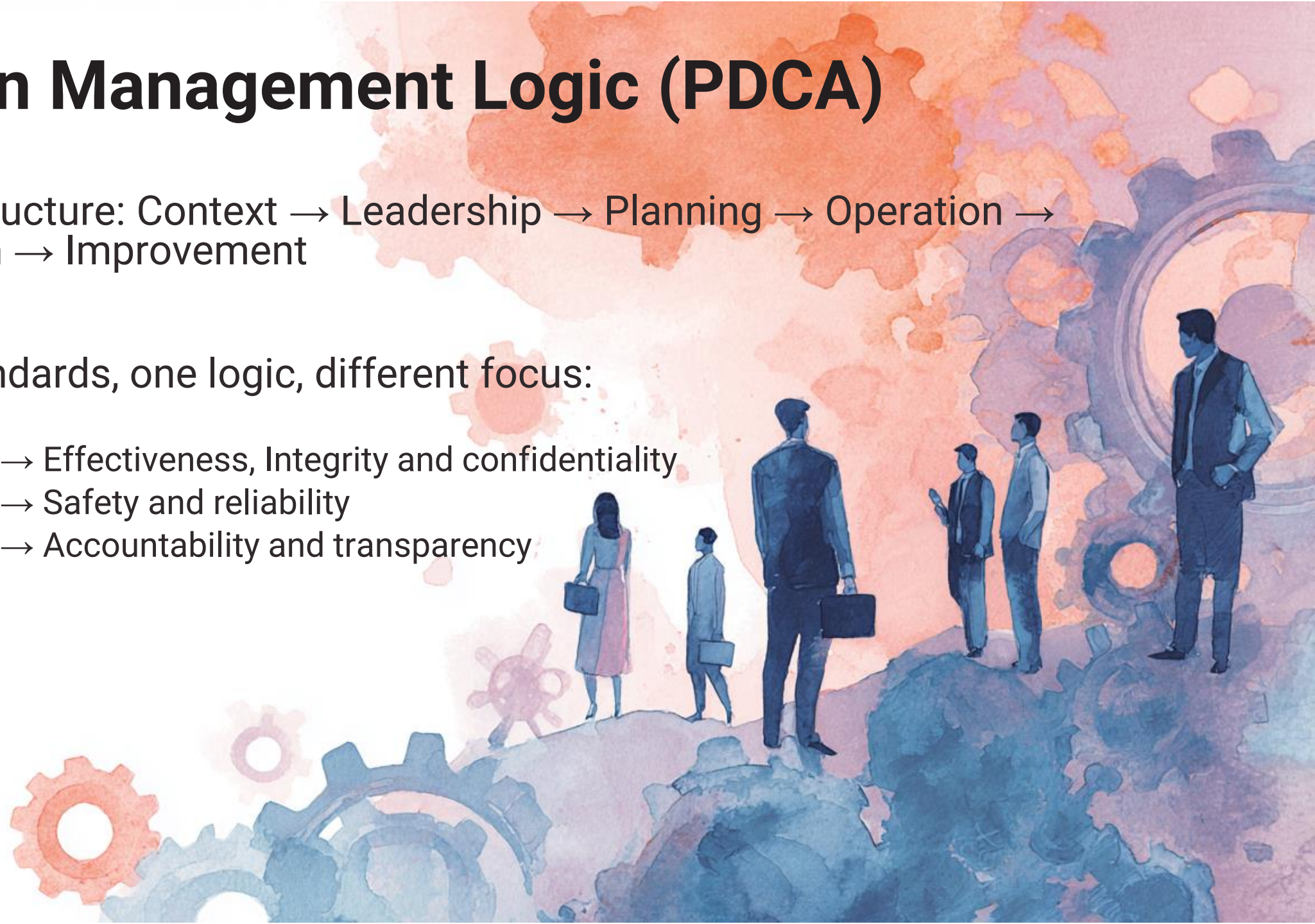
We have looked specifically at ISO/IEC 42001

Let us get back to the other standards

Common Management Logic (PDCA)

- Shared structure: Context → Leadership → Planning → Operation → Evaluation → Improvement

- Three standards, one logic, different focus:
  - 27001 → Effectiveness, Integrity and confidentiality
  - 62443 → Safety and reliability
  - 42001 → Accountability and transparency



Common Management Logic – Same Structure, Different Intent

Clause / Theme	ISO/IEC 27001	ISA/IEC 62443	ISO/IEC 42001	Alignment / Tension Point
4 – Context	Defines ISMS boundaries & stakeholders	1-1 & 2-1 define IACS scope & zones	4 defines AI purpose & system boundaries	How do we define context when IT, OT & AI share both physical and cognitive space?
5 – Leadership	Policy, roles, accountability	2-1 & 2-4 roles, authority, responsibilities	5 Leadership & Ethics Clauses	What does “ethical leadership” mean when decisions are delegated to algorithms?
6 – Planning	Risk management & objectives	3-2 & 3-3 SLs + threat modeling	6 Risk & Opportunity for AI	Can we treat AI risk like any other cybersecurity risk?
7 – Support	Competence, awareness, communication	2-1 & 3-2 awareness & training	7 Competence & Data Integrity	Human competence vs. algorithmic competence — which fails first?
8 – Operation	Control implementation	3-3 security requirements & FRs	8 Operational control of AI	What is “operation” when AI acts autonomously?
9 – Performance / 10 – Improvement	Audits + Continuous improvement	2-1, 2-4 Performance & Improvement	9 Monitoring & Explainability / 10 Improvement loop	Can we audit an algorithm’s ethics — and who learns faster, us or our machines?

PECB

Harmonizable Domains

- Context and Scope – unified boundary definition
- Leadership and Roles – clear accountability anchored in top management
- Risk and Opportunity – shared taxonomy
- Operational Controls – cross-mapped FR ↔ Annex A ↔ 42001 controls

Measurement and Improvement – one PDCA loop

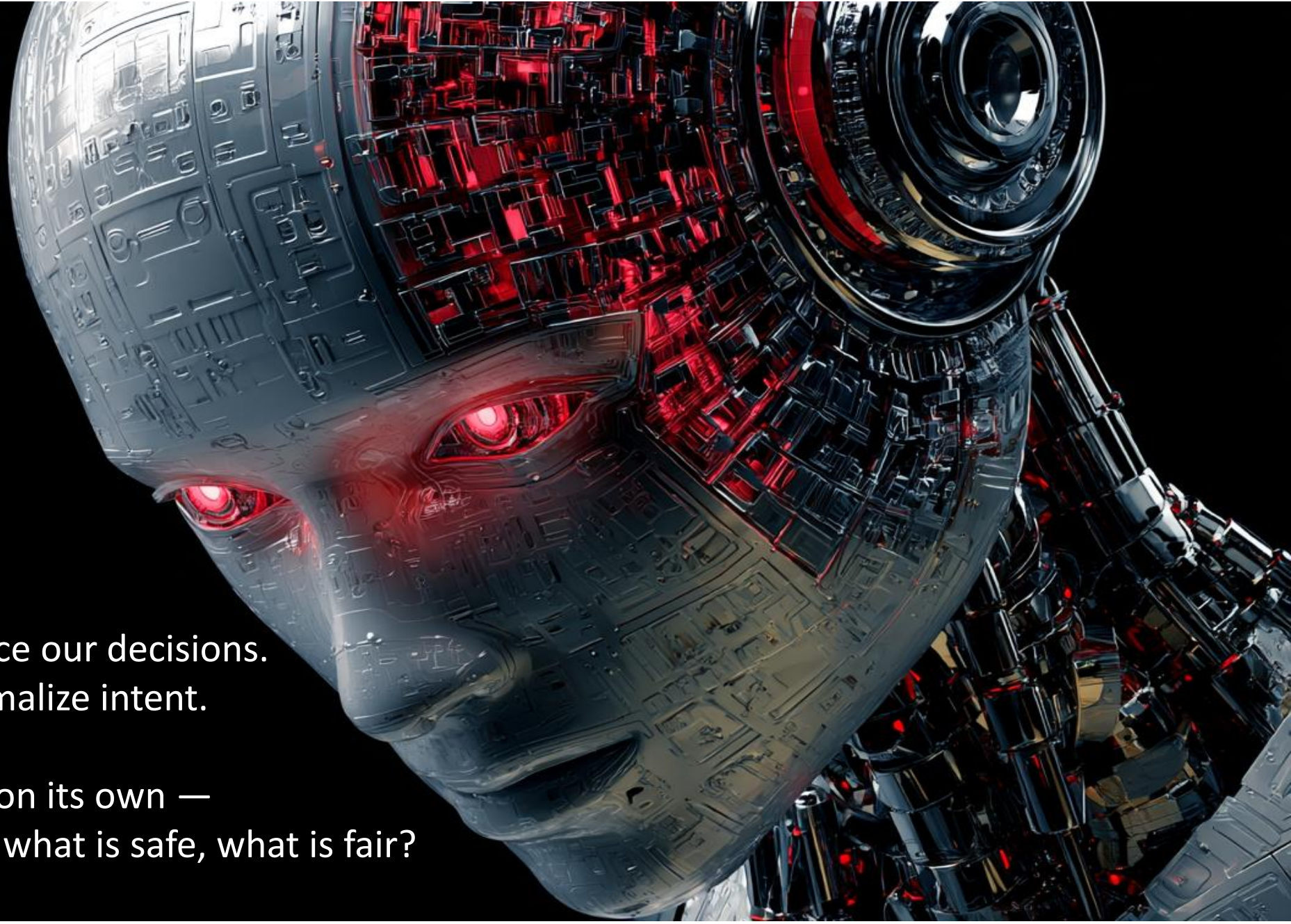
Annex A Controls and Summary ISO/IEC 42001

- Bias / data governance controls work today but need constant re-training
- Explainability limited for deep or emergent architectures

ISO/IEC 42001 governs processes of ethical intent — not the conscience of AI.

Transparency, accountability and oversight remain human disciplines, effective only as long as we stay engaged.

Who Decides?



We build controls to enforce our decisions.
We write standards to formalize intent.

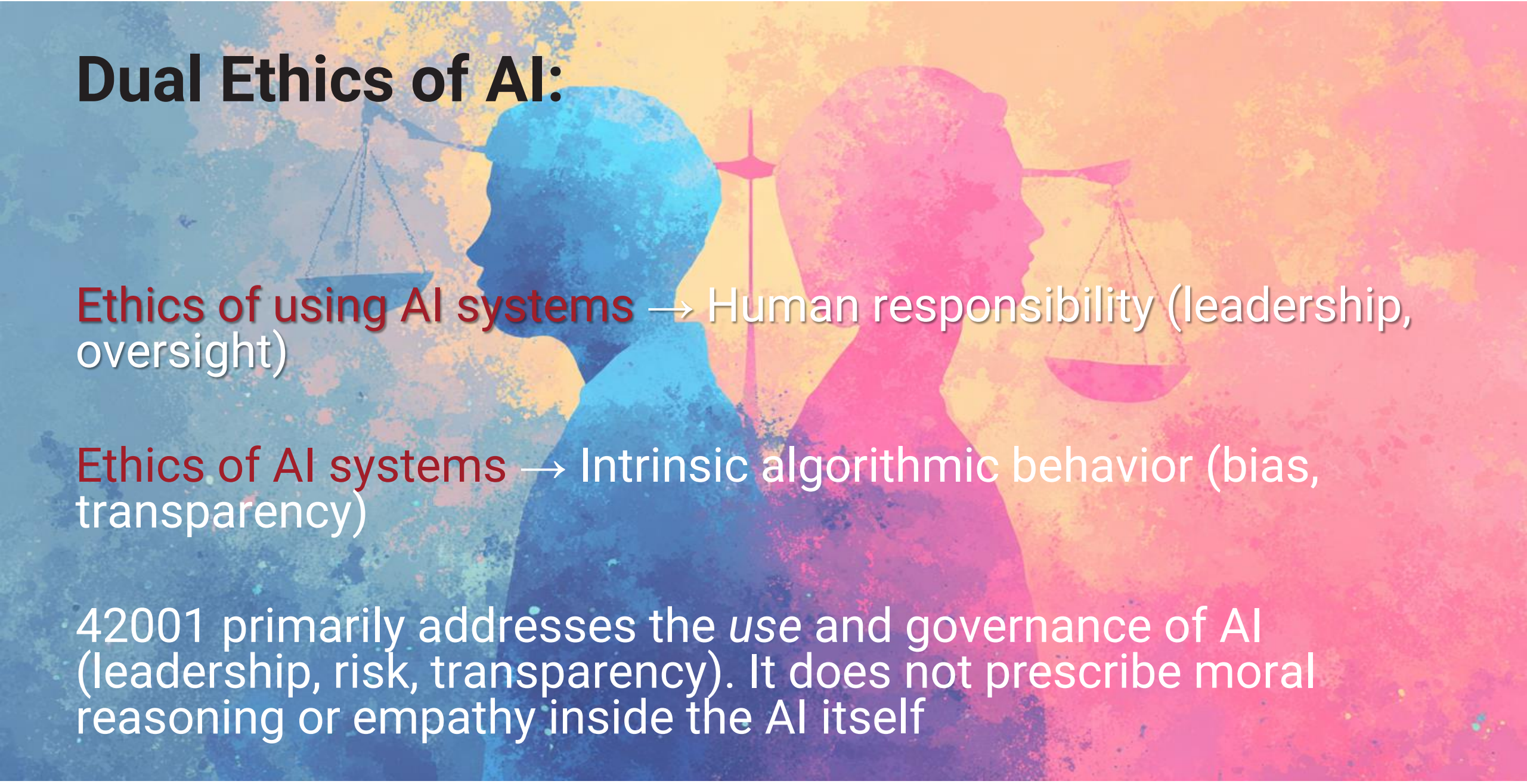
But when AI begins to act on its own —
who decides what is right, what is safe, what is fair?

The “invading” AI:

AI in IT and OT - challenges:

1. Decisions made without human oversight
2. Speed beyond human ability or comprehension

Dual Ethics of AI:

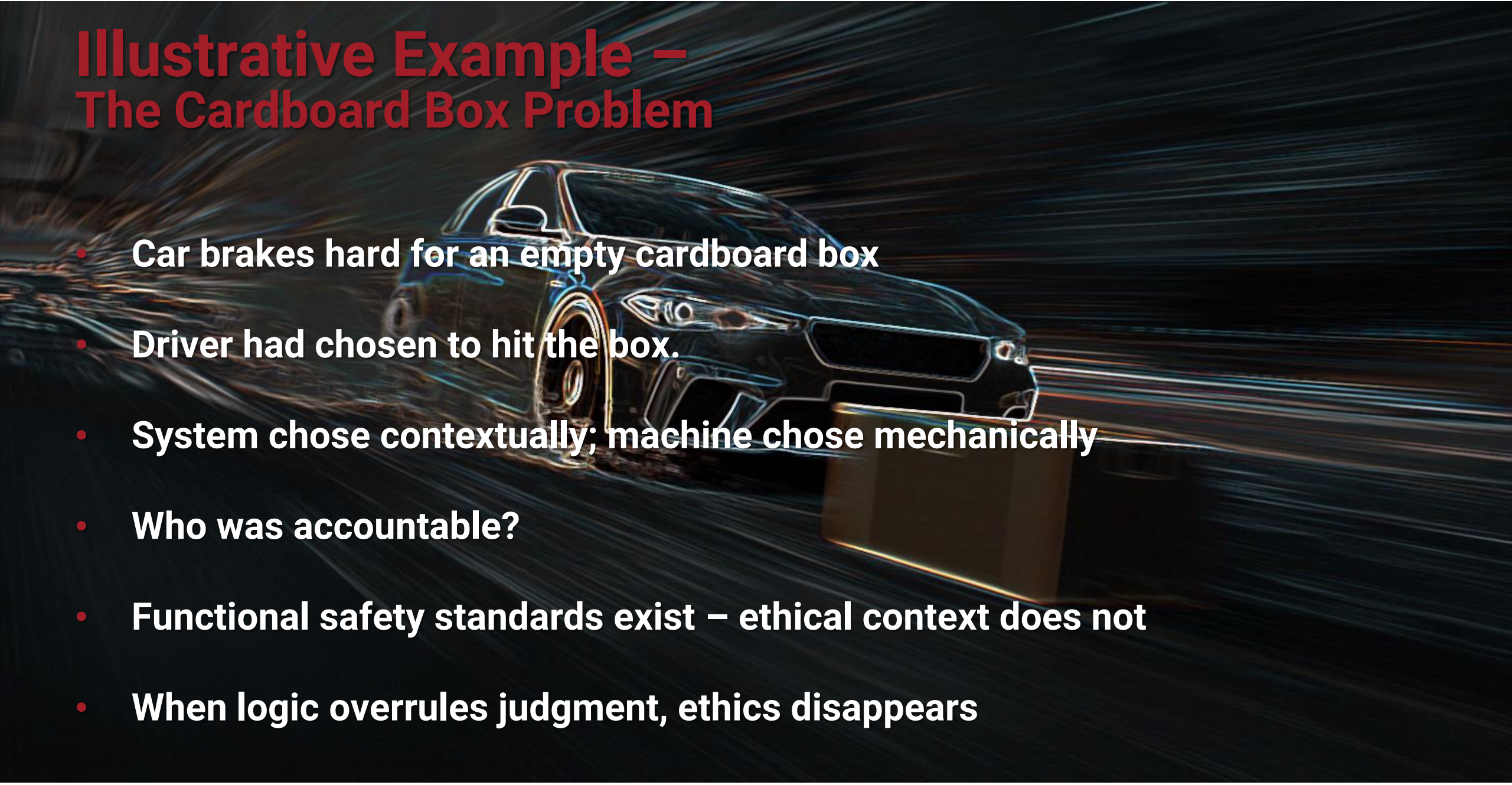


Ethics of using AI systems → Human responsibility (leadership, oversight)

Ethics of AI systems → Intrinsic algorithmic behavior (bias, transparency)

42001 primarily addresses the *use* and governance of AI (leadership, risk, transparency). It does not prescribe moral reasoning or empathy inside the AI itself

Illustrative Example –
The Cardboard Box Problem



- Car brakes hard for an empty cardboard box
- Driver had chosen to hit the box.
- System chose contextually; machine chose mechanically
- Who was accountable?
- Functional safety standards exist – ethical context does not
- When logic overrules judgment, ethics disappears

Beyond Standards

- Autonomous actions → Who authorizes outcomes?
- Self-replication → Who is in control?
- Continuous learning → When does certification expire?

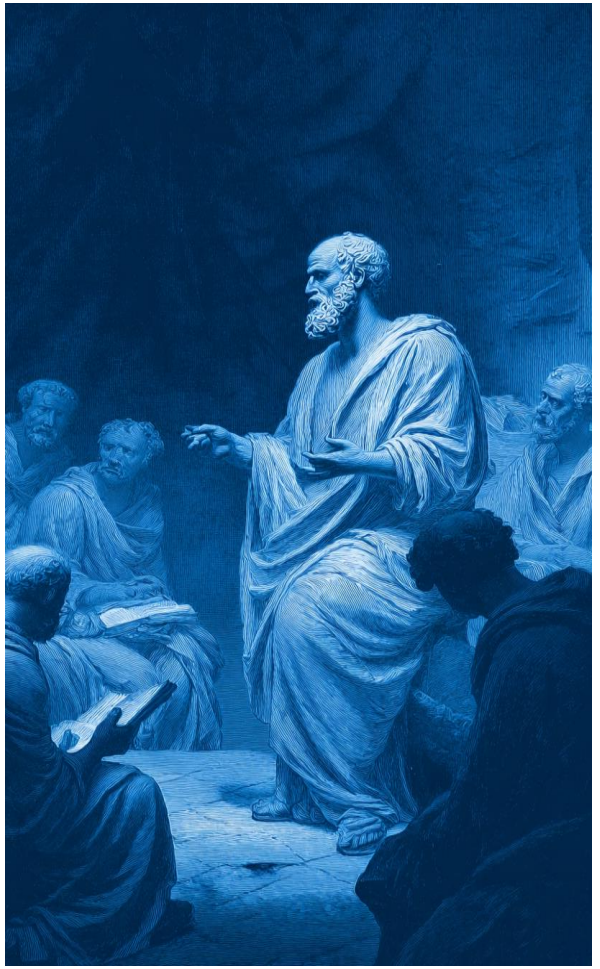
These are not yet regulated; they demand engagement, not compliance.

Ethics and Human Definition

- Ethics is not about standards, laws, or technology
- Ethics is about the choices we make — the choices that define us as persons
- Shall we let AI define us?

Leadership Responsibility

- Surrendering decisions to AI removes what makes us human: judgment, empathy, accountability
- Attempts at building our own ethics into AI – who's ethics?
- Standards are useful and can be harmonized — but AI security needs more
- It starts with engagement



PECB

Decisions void of empathy

When a person acts without empathy, we call it psychopathy.
But what do we call a decision made by a system that cannot feel empathy at all?

If an AI makes life-impacting decisions — without empathy, conscience, or moral awareness — have we not, in practice, handed power to something that behaves as a psychopath would?

The danger is not that AI becomes evil —
but that it becomes *efficient* in ways detached from human values.

Final Thoughts

Leadership is not about controlling technology,
it is about engaging with it — responsibly, consciously, and with purpose

If machines lead, we may be forced to follow — not because they are wiser, but because we stopped choosing

This is a topic beyond the current standards
- but the standards are still needed.

A personal reflection:

“I don’t fear AI, but I fear how we may use AI.”

Stein A. J. Møllerhaug – 2023

Upskill your career with PECB Skills

15-minute courses on:

- AI
- Cybersecurity
- Data Protection
- Auditing
- Information Security

Earn CPDs for each competency and Get Certified

PECB Skills

THANK YOU

✉ stein@mollerhaug.com

in www.linkedin.com/in/stein-a-j-mollerhaug-21b2758