Seminar: Complying with the EU AI ACT

The "Complying with the EU AI ACT: What is needed for Products and Systems?" seminar was held at the DoubleTree by Hilton in Brussels, Belgium, on 9th October 2025 and hosted by Mike Parsons and Davy Pissoort. This seminar covered the EU AI ACT itself and discussed the implications for organisations and engineers working with AI technology.

This event was the SCSC's second seminar to be held on mainland Europe after the highly successful seminar (Safe Autonomous Transport - the Good, the Bad and the Ugly scsc.uk/e1134) that was held the previous year in Munich. This time the seminar was held in Brussels, Belgium with local support provided by Prof. Davy Pissoort who helped arrange speakers for the event.

As with the previous trip, all the audio/video equipment needed to be brought by train from the UK so the UK organising team met at St Pancreas for another Eurostar trip. The team were also joined by Karin Rudolph who was one of the speakers based in the UK.

The hotel was only a short train journey from the main Brussels Midi terminal and proved to be an excellent venue for the seminar.

The room was spacious and the coffee break snacks and lunch were excellent and catered for all dietary requirements.

The hotel had an Art Deco feel while retaining the Belgian heritage with waffles and other local savoury treats available at breakfast.

Mike Parsons opened the seminar describing the challenges of AI and Large Language Models (LLMs) and how these technologies are presenting challenges to system safety. Davy Pissoort, a professor at KU Leuven university, then took over to introduce the speakers. He said they have several projects working on AI safety, and that standardisation in AI is a significant concern for many companies. There were six talks in total:

- **Jelle Hoedemaekers**, Agoria - The AI Act: A stress test for standardisation
- **Jan De Bruyne,** Professor IT law at KU Leuven and Head of the Centre for IT & IP Law - The Regulation of Artificial Intelligence under the AI Act and Liability – Challenges and Ways Forward
- **Karin Rudolph**, AI Ethics and Governance consultant and Founder Collective Intelligence - Who's Accountable? Ethics and Liability in the New AI Regulatory Landscape
- **Thor Myklebust and Dorthea Mathilde Kristin Vatn**, SINTEF Digital - The AI Act and The Agile Safety Plan
- **Isabella Ferrari**, Professor at Università degli Studi di Modena e Reggio Emilia - The Protection of Intellectual Property in the Training of Artificial Intelligence: Balance and possible Implications
- **Mathias Verbeke,** Faculty of Engineering Technology, Flanders Make@KU Leuven - From Standards to Practice: Bridging the Technological Gaps in EU AI Act Compliance Towards Safer AI Systems

Jelle Hoedemaekers

Jelle Hudemaekers presented the first talk of the day on AI standardization related to the EU AI Act. He explained the importance of standards as "unsung heroes" of our technological lives, giving examples such as the standard for container dimensions which dramatically improved global trade and safety.

He differentiated between de facto industry standards and formal standards developed by Standards Development Organizations (SDOs) like ISO, IEC, CEN, and CENELEC.

He explained the New Legislative Framework (NLF) used in Europe, where high-level requirements are in legislation while technical specifications are in standards. The AI Act follows this approach.

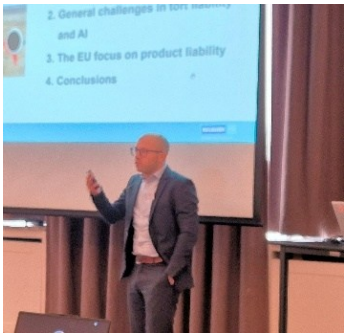
For high-risk AI systems, implementing harmonised standards will provide "presumption of conformity" with the AI Act, making market access easier.

He described the standardization process and outlined the key challenges in AI standardisation:

- Applying a physical product framework to digital products
- Issues with standards accessibility (Malamut case)
- More mandatory requirements in European standards than international ones
- Tight timelines with August 2026 compliance deadline
- Lack of clarity on which standards companies need to implement
- Criticism about standardization process transparency

He emphasised the need for more experts to actively participate in standards development rather than being critical of the work "from the sidelines".

Jan De Bruyne



Jan de Bruyne was next up and gave a presentation on the EU AI Act and related liability issues. He first introduced the AI Act which was adopted in 2024 and builds upon previous ethical guidelines for trustworthy AI.

He said the AI Act is part of a broader regulatory landscape that includes ethics, technology, and market mechanisms. Some provisions became applicable in February 2025, but most will apply from August 2026 with Type 1 high-risk AI systems have until August 2027 to comply.

The Act has a risk-based approach covering:

- Prohibited AI systems (e.g., social scoring systems)
- High-risk AI systems (allowed but with strict requirements)
- Systems requiring transparency (e.g., chatbots, deepfakes)
- Minimal risk systems (not heavily regulated)
- General-purpose AI models (with separate requirements)

For high-risk AI systems he said there were two categories of AI system making a distinction between those that are:

- Safety components of products requiring third-party conformity assessment
- Used in specific sectors for specific purposes

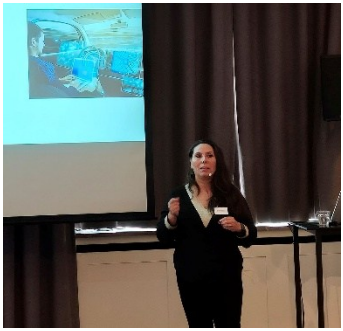
Requirements in the act include risk management, data governance, technical documentation, transparency and human oversight. Importantly, it was noted that there is a reversal of the burden of proof from the victim having to prove defective operation to the manufacturer having to prove correct operation.

Jan concluded with some liability issues:

- Distinction between contractual and extra-contractual liability
- Revised Product Liability Directive now includes software as a "product"
- Focus on "legitimate safety expectations" as a standard
- Challenges with burden of proof for victims of AI harm

Jan emphasized that while the AI Act sets high-level requirements, standards (as discussed by Jelle) will be crucial to make these requirements concrete and implementable for companies.

Karin Rudolph



After a coffee break we heard from Karin Rudoplh from Collective Intelligence.

Karin's presentation focused on accountability, ethics, and liability in AI systems. She began by discussing the complexity of determining responsibility when AI causes harm, using examples like autonomous vehicle accidents and misleading AI chatbots.

She said that the new Product Liability Directive, now includes software and digital products, making it challenging to prove causation between AI defects and harm. She covered ethical frameworks that could be applied to AI:

- Utilitarianism (consequence-based ethics)
- Deontology (rule-based ethics using principles like human rights)
- Virtue ethics (focusing on developing good character)

She then gave examples of ethical approaches in AI:

- The "Utilitarian Self-Driving Car" dilemma (People accept it is better for the vehicle to sacrifice the vehicle occupant rather than kill 20 pedestrians unless they are the occupant themselves!)
- Claude's constitution based on human rights principles to build ethical and transparent AI systems

Karin went on to discuss the aspects such as:

- The concept of moral agency in AI systems and whether machines should make moral decisions
- The EU Code of Practice for general-purpose AI models, focusing on risk mitigation throughout the AI lifecycle
- The challenge of systemic risk assessment with AI that has emerging capabilities that cannot be fully predicted
- The shift from narrow AI governance to dealing with more complex general-purpose AI and AI agents
- Future considerations including the debate around AI personhood and the changing relationship between humans and AI

Karin concluded by highlighting implementation challenges, the need for agility in regulation, the changing role of engineers, and the importance of being curious and open-minded about these rapidly evolving technologies.

Thor Myklebust and Dorthea Mathilde Kristin Vatn

After lunch, the next talk had two speakers with Thor first covering AI Safety Case considerations and then Dorthea covering Human Factor aspects of AI systems.

Thor started the presentation by introducing the book he had published called "AI Act and The Agile Safety Plan", which provides guidance on how to produce Safety Plan for an agile project. It covers all the relevant topics and issues, discussing compliance in high-risk systems development and establishes a connection to the safety cases to help produce these efficiently.

Thor went on to discuss some of the projects his company has been involved in especially in helping clients gain a foothold in the marketplace. He said the development of safety plans and safety cases for AI components is in its infancy and changes are expected to the AI Act as it is open to different interpretations by stakeholders. The remainder of his talk focussed on the challenges of producing a Safety Plan such as definitions of the system, managing software including the AI lifecycle, data, biases and issues with AI training material and outliers, compliance, proliferation of unqualified tools, documentation, procurement and sub-contractors.

Dorthea presented on the human factor's perspective of safe AI development and use.

She started by saying that the human factors perspective emphasises that knowledge of how the human brain processes information should guide technology design, especially in safety-critical domains. She highlighted examples of technology failures, including car accidents with automated features where drivers blamed their vehicles, demonstrating the importance of considering human limitations in design.

She then introduced the concept of situational awareness, developed by Mika Ensley in the 1990s, which is crucial for operators who serve as the ultimate fallback mechanism when automated systems fail. She discussed Article 14 of the AI Act regarding human oversight, which requires humans to maintain ultimate control and decision-making power over AI systems in safety-critical contexts.

She said that explainable AI (XAI) is not a fixed characteristic but a capability that needs continuous development, as machine learning systems and user needs are constantly changing.

From her PhD research with a Norwegian renewable energy company, she found that developing XAI capabilities requires not only technical resources but also organisational structures, expertise, and processes for collaboration and mutual learning.

She concluded with key takeaways:

- the importance of human factors expertise
- early user focus in development
- consideration of human factors in safety-critical contexts
- the need for organisations to invest in tools, people and processes to develop XAI capabilities.

Mathias Verbeke

Matthias's presentation focused on the technological gaps in AI safety and the role of standards in addressing them. AI integration in mechatronic systems offers opportunities but creates new safety challenges. He noted the AI Safety Paradox: as AI systems become more capable, they become both harder to assure for safety but it is more important that this is done.

He said that traditional safety methods struggle with AI's non-deterministic behaviour. For example, it is difficult to incorporate all possible scenarios into model training and models degrade over time due to data drift.

While standards like those from the CENELEC Joint Technical Committee 21 (JTC 21) provide good coverage of the AI Act requirements, they lack harmony and technical depth. They explain the "what" and "why" but are vague on the "how."

He said work is in progress to develop a more coherent structure of standards to address interrelationship gaps and provide clearer mapping to standardization requirements.

There still remain technical implementation gaps with three key areas that need to be addressed:

- Safety specification (defining system purpose and associated risks)
- Uncertainty quantification (measuring model output uncertainty)
- Model monitoring (tracking performance over time and addressing degradation)

He said there are however, promising developments: Standards like ISO/IEC 5469 provide useful guidance on incorporating AI in safety-critical systems, but more detailed technical specifications are needed.

Matthias concluded by saying that he and his colleagues are actively researching formal safety specification methods, robust uncertainty quantification, and runtime safety monitoring to help bridge the gap between current standards and practical implementation.

Isabella Ferrari

Our final talk of the day was given by Isabella Ferrari who presented remotely. Isabella focused on legal issues in AI training, particularly copyright, intellectual property protection, and privacy. She explained how AI training relies on datasets that can be protected by copyright, with data falling into four categories:

- open domain
- requiring authorisation
- illegally scraped
- corporate confidential data

She discussed different types of licenses like MIT and GPL, which have varying requirements for attribution and redistribution. She then highlighted several legal cases; the first was Dr. Steven Taylor's experiments with trying to get AI systems recognised as inventors/creators (which were rejected due to AI lacking personhood).

Secondly, she covered in detail the ongoing New York Times lawsuit against OpenAI and Microsoft for using copyrighted articles for training ChatGPT without permission. This case centres on whether AI training constitutes "transformative use" under the "fair use" doctrine.

For privacy concerns, Isabella emphasised the importance of data anonymisation techniques in different sectors. In healthcare, pseudonymisation preserves useful information while removing personal identifiers. For automotive applications, she suggested using synthetic data from video games to avoid privacy issues with real-world imagery.

Mike Parsons – Discussion

Mike Parsons then hosted a general discussion. The first observation was that, in the aviation industry, there's currently no recognised way to certify AI systems for safety-critical applications since existing standards don't account for AI's non-deterministic nature.

There was consensus that clarity on AI regulation and standards might take several years, with estimates ranging from 3-4 years.

Karin highlighted the unprecedented complexity of AI systems, especially as they begin to interact with each other, creating new dimensions of challenges.

Jelle raised concerns about the pace of standards development compared to technological advancement, questioning whether standards can keep up with both AI development and the need for legislation.

There was acknowledgment that standards typically take about 10 years to develop while legal systems take even longer, creating a significant gap between technology and governance.

The overall sentiment was one of uncertainty about the future of AI regulation, with recognition that many questions remain unanswered despite the day's discussions.

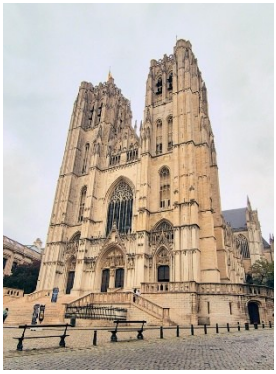
Brussels Bustle!

The evening presented an opportunity to visit the centre of Brussels and experience its vibrant night life and many colourful and intriguing shops – not least its rubber duck shop! There were also a few shops with no prices of the handbags and watches being offered for sale in the window – as the saying goes, "if you need to ask the price, you probably can't afford it!"

There was also ample opportunity to shop for Belgian's other great export – chocolate! The central Grand-Place plaza we visited was particularly bustling as a local university was holding its graduation ceremony in the square. The square itself was delightful especially in early evening when all the lights of the buildings, restaurants and food stalls gave a warm and enticing ambiance to the scene.

After taking in the marvels of the gothic façade of the Town Hall and other building dating back to the 14th century, we found a restaurant where we enjoyed a 11 samples of Belgian beer, mostly of which were over 8% alcohol!

With a few free hours before our train back to the UK the next day, we returned to the centre briefly the following morning to see the 1000-year old St. Michael & St. Gudula Cathedral with its amazingly intricate pulpit.



Report by Paul Hampton, SCSC Newsletter Editor