



18<sup>th</sup> International

## FRAMily Meeting & Workshop 2026

📍 Technical University of Munich, Germany | 📅 15 – 17 June 2026

# FROM LATENT CONDITIONS TO EMERGENT HAZARDS: A FRAM-Based Integration of TARA and HARA for CAV Systems



Iryna Bernyk



Dr Tingting Li and Dr Yulia Cherdantseva



Cardiff University, Wales, UK



bernyki@cardiff.ac.uk





## Iryna Bernyk

PhD Researcher

School of Computer Science and Informatics

Cardiff University

bernyki@cardiff.ac.uk



### Academic Background

- BSc in Computer Science with Cybersecurity and Digital Forensics specialisation
- BSc focus: cybersecurity of IoT devices, with emphasis on penetration testing
- MSc in Cybersecurity
- MSc research: Enhancing the Resilience of Healthcare Environment Against Cyberattacks
- Teaching on the MSc programme, including the module "Business Continuity and Digital Transformation"



### Current Research

- PhD research on cybersecurity for Connected Autonomous Vehicles (CAVs)
- Focus on how cyber threats can influence safety-critical vehicle behaviour
- Integration of safety and cybersecurity analysis
- Interest in functional variability, resilience, and emergent hazards



LinkedIn

Scan to connect and follow my research updates.

- 1 → How many of you **drive**, or regularly **travel by car**?
- 2 → Have you ever considered how many **safety-critical tasks** are involved in getting from point A to point B?
- 3 → When driving, would you agree that we are constantly **perceiving, interpreting, anticipating, deciding**, and **adapting** — often without consciously noticing it?
- 4 → Would you feel comfortable allowing a machine to **take full control** of those tasks?
- 5 → Would you feel equally comfortable if that machine could potentially be **influenced remotely**?

Fiction often imagines remote vehicle takeover.  
But the concern is not purely fictional.

**The Jeep Cherokee hack was a cold shower for the industry.**



### Fictional portrayals

Popular culture remote takeover



### Real-world demonstration

Jeep Cherokee hack

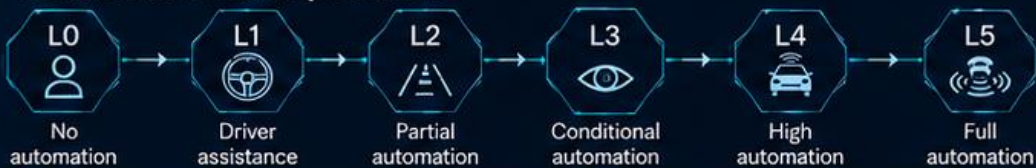


## Why automate driving?

The automotive industry's pursuit of highly automated vehicles is commonly justified by empirical road safety data that consistently identify human factors as a dominant contributor to road collisions. Delegating vehicle platform control from a Human Driver (HD) to an Automated Driving System (ADS) is positioned as a promising response to this persistent safety concern.

**Long-term vision:** as automation capabilities mature, the HD's role is progressively relegated to that of a passive passenger.

## How is this seen in practice?



HD in control → Shared responsibility → ADS in control

✓ Higher levels of driving automation, particularly Levels 4 and 5, are widely believed to have significant potential to improve road safety.

✓ At Levels 4 and 5, the ADS is expected to achieve a minimal-risk condition and bring the vehicle to a safe stop or safe place when required.

## Connectivity also increases



As automation increases, vehicles also become more **connected, data-dependent** and **software-reliant**.



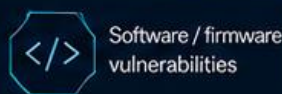
Cyber intrusion and remote attacks



Loss or degradation of connectivity



Data manipulation and spoofing



Software / firmware vulnerabilities



Privacy, trust and behavioural adaptation



Highly automated and connected vehicles are best understood as **cyber-physical-social systems of systems**.

## A Safety-I narrative: three tensions



### 1. Paradox

Official road safety metrics attempt to understand operational safety mainly through unsafe events, while neglecting the countless successful bountlen Interventions that occur every day.



### 2. Irony

In seeking to optimise safety by removing human error, the industry may also remove human flexibility — the mechanism that often prevents minor anomalies from escalating into accidents.



The **Automated Vehicles Act 2024** requires authorised self-driving vehicles to achieve a level of safety equivalent to, or higher than, that of a careful and competent human driver.



### 3. Comparative vacuum

While human-driver collisions are extensively tracked, comparable transparent public datasets on ADS-caused failures remain limited. Without equivalent data, claims of superior ADS safety remain statistically unproven.

The transition to highly automated and connected vehicles is not just a technological shift — it is a fundamental shift in the nature of safety.

**New capabilities bring new vulnerabilities, new interactions, and new forms of risk.**



# Research Problem & Gap



## HARA — HAZARD ANALYSIS AND RISK ASSESSMENT

ISO 26262: Functional Safety

### Primary focus:

Hazardous behaviour arising from malfunctioning electrical/electronic systems.

### Typical analytical logic:

- 1 Item definition
- 2 Identify hazards and operational situations
- 3 Form hazardous events
- 4 Assess Severity, Exposure and Controllability
- 5 Assign ASIL or QM
- 6 Derive safety goals



**HARA asks:** “What can become hazardous if the item malfunctions?”

### What it does well:

- ✔ Structures functional-safety risk.
- ✔ Links hazardous events to safety goals.
- ✔ Supports development assurance through ASIL classification.

### Boundary / limitations:

- Centred mainly on malfunctioning behaviour.
- Cyberattack origin, attacker intention and attack feasibility are not its primary concern.
- Interaction-driven hazards without a clear malfunction may be difficult to represent.

## THE ANALYTICAL ABYSS



The missing piece is not only “What is the threat?” or “What is the hazard?” It is:  
**How does the threat alter system functioning until a hazard emerges?”**



## THE COMPLETENESS PROBLEM

Can every operational situation be enumerated?

Can every attack path or vulnerability be identified?

Can completeness ever be demonstrated in an architecture that continues to evolve?

For CAVs, this becomes increasingly difficult because:



Functions are distributed across sensors, actuators, ECUs, networks, cloud services and infrastructure.



Multiple attack entry points exist across damage dependencies.



The number of operational and environment combinations grows rapidly.



Interactions can create unanticipated behaviour when individual components seem safe.



## TARA — THREAT ANALYSIS AND RISK ASSESSMENT

ISO/SAE 21434: Cybersecurity Engineering

### Primary focus:

Cybersecurity risks to vehicle assets and system properties.

### Typical analytical logic:

- 1 Item definition
- 2 Identify assets
- 3 Identify threat scenarios
- 4 Assess damage
- 5 Analyse attack paths
- 6 Assess attack feasibility
- 7 Determine cybersecurity risk
- 8 Select risk-treatment decision
- 9 Derive cybersecurity goals



**TARA asks:** “What can an attacker compromise, how, and with what impact?”

### What it does well:

- ✔ Identifies assets, threats and attack paths.
- ✔ Considers attacker capability and feasibility.
- ✔ Supports cybersecurity goals and treatment decisions.

### Boundary / limitations:

- Safety consequences are commonly represented as damage or impact categories.
- It does not inherently model how disturbed functions interact over time.
- Propagation from compromised asset to emergent vehicle behaviour can remain implicit.



## RESEARCH GAP

HARA identifies safety-relevant hazardous events.  
TARA identifies cybersecurity threat scenarios.



Neither, on its own, systematically explains how cyber-induced functional variability propagates through interdependent CAV functions and contributes to emergent physical hazards.

TARA  
Cyber threat



MISSING ANALYTICAL BRIDGE  
Variability • Interaction • Resonance



HARA  
Safety hazard

We need an analytical bridge that captures interdependencies, variability and interactions across the full cyber-physical system to understand how cyber events become safety hazards.

# MERLIN: Modelling the Journey Between Cyber Threats & Physical Safety Hazards



## MERLIN: Modelling and Evaluating Risks in Latent and Nonlinear Interactions among Interdependent Systems



To address these limitations, we are developing MERLIN, a **resilience-oriented, FRAM-inspired** framework intended to incorporate TARA and HARA into a unified functional model.

The aim is to analyse how **cybersecurity threats, hazardous operational situations, latent conditions, environmental influences, and adaptive performance adjustments** interact across interdependent CAV functions under dynamic operational conditions.

### MERLIN Objectives



**Integrate** TARA and HARA within a unified functional representation.



**Trace** how cybersecurity threats affect safety-critical functions.



**Capture** latent interdependencies and nonlinear interactions.



**Analyse** the propagation, amplification and damping of functional variability.



**Represent** environmental influences and adaptive performance adjustments.

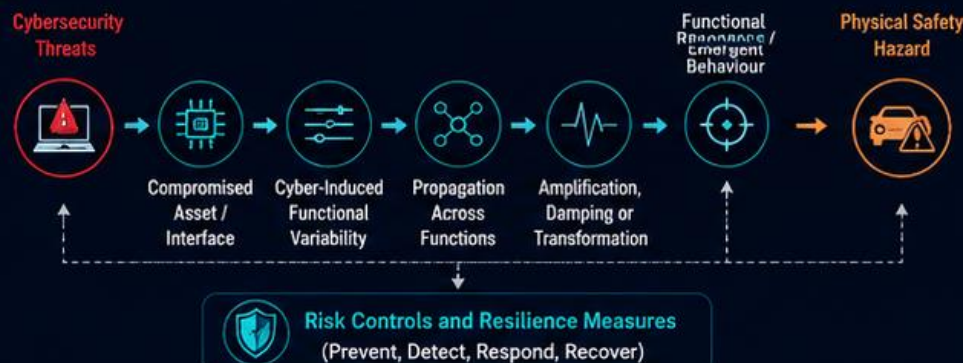


**Identify emergent** hazards and functional resonance.



**Support resilience-oriented** risk controls and safety-security decision-making.

### MERLIN Analyses the Journey



### MERLIN is Built on the Foundation of Existing Research

Patriarca et al.  
(2017)



FRAM with Abstraction/ Agency structure across agents and abstraction levels.

**Gap:** Conceptual and domain-general; does not address cybersecurity or cyber-to-safety pathway.

Grabbe et al.  
(2020)



Safety-II perspective and FRAM as a proactive method for road-system interactions.

**Gap:** Focused on safety; explicitly excluded security.

Grabbe et al.  
(2022)



FRAM applied to overtaking scenario; agent and space-time structuring for variability propagation.

**Gap:** Nominal/non-adversarial performance; did not connect cyber threats, attack paths or security risk.

Li et al.  
(2024)



Integrated ISO 26262 and ISO/SAE 21434 via enhanced STPA for safety-security co-analysis and unified risk assessment.

**Gap:** Limited in representing everyday functional variability, nonlinear resonance and functional emergence.

Deng et al.  
(2024/2025)



FRAM + Bayesian Networks to identify functional resonance chains and quantify risk in AEB system.

**Gap:** Focused on safety quantification in a bounded subsystem; cybersecurity threats, HARA-TARA integration and socio-technical interactions not main concern.

### Existing Research Highlights Key Advances but Leaves a Critical Gap



FRAM can reveal functional interactions, variability and emergence.



Multi-dimensional structuring can improve knowledge representation.



Safety and security need to be considered together.



Quantification and standards alignment can strengthen risk assessment.



**No reviewed approach simultaneously connected cyber threats to functional variability, traced their propagation across agents, stages and abstraction levels, and linked the resulting emergent behaviour to automotive safety risk.**



These insights define the requirements and objectives of MERLIN.



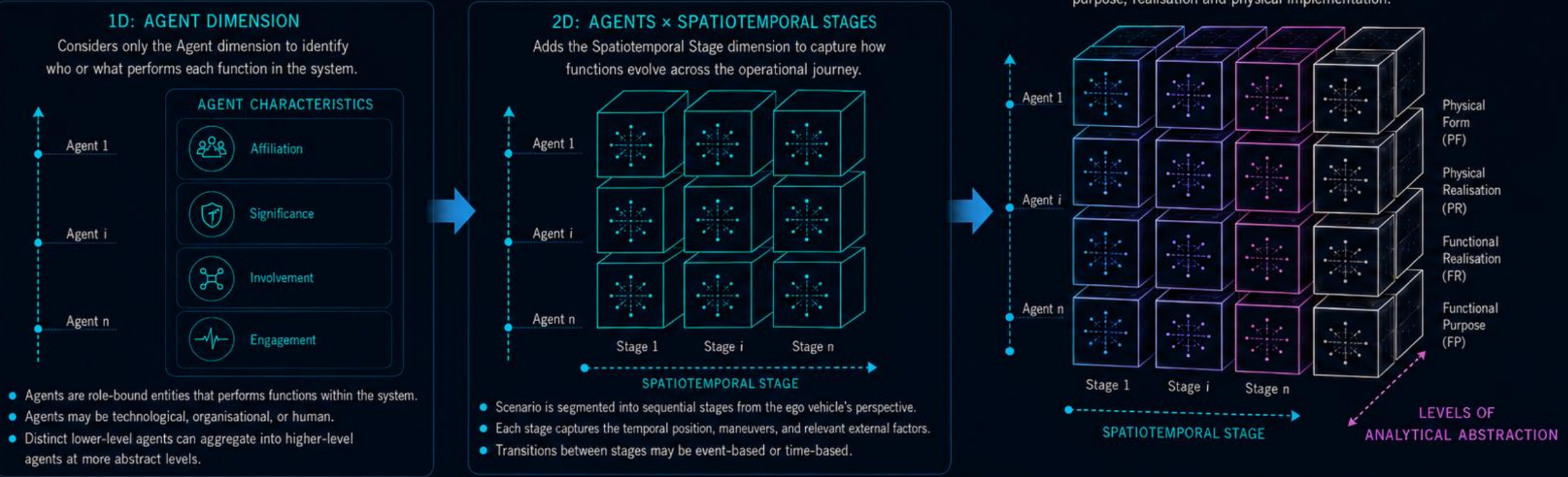
MERLIN examines not only individual threats or hazards, but how risk emerges through **interactions across the wider CAV system.**



# MERLIN: Modelling the Journey Between Cyber Threats & Physical Safety Hazards

## The 3D-FRAS: Building the Analytical Space

The 3D Functional Risk Analysis Space (3D-FRAS) defines the analytical space within which MERLIN analyses how cyber threats propagate through functions performed by different agents across spatiotemporal stages and abstraction levels, potentially leading to physical safety hazards.



The 3D-FRAS enables MERLIN to analyse how interactions among agents, across **spatiotemporal stages** and **abstraction levels**, contribute to variability, propagation, functional resonances and emergent hazards.



# MERLIN Modelling & Risk Assessment Steps

The detailed steps for each part of the MERLIN modelling and risk assessment framework are currently **under development**.



**Part 1:**  
System Definition &  
Operational Context

STATUS  
UNDER DEVELOPMENT



**Part 2:**  
Identification & Description  
of System Functions

STATUS  
UNDER DEVELOPMENT



**Part 3:**  
Variability Aggregation,  
Functional Resonance &  
Unified Risk Assessment

STATUS  
UNDER DEVELOPMENT



**Part 4:**  
Variability &  
Risk Management

STATUS  
UNDER DEVELOPMENT



We are building a rigorous, traceable and context-sensitive framework to support **safe, secure and resilient** automated driving systems.



# Application of MERLIN



**MERLIN** extends the baseline FRAM model by treating cybersecurity compromise as a source of functional variability and tracing how its effects may propagate, combine and resonate across the wider system.

## Baseline model and analytical purpose

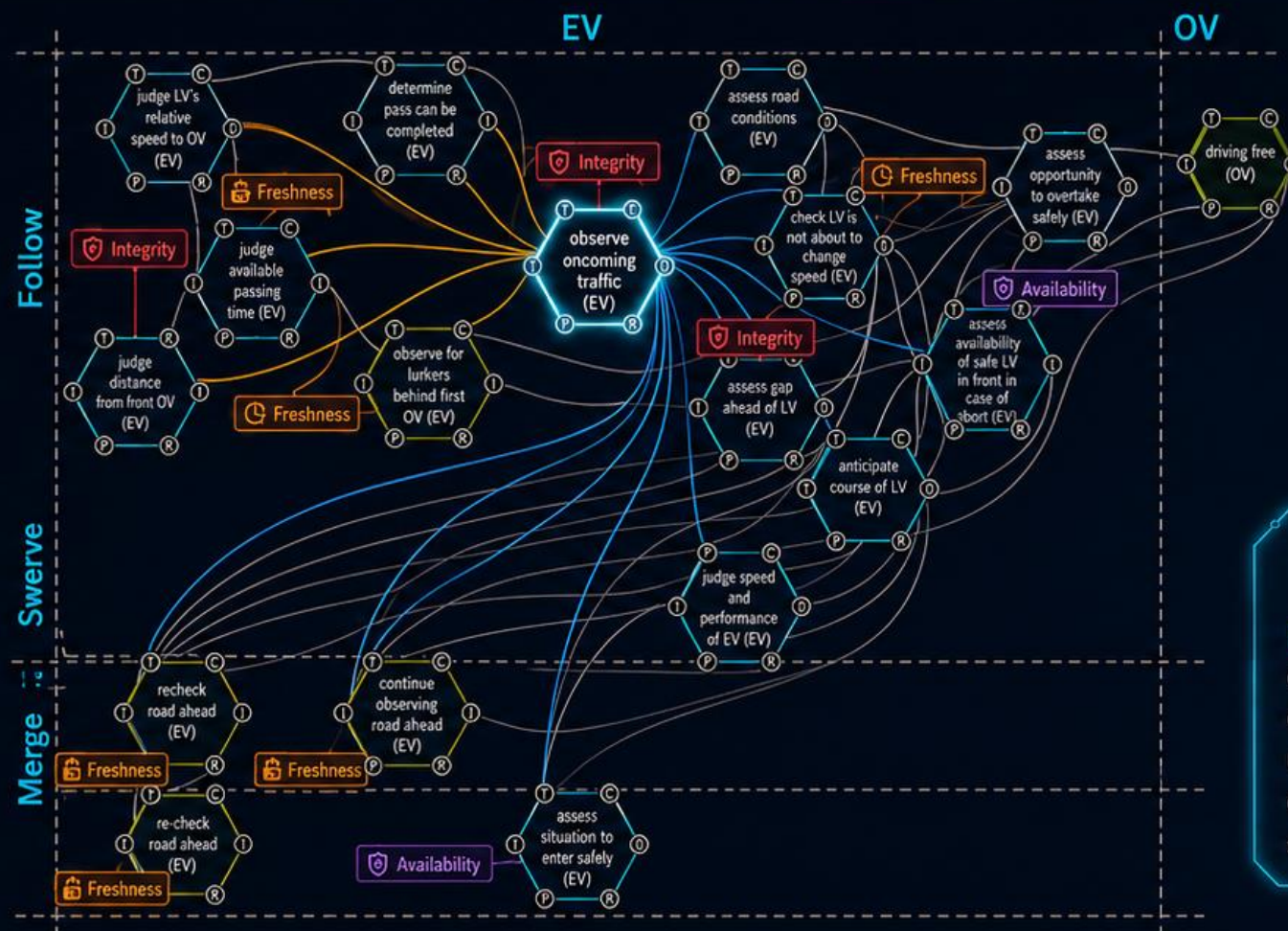
- Adapted from Grabbe et al. (2022), Figure 14.
- Scenario: SAE Level 4 ego vehicle overtaking on a rural road.
- Original focus: <observe oncoming traffic (EV)>.
- MERLIN application objective: examine how cyber-induced compromise may introduce or modify functional variability along this critical path.



## Motivating accident pattern

Degraded perception, unstable object interpretation, and inhibited safety response can combine into a fatal outcome.

The Uber crash is used only as an analogue; it is not reproduced directly. Its failure pattern is translated into a hypothetical cyber-induced overtaking instantiation.



## Illustrative cyber-induced variability

- Integrity** — manipulated or misleading perception data.
- Freshness** — delayed or replayed information.
- Availability** — safety function unavailable or suppressed.
- Authenticity** — spoofed or false status / signals.



## Potential outcome pathway:

compromised perception and delayed/suppressed response -> unsafe overtaking or failed collision avoidance -> physical safety hazard.



### 1. Road safety motivation is real — but automation changes the nature of risk.

Higher levels of driving automation aim to reduce human-error-related harm, yet they also increase software dependence, connectivity, and system complexity.



### 2. Current assessment practice remains fragmented.

HARA focuses on safety hazards, while TARA focuses on cybersecurity threats; neither alone adequately explains how cyber compromise can propagate into physical safety harm in CAVs.



### 3. MERLIN addresses the missing link.

MERLIN is being developed as a resilience-oriented, FRAM-inspired framework to analyse the journey from cyber threat → functional variability → unsafe system behaviour → physical safety hazard.



### 4. The 3D-FRAS provides the analytical space.

MERLIN traces interactions across agents, spatiotemporal stages, and levels of analytical abstraction to reveal interdependencies, variability propagation, amplification, damping, and emergent hazards.



### 5. This is work in progress — and expert feedback matters.

The modelling and risk assessment steps are under development, and feedback from the FRAMily community is highly valued to strengthen the framework and its application.



**Core message: Cybersecurity compromise in highly automated vehicles should be understood not as an isolated technical fault, but as a potential source of system-wide functional variability and emergent safety risk.**

# Thank You for Listening!



## Welcome Questions and Discussion

Your insights and feedback are invaluable as this research develops.

Connect • Collaborate • Improve



### Contact Me



Let's stay connected!

Scan to view my LinkedIn profile and get in touch.

✉ [bernyk@cardiff.ac.uk](mailto:bernyk@cardiff.ac.uk)  
🏠 Cardiff University, Wales, UK  
🌐 [linkedin.com/in/iryna-bernyk](https://www.linkedin.com/in/iryna-bernyk)

