## **CONNECT** - Continuous and Efficient Cooperative Trust Management for Resilient CCAM

We are heading towards a future of **connect**ed, cooperative, and automated mobility (CCAM). Fuelled by advances in automated driving and communication technologies like 5G cellular vehicle-to-everything (C-V2X), these developments will enhance the contemporary automated/autonomous driving functionalities and facilitate the next generation of cooperative autonomous driving applications (e.g., intersection movement assist, fleet management systems, cooperative routing, and parking services) and will extend the vision of Cooperative Intelligent Transport Systems (C-ITS) which was investigated and developed since the early 2000s to improve road safety, traffic efficiency, and sustainability.

With the increased connectivity and cooperation among different heterogeneous systems that are produced by different manufacturers, operate in highly dynamic, changing, and uncertain environments, and provide safety-critical services, the notion of trust is becoming a major concern and critical property of these systems [1]. The multiparty nature of these systems do not only include the vehicles themselves but also infrastructure technologies like Multi-access Edge Computing (MEC) and the cloud backends. Failures or attacks on one part of the system will have consequences throughout the overall System-of-Systems (SoS).

**CONNECT's main mission** is to enable a dynamic and continuous assessment of trust in a CCAM system and to investigate mechanisms that provide increased trust assurances compared to today's systems. By this, the abstract notion of trust should become quantifiable, assessable, and thus practically usable to enhance the security and safety of CCAM systems.

#### **Motivational Example**

The dynamic nature and the heterogeneity of the CCAM applications, as well as the dynamic environments in which the systems operate, dictate that no initial trust between entities can be assumed. In response, we follow the Zero Trust security principle: **"Never Trust, Always Verify"**. Therefore, we need to explicitly establish sufficient level of trust into remote entities, so they trust one another to collaboratively execute safety-critical tasks. For example, if we consider a scenario from the Cooperative Intersection Management use case [2], where two vehicles drive towards an intersection, then we require a trust assessment mechanism that answers the question "How much trust can vehicle V<sub>A</sub> put into vehicle V<sub>B</sub> to cooperatively execute a specific function (e.g., safely passing the intersection)?".





#### INTERSECTION CROSSING WITHOUT COLLISION

Two vehicles drive towards an intersection, and they communicate their state information (e.g., position  $p_a$  and  $p_{b'}$  for vehicle  $V_a$  and vehicle  $V_{b'}$ respectively) to the multi-access edge computing (MEC). MEC processes the received information and sends the vehicles their time slots (t<sub>2</sub> and t<sub>b</sub>). The first **animation** shows *Intersection cross*ing without collision: V and V, give correct information about their location to the MEC, and the MEC gives them respective timeslots for crossing. The second animation shows Intersection crossing with a collision. In this scenario, V<sub>2</sub> is malicious and gives the MEC wrong information about its position. V<sub>2</sub> is much closer to the center of the intersection in reality, than what V<sub>a</sub> reports it to be. Based on the wrong information from V<sub>3</sub>, the MEC gives the priority of passing to the  $\rm V_{\rm b^\prime}$  but the vehicles end up crossing simultaneously, resulting in a collision

#### Solution: Trust Assessment!

Trust Assessment at runtime in the second

### INTERSECTION CROSSING WITH A COLLISION

scenario shall enable the MEC to assess the trust in the vehicles and also the vehicles to access the trust among each other. The trust Assessment ideally puts less trust in a malicious vehicle and the information that this vehicle shares, which prevents potential collisions.

> To summarize, we think that trust management is a key ingredient to safe and secure CCAM systems. The requirement is that this assessment of trust relationships is quantifiable, verifiable, and assessable both at design- and runtime. CONNECT therefore works towards a technical implementation of such trust assessment in a trust management framework.

Find out more about this Project: https://horizon-connect.eu



"NEVER TRUST, ALWAYS VERIFY"



## **Project Coordinator**

Technikon, Austria

## Technical Lead

Thanassis Giannetsos, Ubitech Greece

## **Scientific Lead**

**Frank Kargl,** University of Ulm Germany

Call: HORIZON-CL5-2021-D6-01

**Topic:** HORIZON-CL5-2021-D6-01-04



Budget

€ 5.7 Million 100% EU-funded



## Consortium

17 Partners 9 Countries



## Duration

**36 Months** 09/2022 - 08/2025

### Design of a Trust Management Framework

Implementing this trust management framework requires a number of challenges to be solved and solutions to be developed. Starting from a system model, we need a suitable representation of trust which allows us to model trust relationships in CCAM systems in a way that fulfils the requirements stated above. Second, we need to embed this trust model into a framework that can execute trust assessment and take decisions on whether the required trust is achieved or not.

# Reasoning under uncertainties with subjective Logic

We approach the first challenge by using a well-establish logic framework called **Subjective Logic** that allows to reason about trust while also allowing to consider uncertainty in our judgement. This uncertainty can stem from incomplete evidence about trustworthiness that would prevent us from making dogmatic judgements.

In order to reflect this uncertainty, CONNECT uses Subjective Logic for trust assessment, i.e., for reasoning, assessing and quantifying trust in CCAM. The general idea of Subjective Logic is to enrich probabilistic logic by explicitly including uncertainty about probabilities and subjective belief ownership. Subjective Logic explicitly represents the amount of 'uncertainty on the degree of truth about a proposition' in a model called subjective opinion [3]. Based on this, **Subjective Trust Networks** allow to model complex trust relationships and to assess trust from the perspective of individual actors in our system.

#### **Taking Trust Decision**

Modelling and assessing trust using Subjective Trust Networks then form the basis for trust decisions, i.e., answering the question if there is sufficient trust in a specific situation to allow safe and trustworthy operation of a CCAM system and a specific driving function.

For this, two trust values have to be determined and compared. The first is the current level of trust also referred to as **Actual Trust Level** (**ATL**). The second is the required level of trust among so that a specific function can be executed in a trustworthy manner – referred to as **Required Trust Level (RTL**). Both can reference to a data item that an entity might receive and use in a driving function, or to another entity from which it consumes a service that it relies on. Only if the computed ATL exceeds the RTL, the execution of a specific function can proceed in a trustworthy manner.

Referring again to the motivational example: When we ask "How much trust is vehicle  $V_A$  required put into vehicle  $V_B$  to provide data correctly to safely engage in a maneuver at a cooperatively managed intersection?", this determines Required Trust Level. On the contrary, if we ask "What is the actual level of trust that vehicle  $V_B$  or to vehicle  $V_B$  in general with respect to performing a joint maneuver in a cooperatively managed intersection?", then this determines the Actual Trust Level.

In CONNECT, we want to investigate, design, and develop this Trust Management Framework in order to bring Trustworthy CCAM closer to reality.

- [1] https://upstream.auto/reports/glob al-automotive-cybersecurity-report/
- [2] Ulm University, "Securing Coopera tive Intersection Management through Subjective Logic", presentation, 2022
- [3] Jøsang, Audun. "A logic for uncertain proabilities." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 9.03 (2001): 279-311.
- [4] Jøsang, Audun. Subjective logic. Vol.4. Cham: Springer, 2016

# **Partners**

	TECHNIK <b>UN</b>	0	Trialog	3	FSCOM_
	Technikon Forschungs- und Planungs- gesellschaft mbH, Austria		Trialog, France		FSCOM, France
2	UBITECH	8	DENSO Crafting the Core		STELLANTIS
	Ubitech Ltd, Greece		DENSO AUTOMOTIVE Deutschland GmbH, Germany		Centro Richerche Fiat SCPA, Italy
3	HUAWEI	9	intel.		Politecnico
	Huawei Technologies, Germany		Intel Deutschland GmbH, Germany		Politecnico di Torino, Italy
4			Suite5		System×
	Institute of Communication and Comput- er Systems, I-SENSE Research Group, Greece		Suite5 Data Intelligence Solutions Ltd, Cyprus		Institut de Recherche Tech- nologique SystemX, France
5	I ulm		uni <sub>•</sub> systems		
	University of Ulm - Institute of Distributed Systems, Germany		Unisystems, Greece		University of Surrey, Department of Computer Science, United Kingdom
6	🐣 Red Hat	12	UNIVERSITY OF TWENTE.		
	Red Hat Research, Israel		University of Twente, Department of Philosophy, Netherlands		Follow CONNECT on:
	**** Funded by the European	Union un	der grant agreement no. 101069688. Views		

and opinions expressed are however those of the author(s) only and do not

@connect\_horizon

CONNECT Horizon Europ project 101069688

Funded by recessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.