WHY THREATGET?

In February 2019, the EU launched a cyber security initiative to advance Europe in this critical area. And THREATGET, an Austrian product developed jointly by the AIT Austrian Institute of Technology and LieberLieber Software GmbH, is already available. It helps developers to identify threats early on and to quickly assess the associated risks.

LieberLieber

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

WHY THREATGET?

Our society is currently undergoing a digitalisation phase, and all sorts of everyday devices are increasingly being networked (Internet of Things, IoT). One popular example is the smart home, with manufacturers around the world offering new ways of networking our homes and connecting them with the digital world. But to date this trend has had a central flaw: the failure to consider security in the design. However, this will only become painfully aware to consumers when, for example, they suffer the consequences of unauthorised access to their network. What is currently lacking are methods, designs, and special security architectures which can reliably and securely protect digital networks from unauthorised external access.

Although a simple solution for an affected refrigerator may be to disconnect it from the home network, unauthorised access can have far more critical or even life-threatening consequences in a vehicle. Manufacturers forecast that in the context of automated driving, connected vehicles will become the norm in the future. Today's cars are already connected to the Internet for the purposes of facilitating software updates for navigation systems and trip computers, etc. Additionally, as of last year, all new vehicles registered in the EU are equipped with an emergency call system – eCall – which automatically notifies the emergency services in the event of an accident.

Increasingly, manufacturers are relying on Internet connectivity to facilitate vehicle communications in both directions. This is the only way in which updates can be applied in order to add new features, or provide help more quickly in the event of a breakdown, e.g. by permitting garages to remotely read the engine status. However, although this involves the same security risks as in the smart home example, in a vehicle the potential dangers are much more significant.

Already we are increasingly hearing about vehicle hacking, with premium cars especially impacted because of their many digital features. The AutoBild

magazine, for example, reported on a particular software loophole at BMW discovered by the German automobile club ADAC. This security gap allowed cars to be unlocked via a laptop, by redirecting the signal from the radio key. This allows potential attackers to gain access to the vehicle without the vehicle owner standing next to the car.

If this scenario had been considered during the vehicle design phase, then this vulnerability would never have arisen in the first place. By simply measuring the signal runtime it could have been quickly determined that the redirected signal giving the unlock command could not have come directly from the radio key, but instead via a third-party device. Now, assuming a thief without a key had driven away in the car, you might think it would be simple to programme a vehicle to disable itself once it was at a certain distance from the key. However, this would represent an enormous risk to road traffic safety: just consider the effect of disabling the power steering, steering lock or break booster while the vehicle is travelling on a motorway. As this would create too great a risk to other drivers on the road, the security technology and security design need to be considered and solved before the car is unlocked.

If this scenario had been considered during the vehicle design phase, then this vulnerability would never have arisen in the first place. By simply measuring the signal runtime it could have been quickly determined that the redirected signal giving the unlock command could not have come directly from the radio key, but instead via a third-party device. Now, assuming a thief without a key had driven away in the car, you might think it would be simple to programme a vehicle to disable itself once it was at a certain distance from the key. However, this would represent an enormous risk to road traffic safety: just consider the effect of disabling the power steering, steering lock or break booster while the vehicle is travelling on a motorway. As this would create too great a risk to other drivers on the road, the security technology and security design need to be considered and solved before the car is unlocked.

Conclusion: Connected cars, in particular, constitute an exceptionally security-critical infrastructure. For that reason, prior to establishing an autonomous driving system, special security architecture must already be in place to ensure safe and reliable road transport.

NEW DIRECTIVES – CYBERSECURITY AS A PREREQUISITE FOR TYPE APPROVAL

Given the high relevance of putting in place a comprehensive security concept, the question now is: Why has this not been done already? The answer is simple: because manufacturers have long been able to take a cost-benefit perspective and refer to corresponding insurance schemes. The new European Directive for a high common level of security of network and information systems (NIS Directive; https://www.cert.at/reports/report_2016_chap04/content.html) leads to a substantial change in this traditional approach.

With the introduction of the new European security guideline according to ECE level (UNECE WP29; valid in the EU and partly in Asia), in future vehicle manufacturers will be required to verify the cybersecurity of their vehicle systems before their products can obtain type approval. From now on, manufacturers must prove every three years that they have applied a certified cybersecurity management system which covers all stages ranging from vehicle engineering through to documentation.

Using the cybersecurity management system, manufacturers must

- test the cybersecurity of all vehicle types,
- identify and document potential threats,
- address security-critical problems and suggest solutions, and finally demonstrably verify that these problems have been solved.

PRODUCT LAUNCH AND TARGET GROUPS OF THREATGET

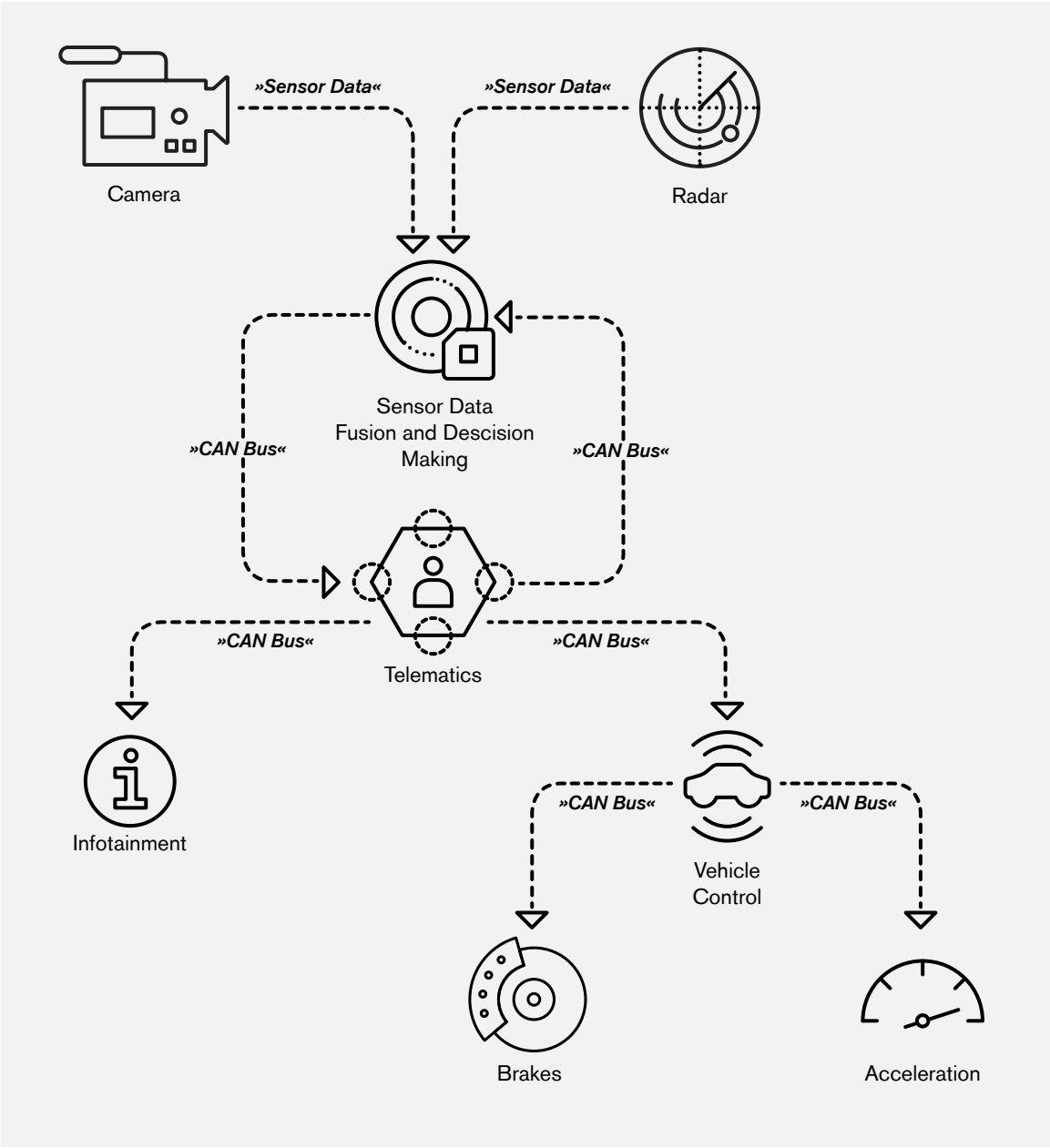
This cybersecurity verification requires a modern tool which, for the first time, allows manufacturers to test their systems for ECE compliance. With this in mind, the AIT Austrian Institute of Technology has developed a software solution for the automotive sector called THREATGET, which is based on a continuously updated catalogue of potential threats. Together with the Austrian company LieberLieber Software GmbH, THREATGET was developed into a product and was now presented to the public for the first time. This unique Austrian development closes an essential gap in the range of security solutions. Set against the background of a strongly growing security engineering industry, THREATGET is targeted at vehicle manufacturers, as well as all companies involved in analysing vehicle architectures and systems in order to issue certification (e.g. the technical inspection association TÜV), as well as those working in the automotive training sector.

ARTIFICIAL INTELLIGENCE AS A MEANS OF MANAGING COMPLEXITY

The database of potential threats and suggested solutions included in THREATGET is currently being updated and maintained as part of applied research and development activities. Users are provided with a list of potential problems and associated solutions for their specific system model (e.g. vehicle platform) which can then be implemented by a security engineer. This manually updated catalogue is complemented with updates of additional threat catalogues which, for example, are compiled by computer emergency response teams (CERT). In future, these external threat catalogues will be updated into the THREATGET catalogue automatically, using artificial intelligence (AI) algorithms. AI thus helps in managing the complexity of our increasingly networked systems. THREATGET ensures that in future the same basic security principle can be guaranteed for all manufacturers. Furthermore, manufacturers of special vehicles (e.g. for the security sector) will also be able to build on this basic principle, at the same time manually expanding specific security levels and rules in their own vehicle systems.

Image: Wolfgang Franz

Helmut Leopold (left) and Peter Lieber (right) are pleased with the market launch of their joint product THREATGET.

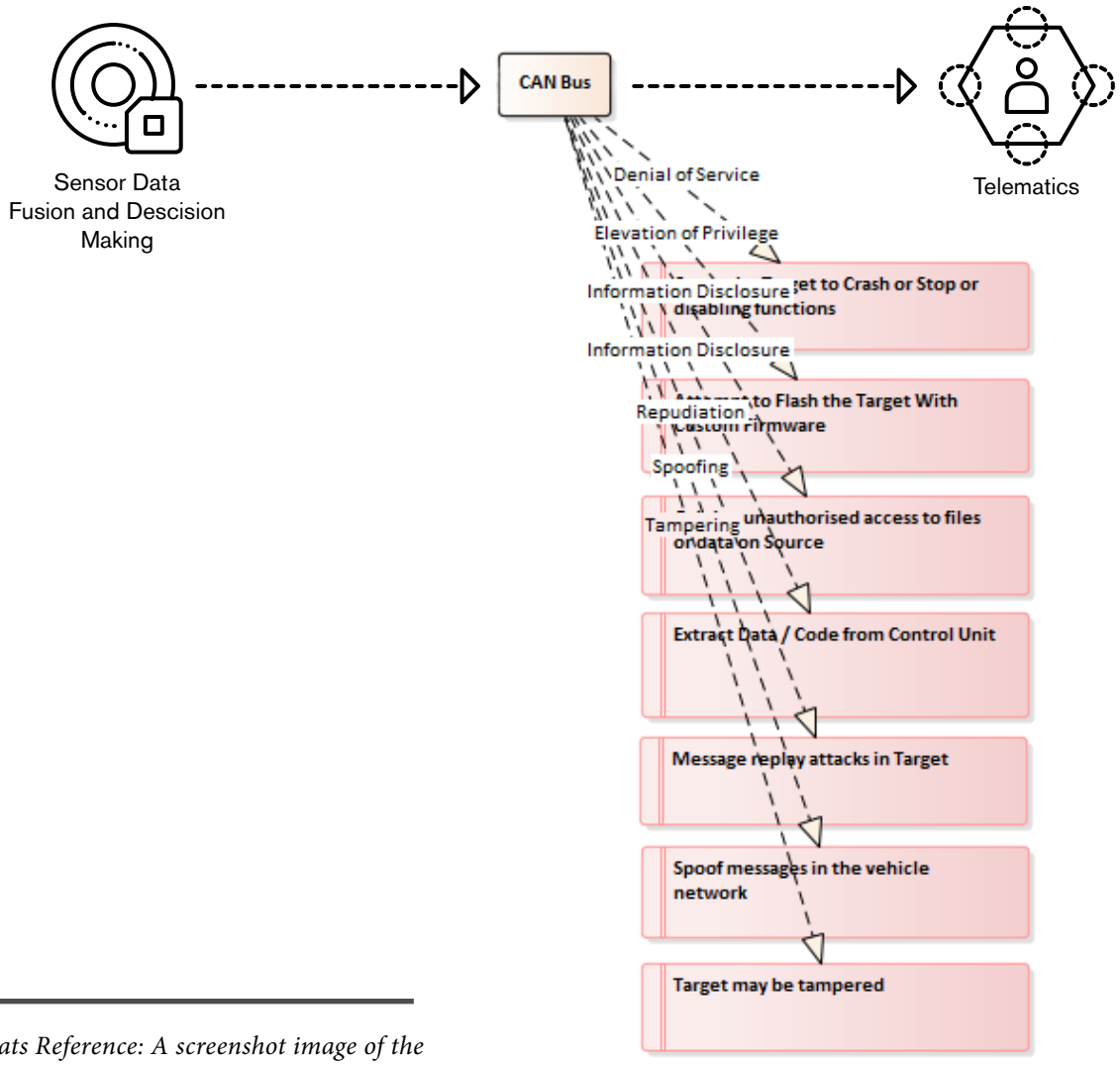


This figure shows the data flow between different internal units in a vehicle. You can see the units „Radar" and „Camera" collecting data from the external environment. These are then processed by „Sensor Data Fusion and Decision Making Methods". The data is transmitted to a telematics system that controls the tracking of the vehicle.

The Telematics interacts with the central Vehicle Control to control the speed of the vehicle either by „Brakes" or by „Acceleration". Infotainment" connects to the telematics unit to provide the driver with information.

(All graphics: AIT)

THREATS REFERENCE



Threats Reference: A screenshot image of the source of detected threats.

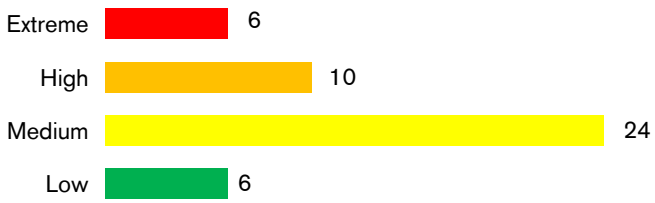
THREATS LIST

	Title	Type	Description	Impact	Likelihood
	16 Spoof me...	Spoofing	Forge or manipulate c...	Major	Likely
▶	17 Spoofing ...	Spoofing	Sensor Control Unit T...	Moder...	Possible
	18 Message ...	Repudiation	Packets or messages...	Major	Likely
	19 Gaining u...	InformationD...	Confidentiality of data...	Moder...	Possible
	20 Extract D...	InformationD...	Accessing data store...	Trivial	Remote
	21 Cause the...	DenialofSer...	DoS on Telematics C...	Critical	Certain

46 Threats Cyber Security Risk Assessment Risk Evaluation

Threats List: details of all potential threats detected

THREAT SEVERITY



Threat Severity: Evaluates the threat level detected to determine both impact and probability based on the parameters.

CYBER SECURITY RISK ASSESSMENT

		LIKELIHOOD					
		1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain	
IMPACT	1 Trivial	1	2	3	4	5	Low 1:5
	2 Minor	2	4	6	8	10	Medium 6:10
	3 Moderate	3	6	9	12	15	High 11:16
	4 Major	4	8	12	16	20	Extreme 17:25
	5 Crirtical	5	10	15	20	25	

Risk = Threat * Vulnerability * Consequence

Threat * Vulnerability = Likelihood

Consequence = Impact

THREATGET performs a risk assessment to calculate the risk level of all detected threats. These risk levels can be assigned via the THREATGET risk matrix.

CONTACT

LieberLieber
cybersecurity.lieberlieber.com

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY