



Agenda

- 1. cyber security in the automotive context: current standards & regulations
- 2. what does quantum computing add to the cyber security equation in automotive
- 3. what do we need to consider to further sustain cyber resilience in the quantum

computing era?



1. cyber security in the automotive context: current standards & regulations

4

connectivity demand from and to vehicles continously increases ...

today, we already achieve 1-2 TB data transfer rates per car every single day.

This is of value for OEMs, suppliers, fleet operators but as well for nation based actors or criminal orgniaztions and the like as a giant attack surface!



global regulation is required: high level building blocks of UNECE WP29

		compan associate	iy ed	type a asso	pproval ciated
<section-header><section-header><text></text></section-header></section-header>	UNECE R155 baseline ISO 21434	Cybersecurity Management System		Cyber Security Vehicle Requirement	
	UNECE R156 baseline ISO 24089	Software Update Management System		Software Update Vehicle Requirement	
technical services (e.g. DEKRA, TÜV SÜD, GTÜ, TÜV-Rheinland,) act as accredited type approval suppliers		issuan accepta	issuance of certificate and acceptance of type approval		Kraftfahrt- Bundesamt

> Structure of ISO/SAE 21434 Standard

	4. General considerations		
	5. Organizational cybersecurity management		
5.4.1 Cybersecurity governance	5.4.3 formation sharing 5.4.4 Systems Tool managem	ent 5.4.6 5.4.7 Information security management audit	
6	5. Project dependent cybersecurity managemen	i.	
6.4.1 Cybersecurity responsibi- lities 6.4.2 Cybersecurity planning 6.4.3 Tailoring	6.4.4 Reuse 6.4.5 Component out-of-context 6.4.6 Off-the-shelf component	6.4.76.4.86.4.9Cybersecurity caseCybersecurity assessmentRelease for post- development	
	7. Distributed cybersecurity activities		
7.4.1 Supplier capability	7.4.2 Request for quotation	7.4.3 Alignment of responsibilities	
	8. Continual cybersecurity activities		
8.3 Cybersecurity monitoring e	8.4 8.5 Cybersecurity event evaluation analysis	8.6 Vulnerability management	
Concept phase	Product development phase	Post-development phases	
9. Concept	10. Product development	12, Production	
9.3 Item definition	10.4.1 Design	13. Operations and maintenance	
9.4 Cybersecurity goals	10.4.2 Integration and verification	13.3 Cybersecurity Incident response	
9.5 Cybersecurity concept	11. Cybersecurity validation	14. End of cybersecurity support and decomissioning	
1	5. Threat analysis and risk assessment method	5	
15.3 15.4 Access Threat scenario	15.5 15.6 15.7 Impact Attack path Attack (easi	15.8 15.9 Risk value Risk treatment	

overall & project specific management processes (similar to ISO 26262) :

- Management Systems
- Policies
- Preparation for assessment

distributed CS activities

Define interfaces between customer, supplier, third parties..

continual CS activities :

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, Development and Post-Development

- Add-on of CS relevant activities during concept and development :
 - Establishment of CS goals and requirements
 - TARA and vulnerability analysis during development
- Consideration of post-development requirements (during of after production, decommissioning ...)
- Definition of post development processes (Production, Incident response,



affected: all types of automotive electronics (each OEM shapes this into proprietary domains)





- o all these listed electronic systems atop are subject to type-approval
- All electronic systems of those domains that sum up to the vehicle E/E Architecture. This architecture has to be compliant to UN-R155/UN-R156 Type Approval and must be the resulting workproduct of the respective CSMS/SUMS
- o only accredited notified bodies are entitled to certify compliance towards UNECE WP29
- o many OEMs currently are left alone due to resource limitations and lack of clear guidance



2.what does quantum computing add to the cyber security equation in automotive?



8

by 2030 about 50% of car production will be caused by electronics – the dependency on those is irreversable



automotive E/E architectures have to be adapted to sustain resilience against future attacks

active now



from todays



further relevant



... well reaching into the



potential Quantum Computing Impact

potential disruption	impact	technology gap	time to realize
Grove/Shor algorithm based encryption hacks	obsolesence of decent cryptographic methods (e.g. RSA)	dedicated software applications not yet available	to be expected withing the next 10 – 15 years
quantum communication	secure transaction within closed quantum transmission networks	lack of mobility enabled quantum devices (e.g. interfering devices, shock and vibration constraints)	not yet clear if this will ever be solvable
improved real time traffic control	increased efficiency for traffic simulation and better traffic control	dedicated applications currently at experimental level	10 – 15 years

11



3. what do we need to consider to further sustain cyber resilience in the quantum computing era?



12

an actual conclusion ...

- 1. we need to anticipate, recognize and consider, that from any potential adversary point of view, quantum computing could increase more efficient hacks for an ever growing attack surface in mobile computing platforms (incl. automotive)
- 2. along the foreseeable technology impact of quantum computing technology, we need to shape sufficient **updates** in UNECE WP29 and subsequent baselines
- 3. any mobile fleet (cars, ships, railways, aviation, etc.) need to anticipate and adapt their cyber resilience **concepts** across industries and with the help of interdisciplinary expert boards



13

DEKRA DIGITAL

Thank You!

for your time



Andy Schweiger Handwerkerstrasse 15 70565 Stuttgart

e-mail: andy.schweiger@dekra.com for your attention phone: 0160 - 6195857

14