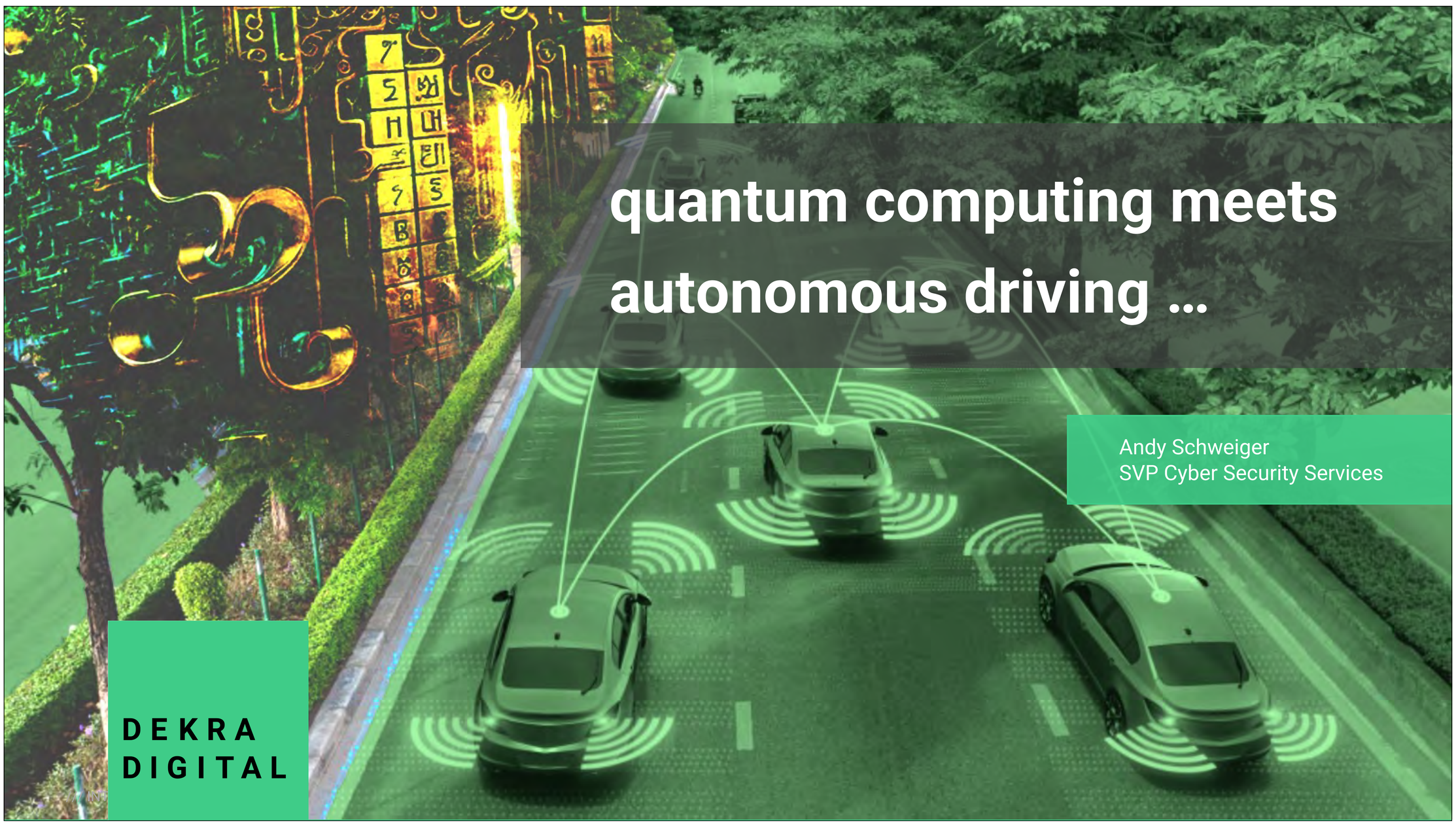


Agenda

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?

/// INTERNAL ///

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

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

		company associated	type approval associated
UNECE WP 29 regulations	**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

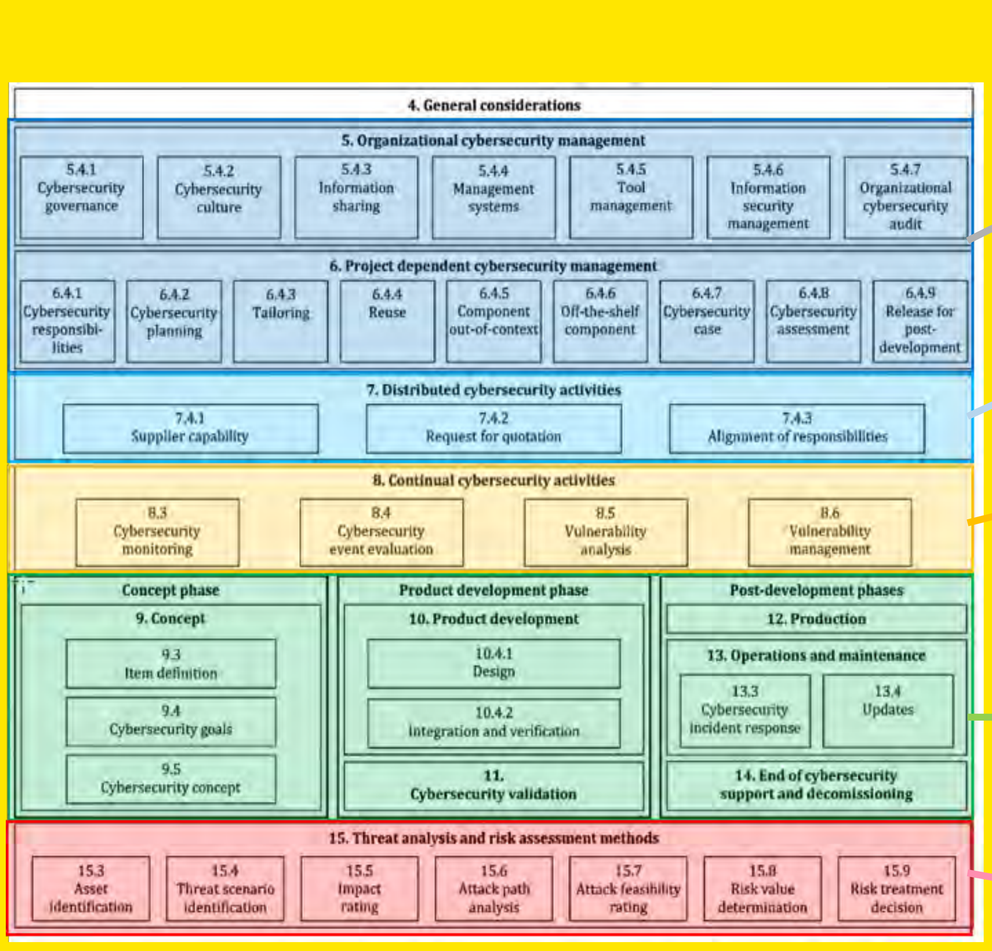
technical services
(e.g. DEKRA, TÜV SÜD, GTÜ, TÜV-Rheinland, …)
act as accredited type approval suppliers

issuance of certificate and acceptance of type approval

Kraftfahrt-Bundesamt

5

> Structure of ISO/SAE 21434 Standard



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..

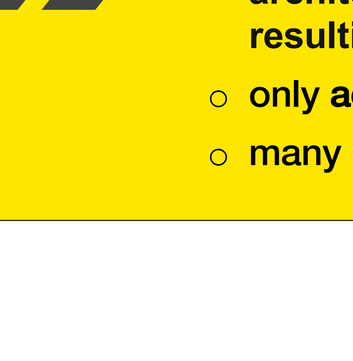
continual CS activities :
- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

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, Update)

TARA : Threat Analysis and Risk Assessment
- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

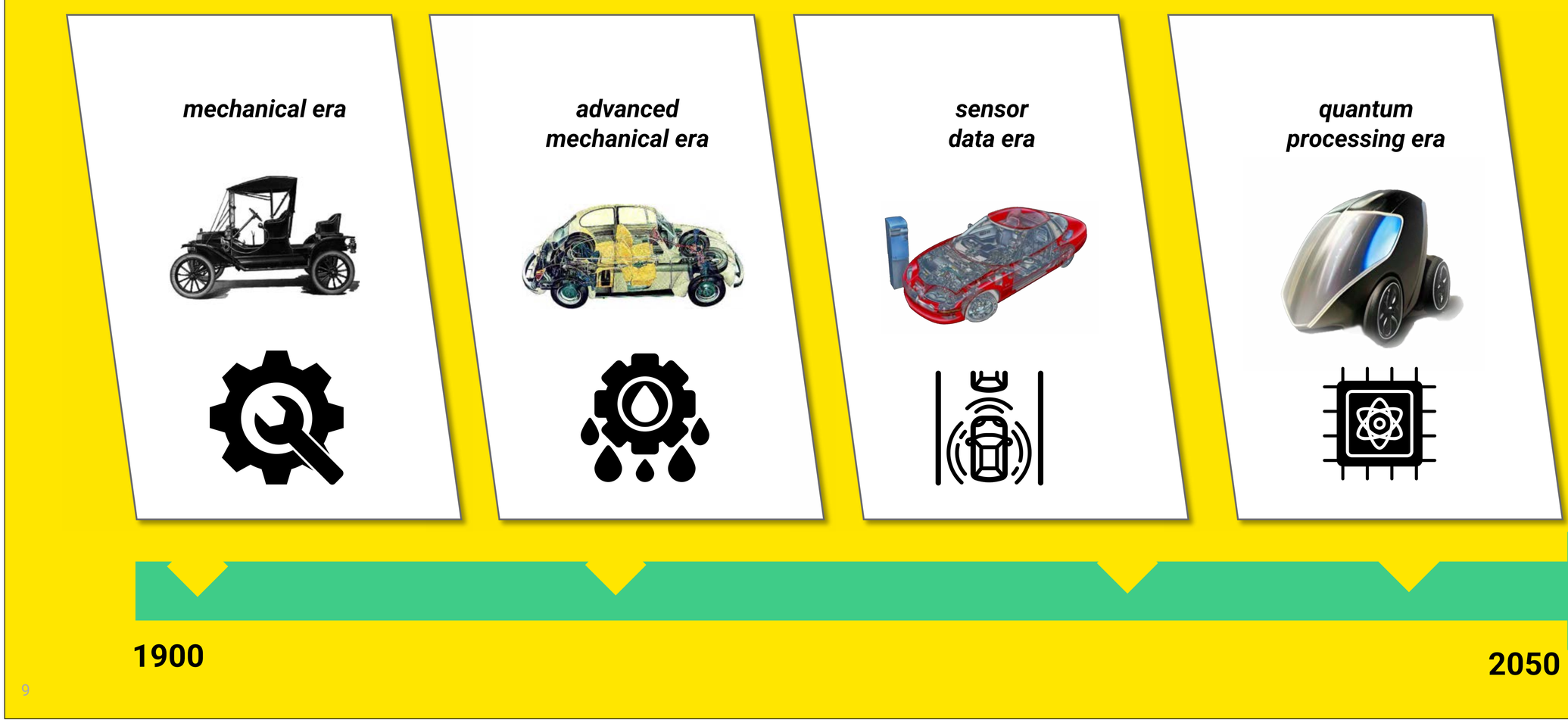
affected: all types of automotive electronics
(each OEM shapes this into proprietary domains)

- **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**
- only **accredited notified bodies** are entitled to certify compliance towards UNECE WP29
- 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?

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



9

9

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

10

10

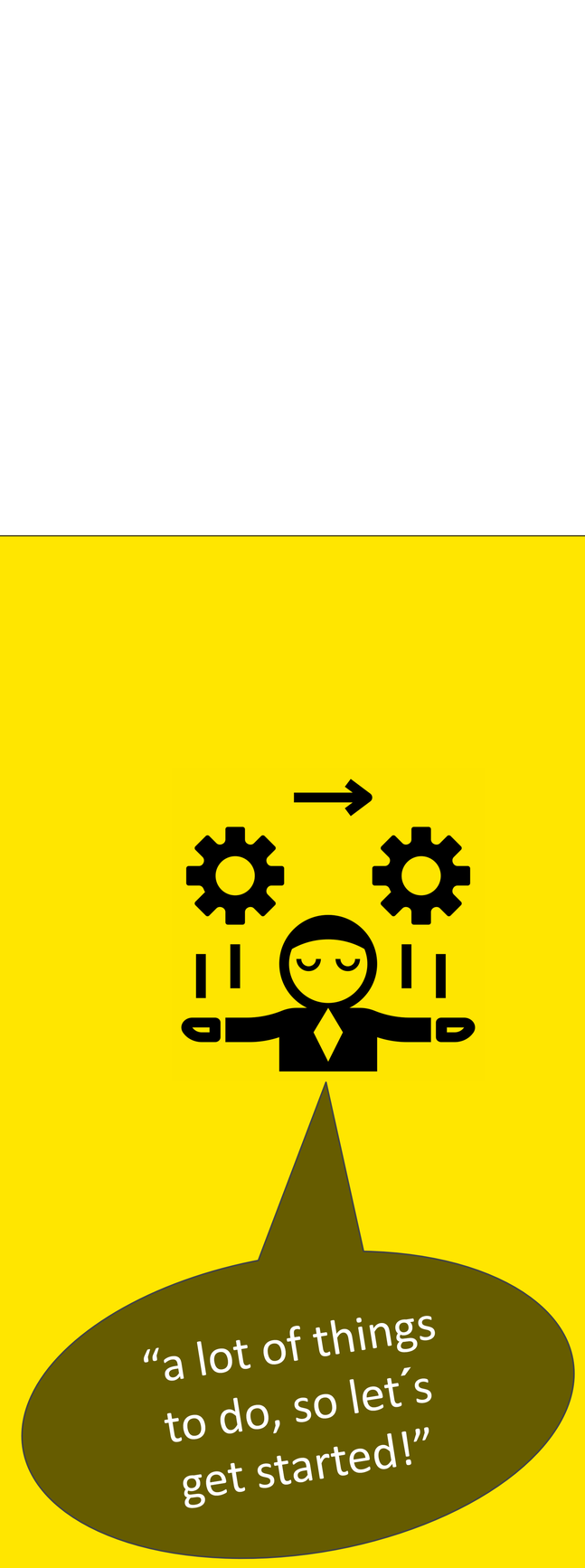
potential Quantum Computing Impact

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

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

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



D E K R A
D I G I T A L

Thank You!

- for your time
- for your attention

Andy Schweiger
Handwerkerstrasse 15
70565 Stuttgart

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