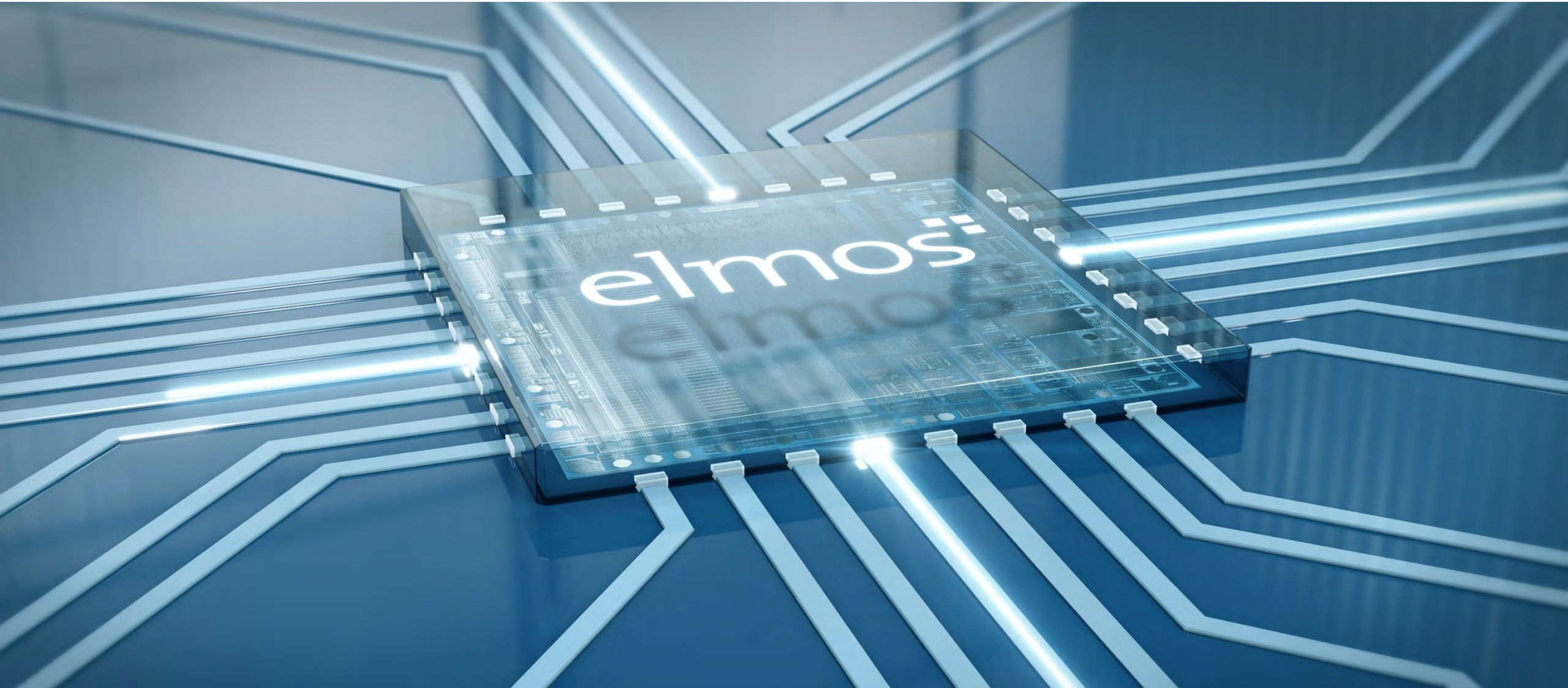


True Random, Truly Secure: Quantum Technology for Next-Gen Automotive Systems“

Dr. Bernd Burchard, Elmos Semiconductor SE

elmos[®]



Mobile Quantum Technologies for the Mobility of Tomorrow

elmos[®]



World Market Leader with Innovative Mixed Signal IC Solutions

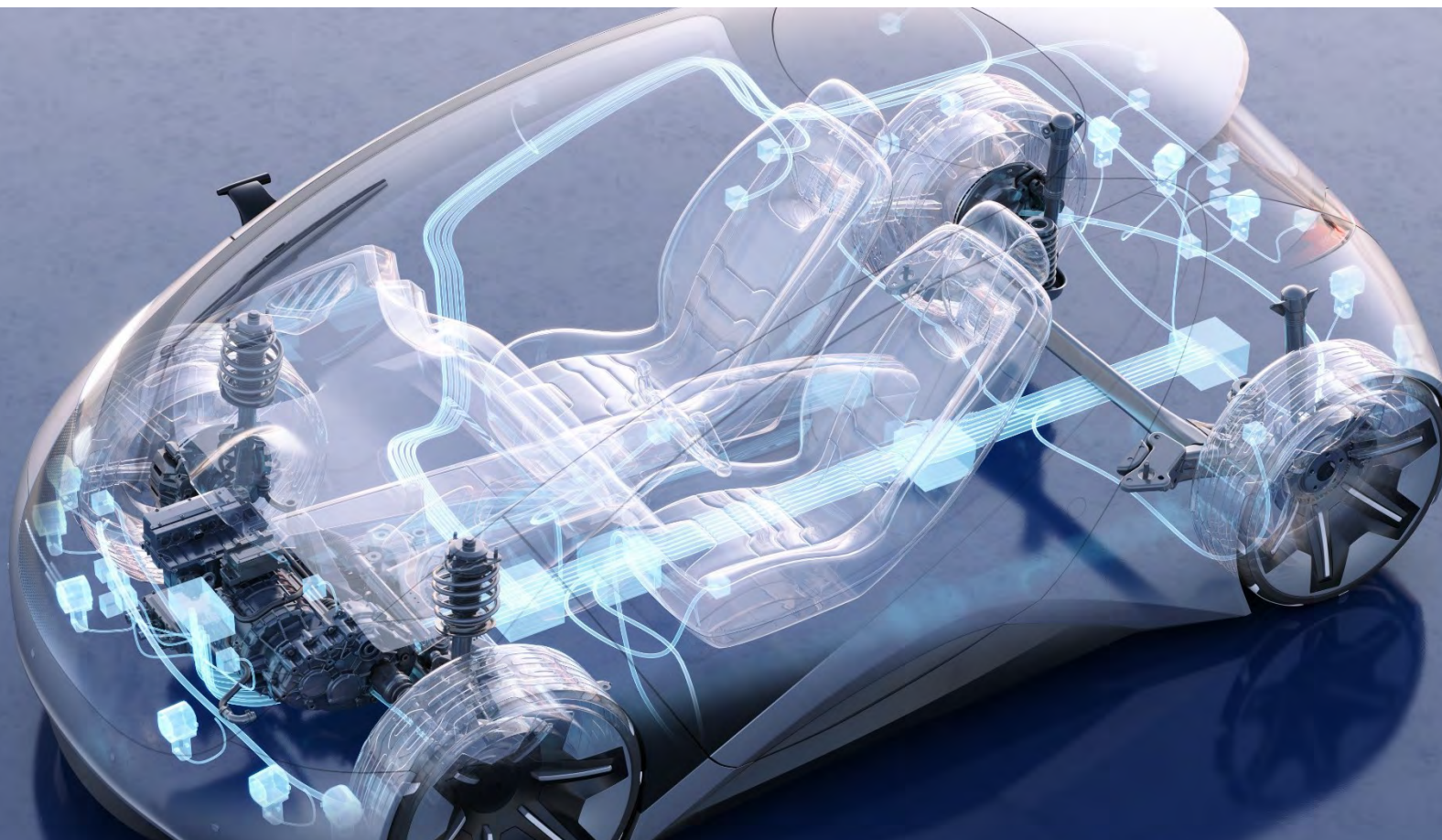
elmos[®]



#1

- ✓ Ambient & Rear LED Light
- ✓ Ultrasonic Ranging
- ✓ Climate Control
- ✓ Dry Braking

The Little Things Matter – Innovations Matters



The **semiconductor content** in today's vehicles is steadily growing

Serving Global Automotive Megatrends



Autonomous Driving and ADAS

Secure Nearfield Ranging

Ultrasonic sensor ICs: environmental mapping



Individualization

Unparalleled Opportunities for Individual Comfort Zones

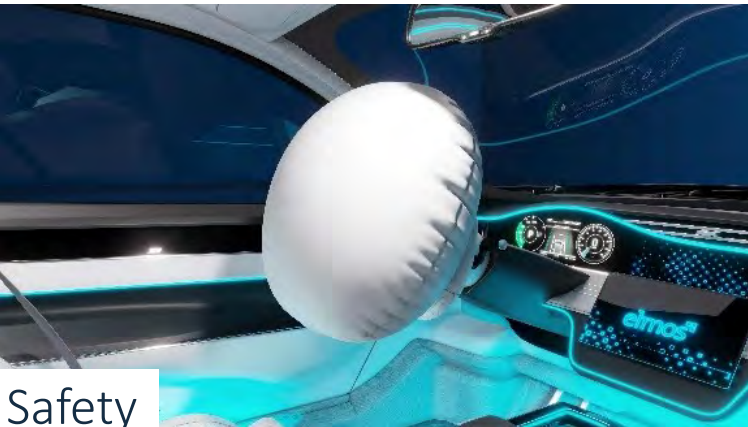
LED driver ICs: static and dynamic ambient lighting



Electro Mobility and CO₂ reduction

Intelligent Thermal Management

Motor Control & Pressure Sensor ICs: cabin, powertrain, battery



Safety

Increased Passenger and Road Safety

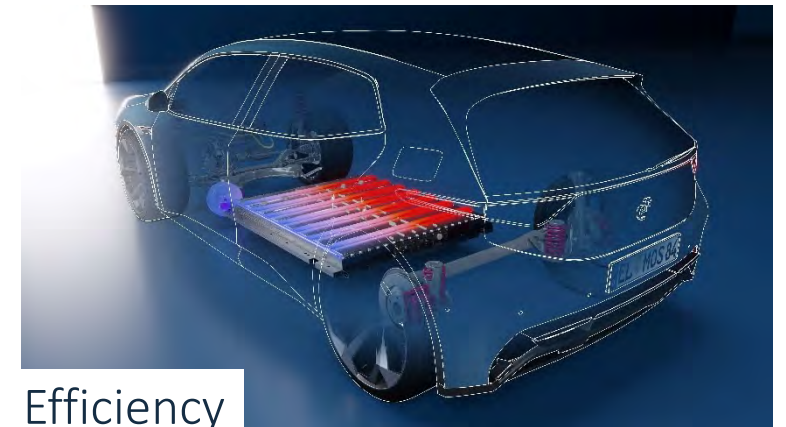
Ultrasonic sensor, rear light LED driver and airbag control ICs



Embedded Software

Hardware Integration Simplified

Elmos standard software



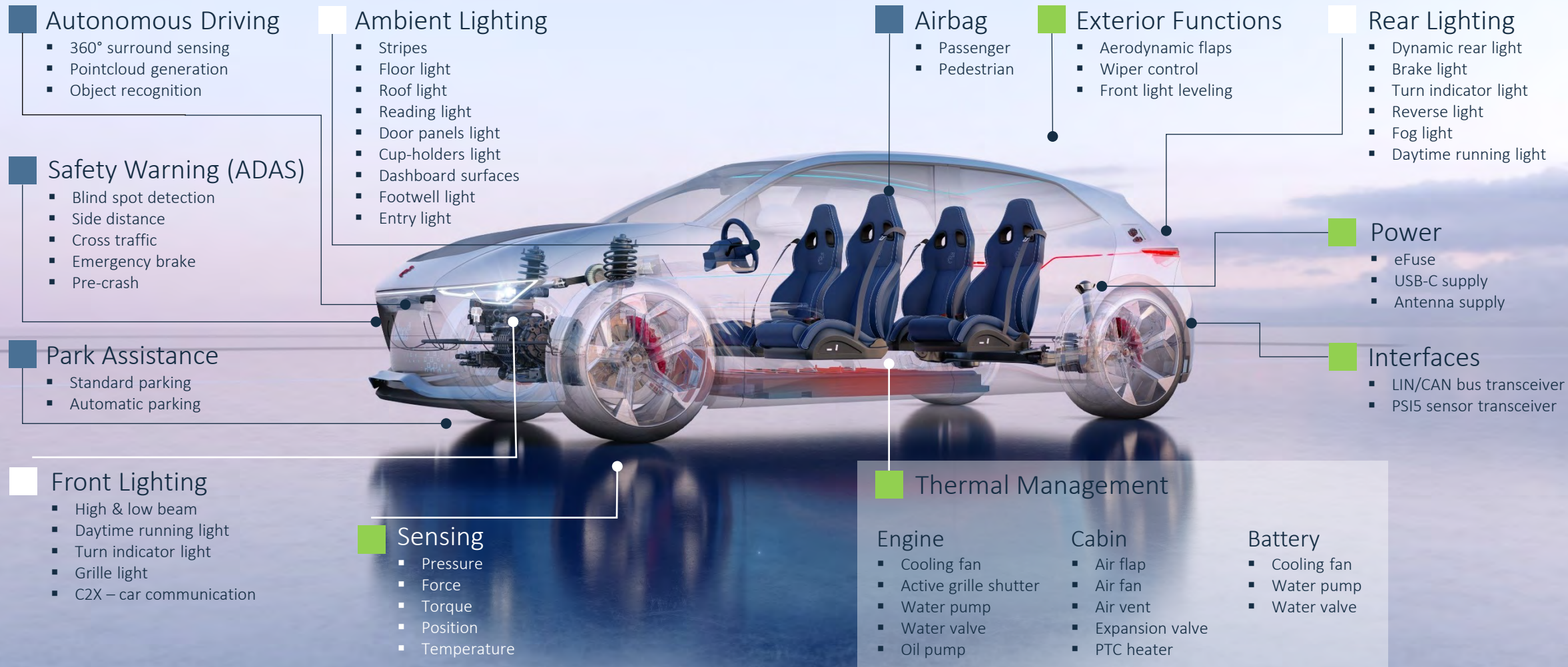
Efficiency

Smart System Solutions

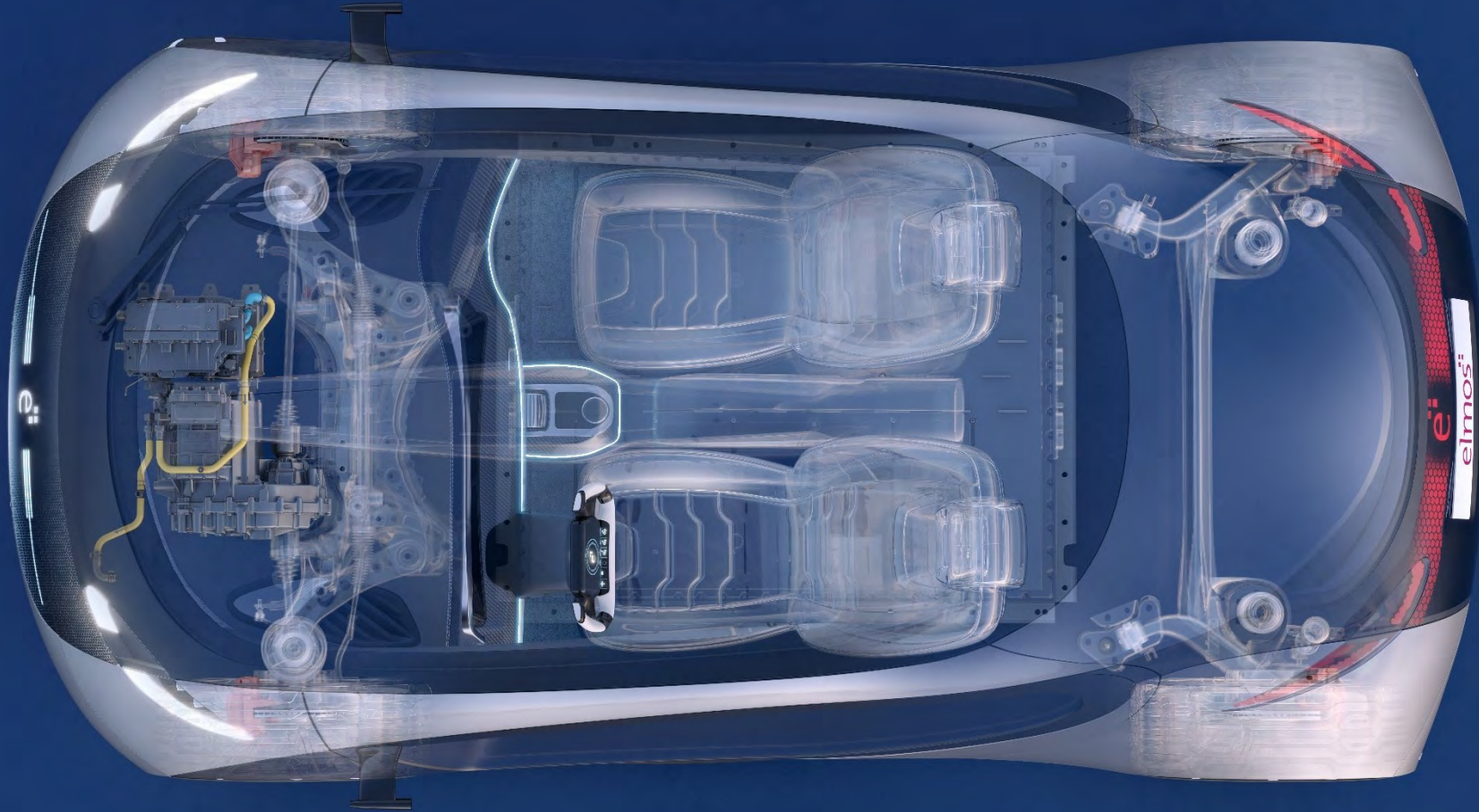
eFuse for new domain and zonal architecture concepts

More Efficient, More Comfortable & Safer

■ Electrification & Efficiency
 ■ Comfort & Premium
 ■ Safety & ADAS



Automotive Applications Powered by Elmos ICs



Product Segment » Motor Control



Highly Integrated Motor Control ICs: Best Performance and Low System Cost

- Broad product portfolio for DC, Stepper and BLDC motors
 - Unique BLDC motor control family for 12V, 24V and 48V board net architecture for typical 5W up to 3000W motors
 - Advanced motor control algorithms for sensor-less drives
- Innovative ICs for motor driven HVAC systems
 - #1 for smart HVAC actuators
 - 750+ million ICs delivered
 - Benchmark for low noise and high efficiency



Improve Comfort and Safety Functions

- #1 in ambient light control
 - 200+ million LIN RGB controller ICs in the field
 - Auto-addressing easing module integration
 - Delivering homogeneous light output of any color over lifetime across temperature
- Elmos rear lighting solutions setting benchmark
 - Highest flexibility for dynamic individual LED control using multichannel operation
 - Brightest LED lighting by best-in-class thermal management technique
 - Constant light intensity at high temperatures
 - Interface scalability and diagnosis for functional safety



Product Segment » Ranging



IC Solutions for Assisted and Autonomous Driving

- Global market leader in ultrasonic ICs
- More than 1.8 billion ranging ICs in the field
- Broad ASSP product portfolio
- From most affordable (Direct Drive) to highest performance (ADAS applications)
- Enabling object localization, level- and flow-metering
- Several ultrasonic master ICs support future system architectures



Product Segment » Sensing



Bridging the Physical World Precisely to Standard Analog and Digital Interfaces

- More than 20 years of experience in automotive and industrial sensing
- Benchmark IC solutions for sensing pressure, temperature, inductance, capacitance and magnetic field
- Portfolio of sensor signal processors
 - Supporting all standard sensor interfaces
 - Enabling functional safety applications
 - Lowest BOM cost at best performance



Reliable IC Solutions for Demanding Applications

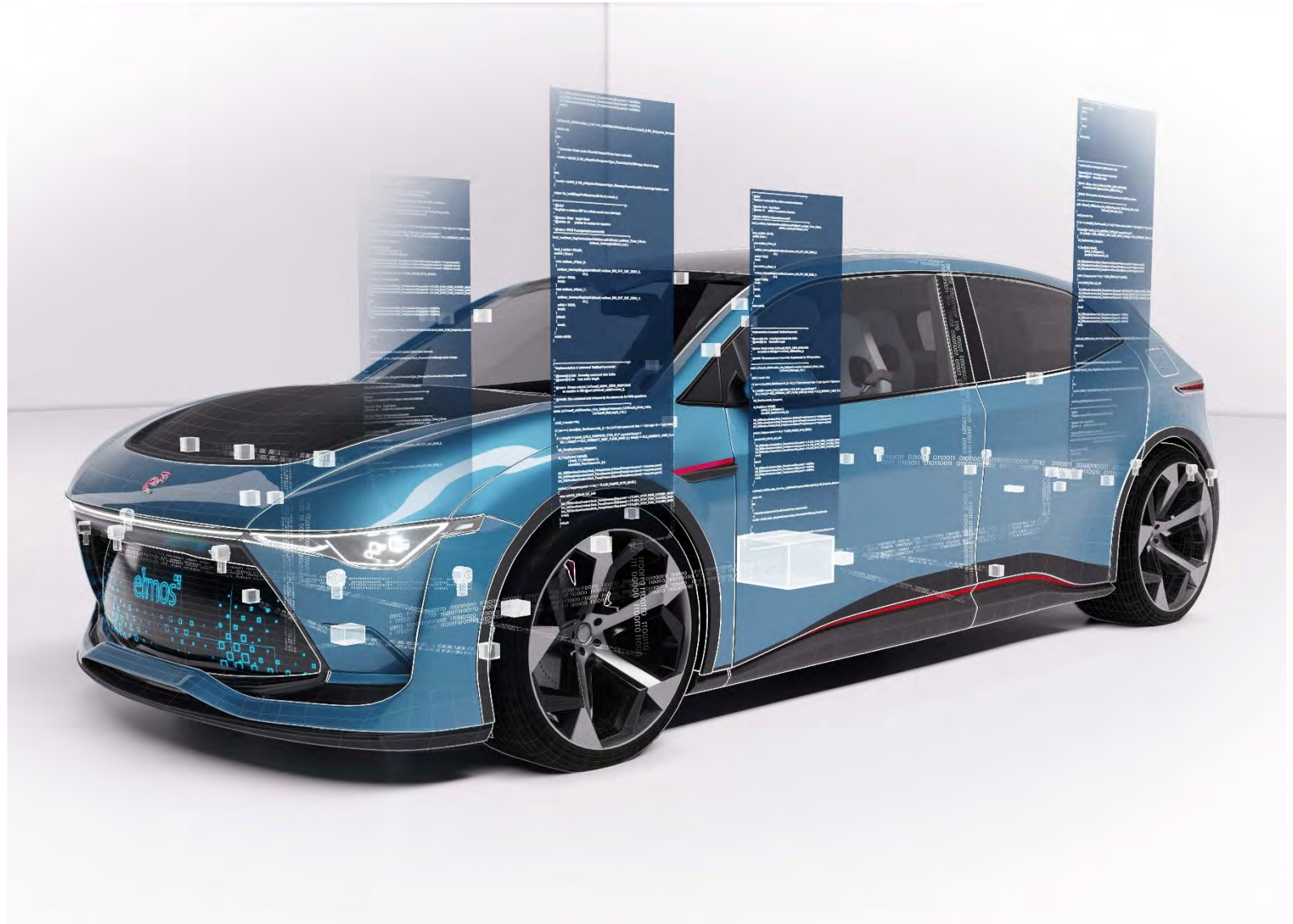
- 20+ years experience in developing passive safety system ICs (up to ASIL-D)
 - Highly integrated companion chips enabling reliable airbag control units
 - Multi-channel PSI5 transceivers to connect peripheral sensors to the ACU
- Application specific power supplies
 - Automotive USB power supplies
 - Power supply for antenna modules
- Comprehensive in-vehicle network portfolio
- Smart power solutions enabling vehicle electrification (e.g. eFuse driver)



Product Development



- **Broad expertise** in analog mixed-signal integrated circuit design for automotive and industrial applications
- **~450 product developers & engineers**
- Global application support and resident engineers at production partners
- **Innovation driven team** – Ø 61 new granted patents per year
- **Broad design IP portfolio**, also incl. ARM μ Cs
- Certified for highest quality and safety standards ISO26262, IATF 16949, AEC-Q100
- **In-house labs** for EMC/ESD and failure analysis





Quantum Sensing NV-Centers for automotive applications

elmos[®]

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

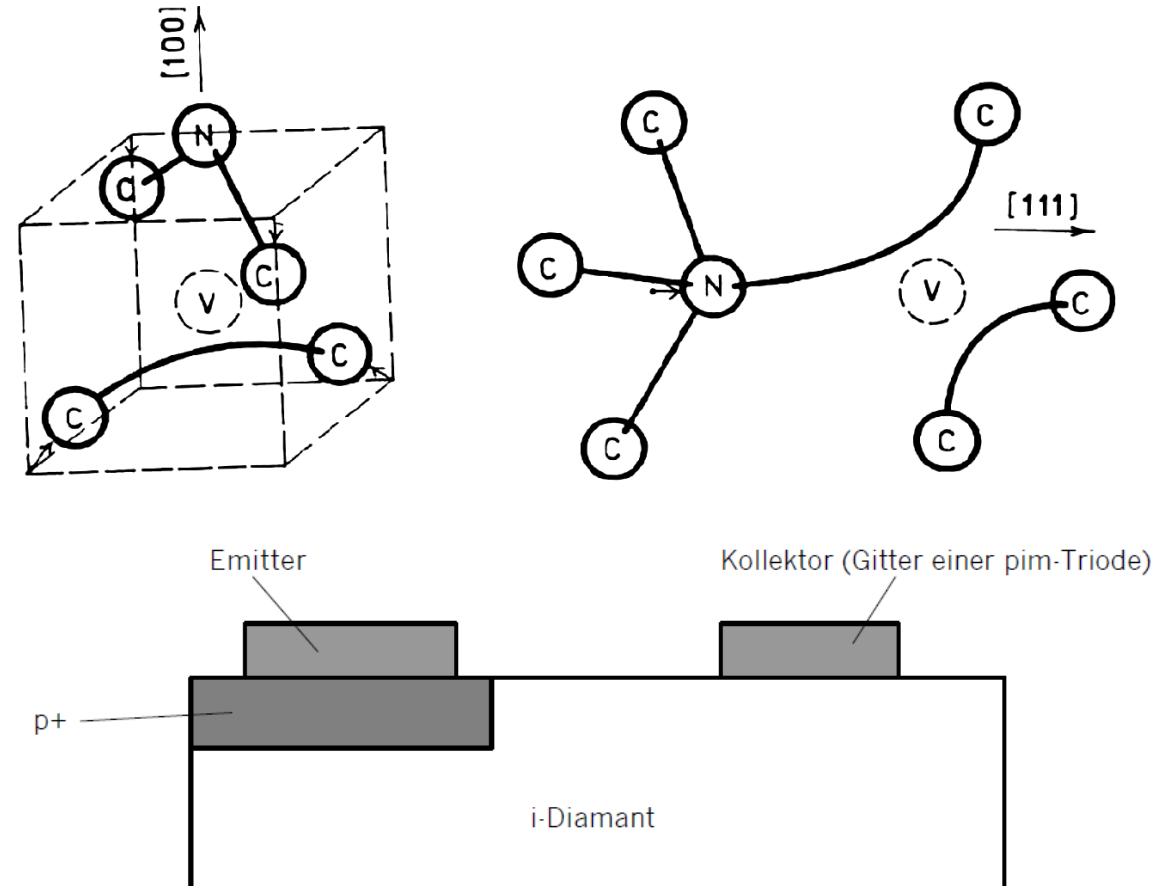
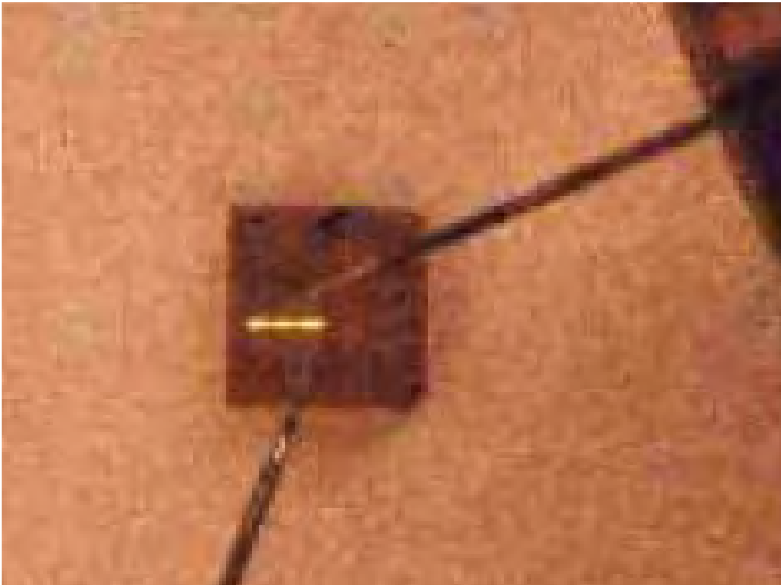
Dr. Bernd Burchard

18.02.2026

elmos[®]

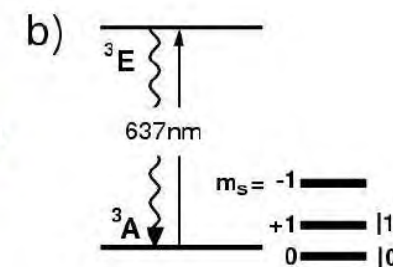
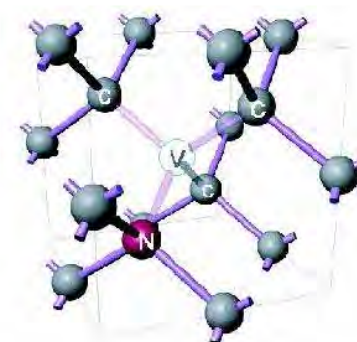
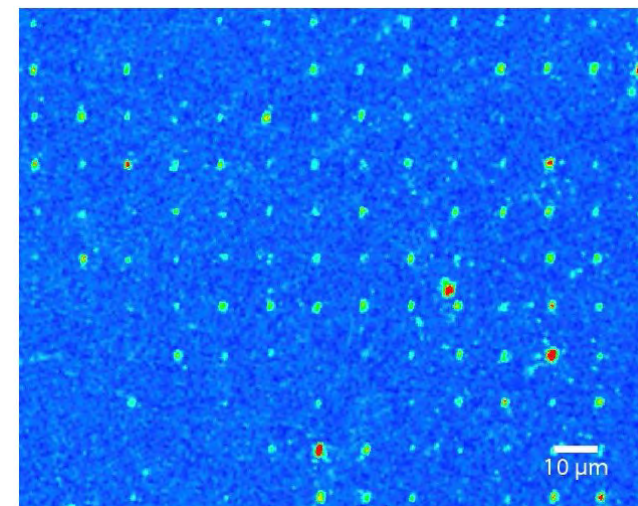
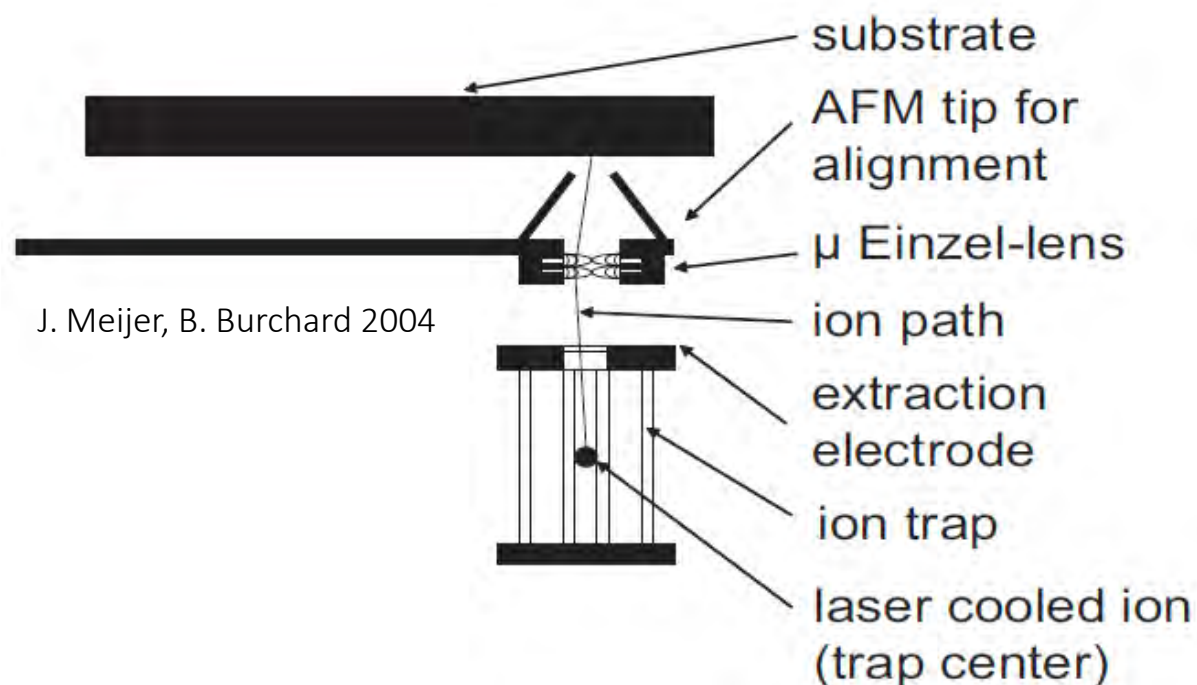
NV center based quantum technologies

- First diamond based LED 1993



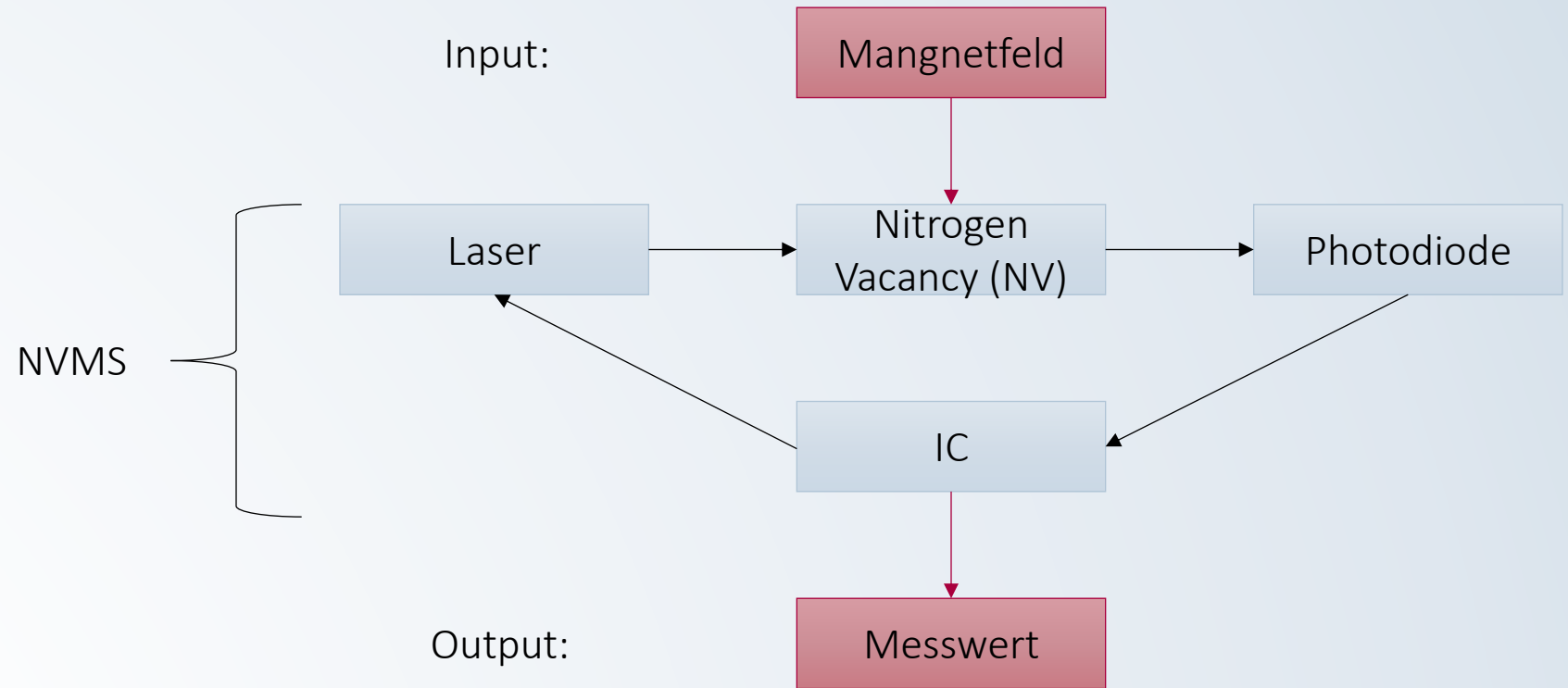
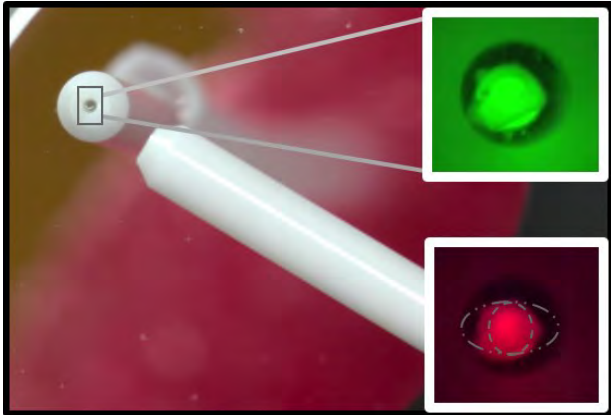
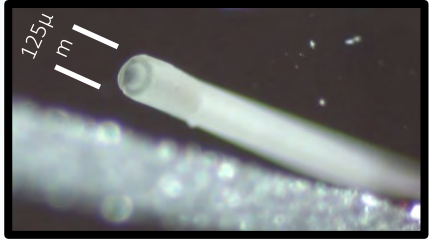
NV center based quantum technologies

- First structured NV center cluster production 2004



B. Burchard, NM Scale Resolution Single Ion Implantation Into Diamond for Quantum Dot Production, Conference: 15th European Conference on Diamond, Diamond-Like Materials, Carbon Nanotubes, Nitrides and Silicon Carbide (DIAMOND 2004)

Disruptive Quantum Sensing at Elmos

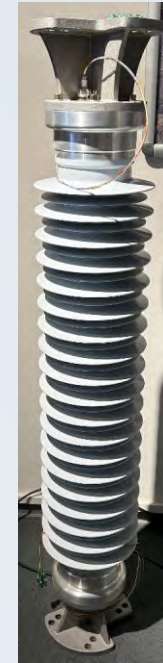
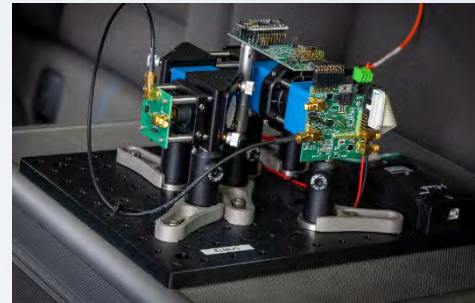
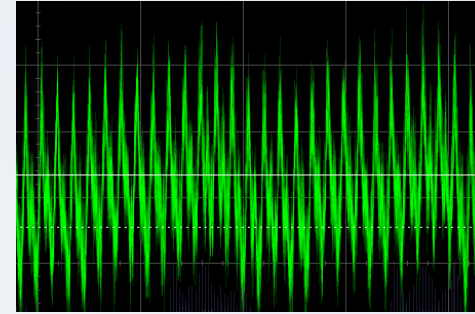
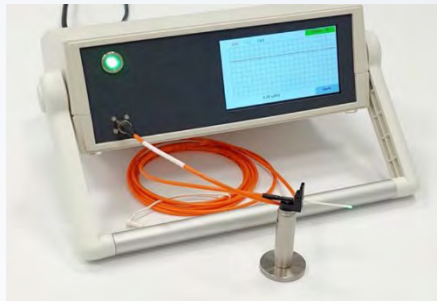
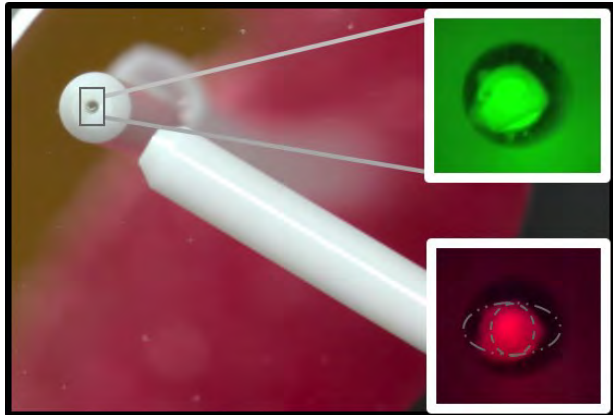
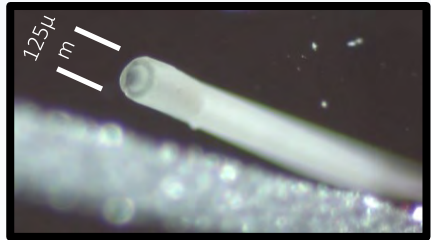


USPs

- Optische Messung
 - Galvanische Trennung
- Als SiP integrierbar

- Hohe Bandbreite
- Sensorkopf dünn wie ein Haar
 - Hohe räumliche Auflösung

- Großer Temperaturbereich
- Einsatz in anspruchsvoller Umgebung möglich
- Shuntlose Strommessung



USPs

- Optische Messung
 - Galvanische Trennung
- Als SiP integrierbar
- Hohe Bandbreite
- Sensorkopf dünn wie ein Haar
 - Hohe räumliche Auflösung
- Großer Temperaturbereich
- Einsatz in anspruchsvoller Umgebung möglich
- Shuntlose Strommessung

next gen QT Sensor interface

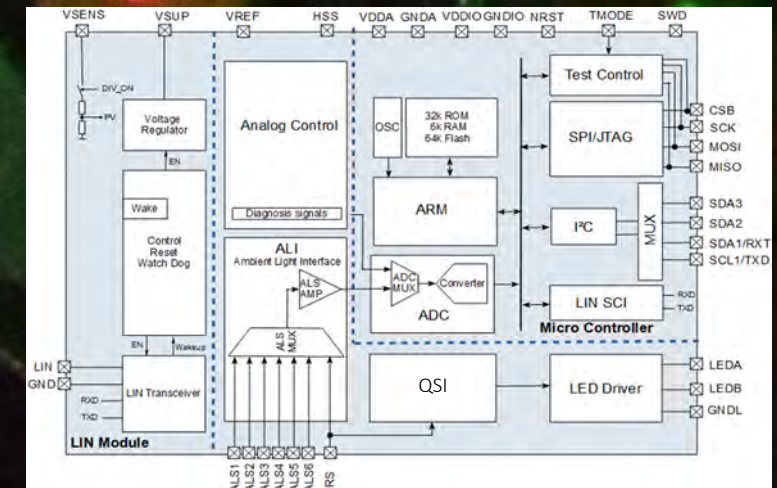
SOC with embedded μ C, LIN and I²C

Key Features

- Quantum Sensor interface
 - HALIOS® technologies inside (immunity against EMV, high ambient light, temperature and aging drifts)
 - 2 x LED channels up to 20mA
 - 1 x Photodiode channel
 - 6 x Ambient Light channels with high sensitivity down to 10pA photo current
- High voltage power supply (12V)
- Low current consumption <20mA
- Embedded 32-bit microcontroller-Arm®
 - 128 Kbyte Flash program memory + 4kbyte NVM for configuration parameters
 - 6kByte RAM
- LIN interface V2.2, SAE-J2602, ISO09141
- Boot Loader and LIN Stack firmware available
- Automotive qualified (AEC-Q100)
- Functional safety (ISO26262), supports ASIL B
- QFN32L5 Package (tape on reel)

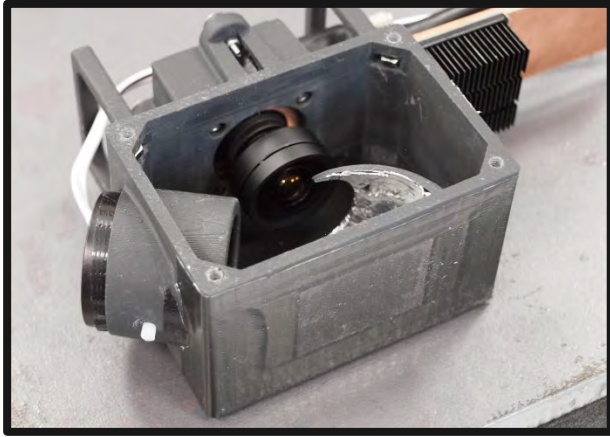


SOC: system on chip
 NVM: non volatile memory
 HALIOS: high ambient light immune optical system

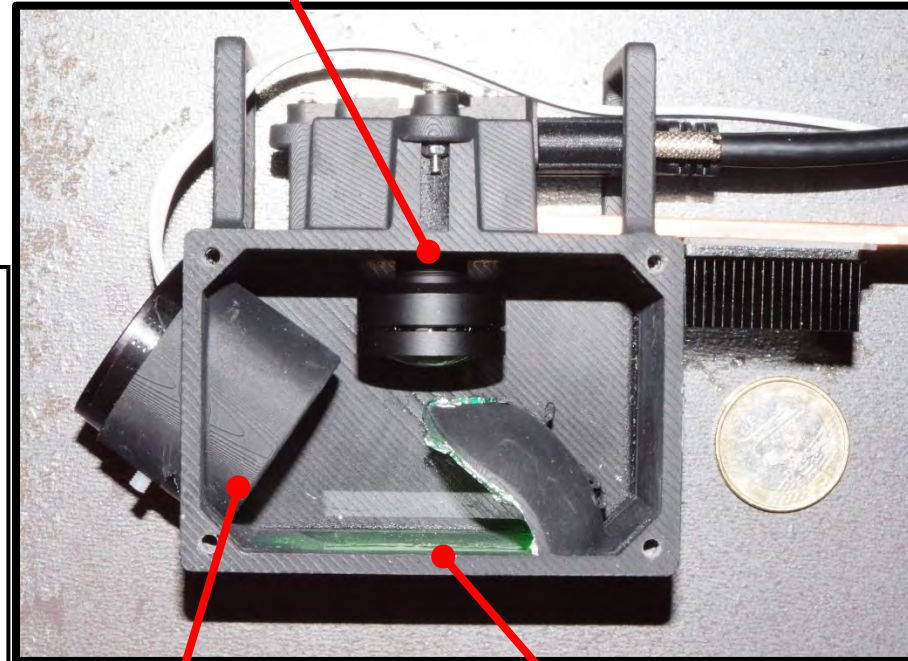


Megapixel magnetic imaging (prototype)

elmos[®]



monochrome camera



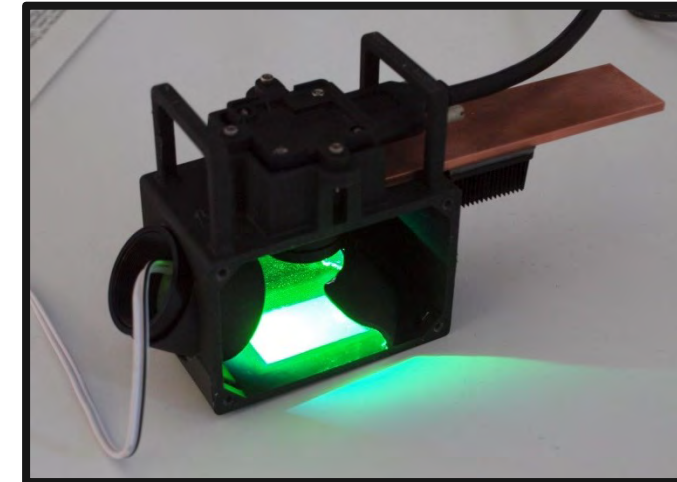
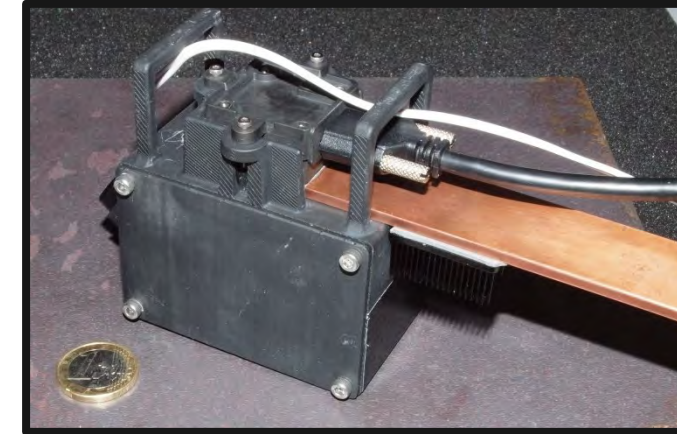
LED illumination

layer of
diamond material

Current specifications:

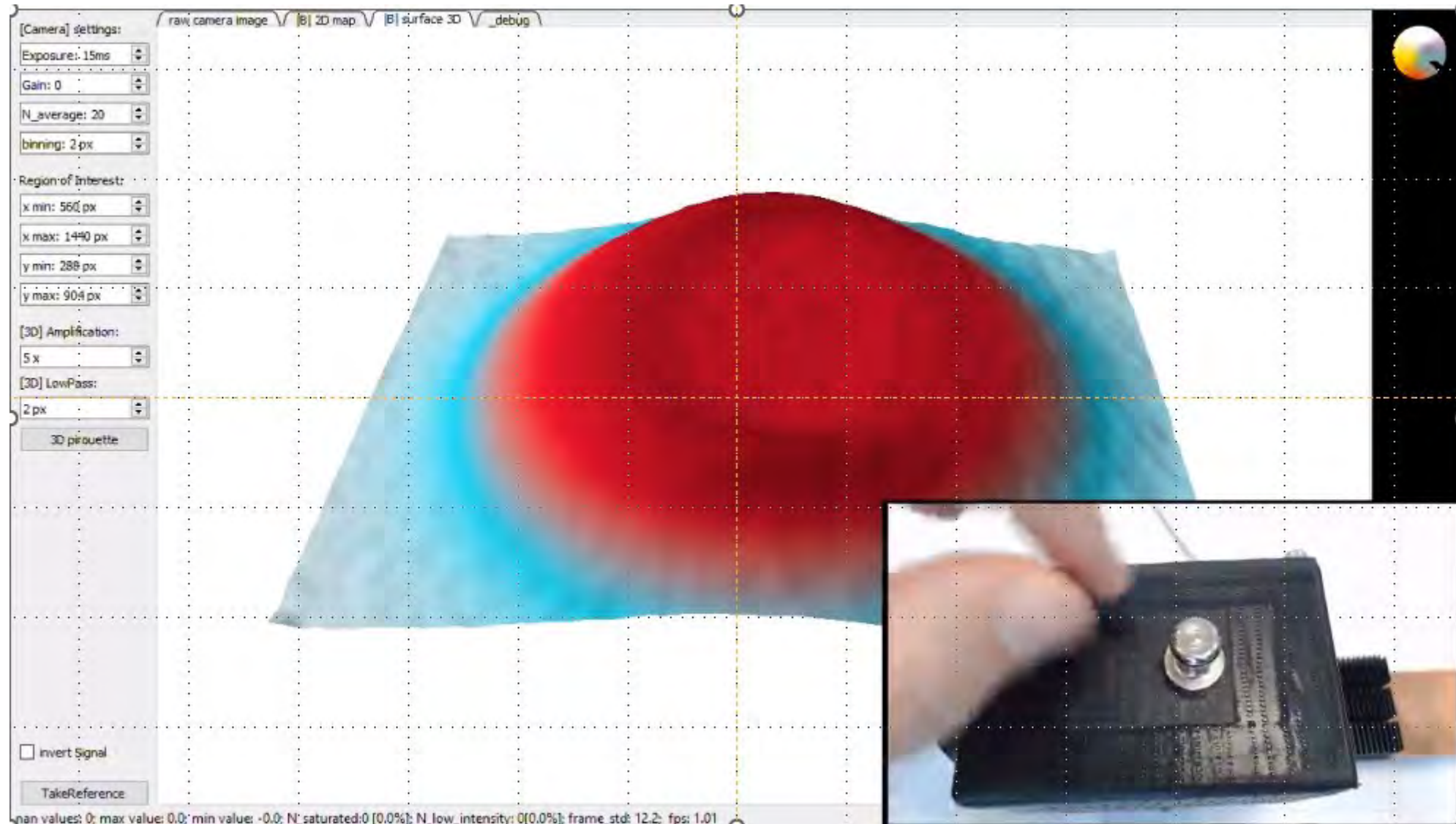
- Sensor Area: 32 x 22 mm
- Effective pixels: ~ 900 x 600 Pixel
- Effective pixel size: ~ 33 x 33 μm
- Magnetic range: 0 ... ~50 mT
- Framerate: up to 160 fps
- Sensor distance to sample: <1 mm

Source: Quantum Technologies GmbH

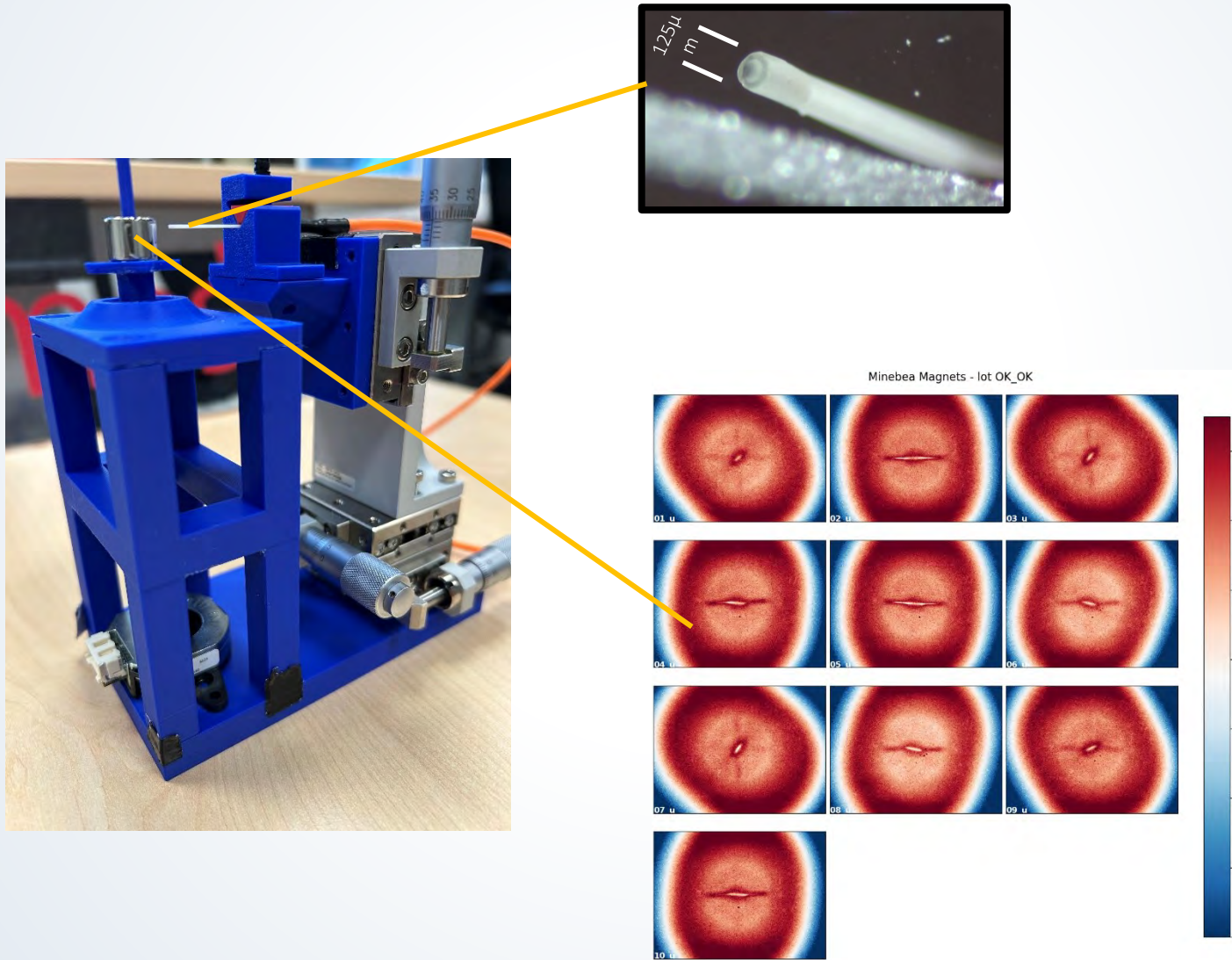


Megapixel magnetic imaging

elmos[®]



NV-Sensoren für die positron detection and QA



Quantum Computing NV-Center based automotive QC

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

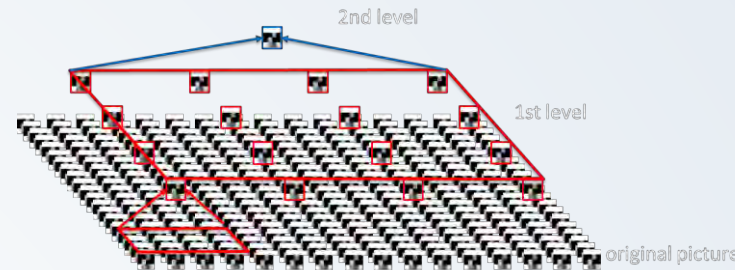
Dr. Bernd Burchard

18.02.2026

Übersicht Quantentechnologien: Quantencomputing

Status heute

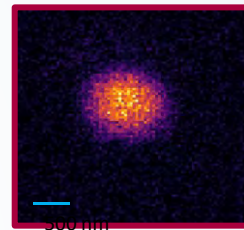
- mobil & raumtemperaturfähig => **automotive fähig**
- Solid State Spin-QBits
- **>1000 Qbit Multi-Core QC** möglich
- Cores mit >10 direkt verschränkbaren Qbits
>30 verschränkbare Qbits bis 2027
(Schlüssel N-Dotierung des Substrats)
- T_2 Zeiten für schwach gekoppelte nukleare Q-Bits ca. 5 Min.
- Effektive Tofoli-Gatter
(=umkehrbare NAND-Gatter)
(VHDL basierte Synopsys-QC-Gatter-Synthese möglich & patentiert)
- **Angriffs-Vektoren für CSPRNGs möglich**
- Defense geeignet



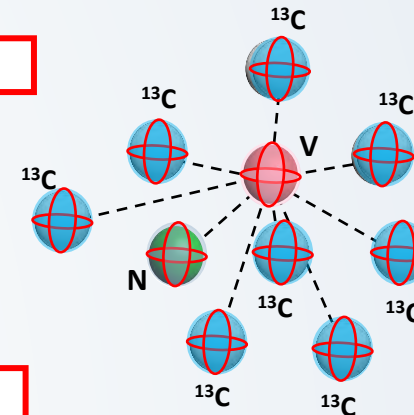
QCNN fähig

Attention Function mit QBits
Faktor 100 Energieeinsparung
Wurde auf der Hannover-Messe
live demonstriert

electron + nuclear qubits



1 NV = 2-10 qubits





Cybersecurity Cybersecurity für neue Automotive Systemarchitekturen durch QRNG

elmos[®]

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

18.02.2026

elmos[®]

Weitere Agenda

- Automotive-Cybersecurity: Bedrohung durch die Entwicklung von KI und Quantencomputern
- Marktwachstum für QRNG
(Quantum Random Number Generator)
- Elmos stellt den weltweit kleinsten QRNG vor
 - Integrationskonzept und QRNG-IP-Bausteine
 - Nachgewiesene Zufälligkeit
 - Robustheit gegenüber physischen und KI-Angriffen
 - Vorteile des QRNG im Vergleich zu TRNG
 - ✓ Geringerer Leistungsbedarf
 - ✓ Kürzere Aufwärmphase
 - ✓ Kleinere Baugröße
 - Timing und Zertifizierung
- Zusammenfassung
- Q&A

Motivation: Automotive Cybersecurity-Bedrohungen

- **Fahrzeuge sind attraktive Hacker-Ziele:**
Ständig vernetzt, hohe Stückzahlen, hoher Wert, lange Lebensdauer
→ riesiger Datenpool
- **Cyberangriffe 2023 => 2024 +150%**, davon **92 % remote** ausgeführt
- **Cybersecurity** wird zu einem **entscheidenden Erfolgs- bzw. Misserfolgsfaktor** in der Automobilindustrie (UNECE R155 bereits in Kraft)

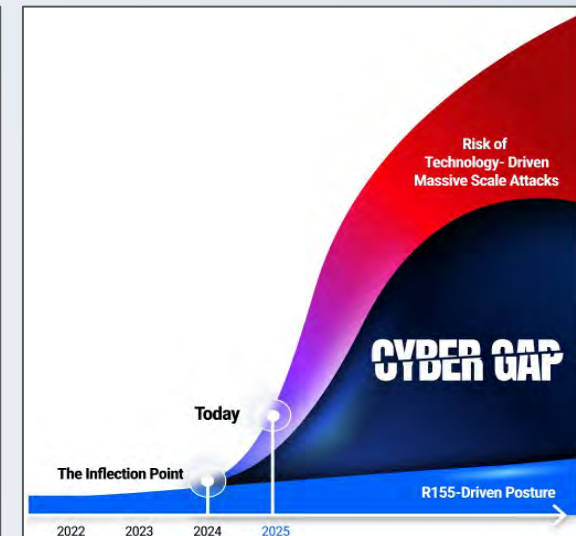
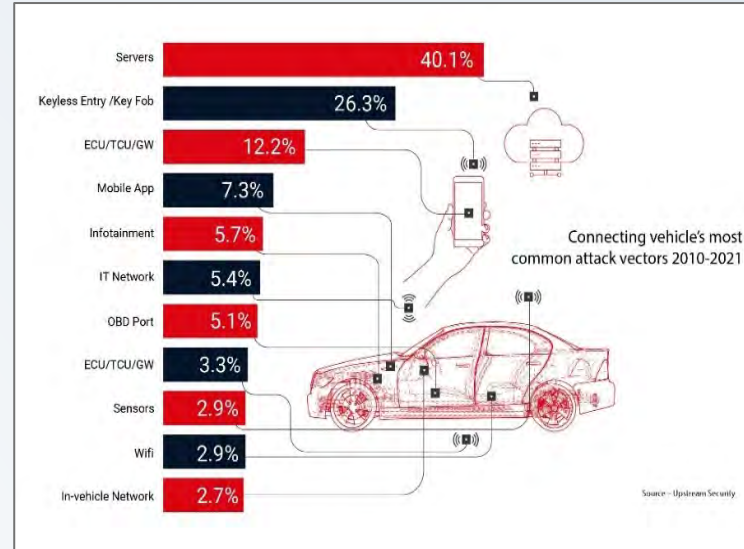
Beispiele für Angriffsvektoren:

- **CAN-Injection:** mit im Darknet verfügbaren Tools (< Eur 500)
→ Car-Hijacking oder -Diebstahl
- **Ransomware-Attacken** über OTA-Updates (Over-the-Air)
- **Zugriff auf sensible Fahrerdaten** über Infotainment-Systeme
- **Verbreitung von Malware** über vernetzte Geräte

Cyber Gap:

Der Lebenszyklus eines Fahrzeugs >15 Jahre!!
=> Konflikt mit der schnellen und exponentiellen Entwicklung von KI, Rechenleistung und krimineller Energie.

=> Daher sind Maßnahmen zur Risikominderung **JETZT** notwendig!



Motivation: Cybersecurity durch QRNG

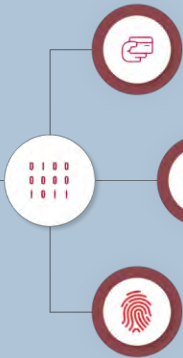


- Cybersecurity benötigt echte Zufallszahlen für Kodierungs-Schlüssel In-Car- und Car-to-X-Kommunikation.
- Aktuell werden deterministische Pseudo-Zufallszahlengeneratoren (PRNG) durch True-RNGs (TRNG) unterstützt.
- Bestehende TRNG+PRNG-basierte Zufälligkeit ist jedoch anfällig für KI-Algorithmen und klassische physikalische Angriffe (z. B. Temperatur, Versorgungsspannung, EMC, Alterung).
- Cyberangriffe nutzen zunehmende Rechenleistung, einschließlich aufkommender Quantencomputer (< 10 Jahre).
- Data-Harvesting: Sammele nun – de-chiffriere später
- All das öffnet neue und gefährliche „Hacking-Backdoors“ in allen Kommunikations-Systemen und Kryptolösungen
- » Quantum Random Number Generators (QRNG) bieten eine Lösung für dieses Risiko
- » Frage: Wer trägt das Risiko, nicht die robusteste Lösung zu nutzen?

Marktwachstum für QRNG

QRNG bereits in Serienproduktion

IDQ brings a new level of quantum enhanced phone security allowing differentiated security solutions for ICT services



Pay Services

Cryptocurrency services



Identification services

Samsung Galaxy Quantum5 Released: A Quantum Leap in Smartphone Mobile Security
By CIOchina / 09/05/2024 / 4 minutes of reading
Samsung has released a new smartphone with quantum security, the Samsung Galaxy Quantum5. The company developed this device in partnership with SK Telecom. If you're outside of South Korea, you won't be able to get your hands on one. Another key partner in making this phone a reality is ID Quantique (IDQ), a company that has provided the quantum cryptographic chip in the device. This chip is what makes the Galaxy Quantum5 stand out from the rest of Samsung's lineup.

Marktwachstumsprognose für QRNG



Kommunikation zwischen Auto und X: Überall, jederzeit und ... sicher



Die Nachfrage nach QRNGs steigt stark – insbesondere in den Bereichen IoT, Gaming, Mobiltelefonie und Automotive.

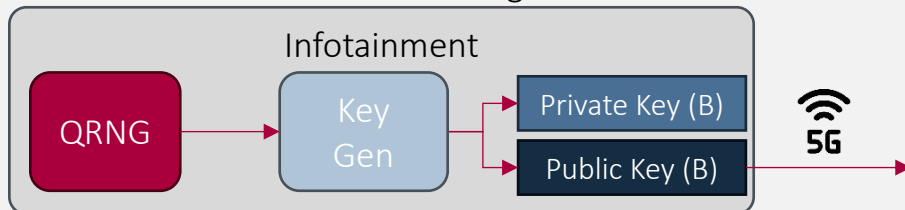
- Automotive
 - Automotive „Total Addressable Market“ (TAM) ~ 90 Millionen Fahrzeuge/Jahr.
 - Schlüssel-Anwendungen: Keyless Entry, Car-to-X-Kommunikation und Software-Updates „Over the Air“ (OTA)
- Aktuelle QRNG-Lösungen sind noch zu groß und teuer für breite Marktakzeptanz

Elmos zielt daher auf Miniaturisierung und Kosteneffizienz

Automotive-QRNG-Anwendungen: Infotainment

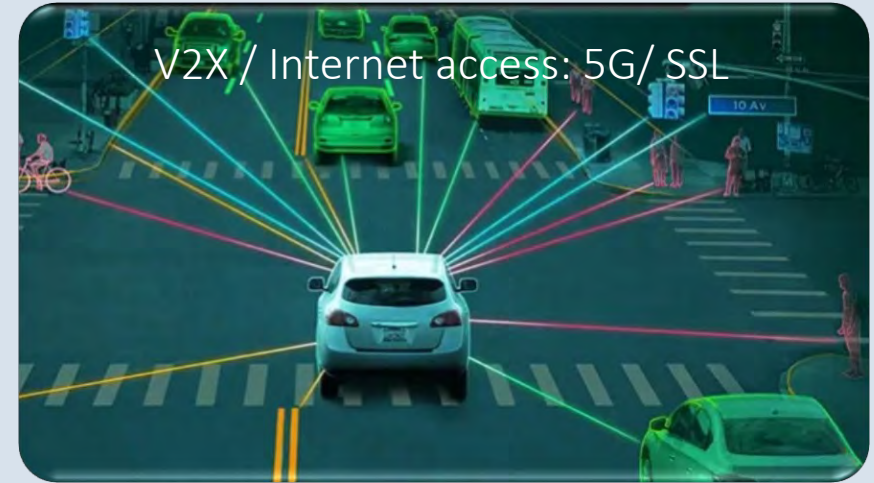
Typische Anwendungen, die von QRNG profitieren:

- **Internetnutzung**
 - HTTPS: TLS / SSL mit RSA / ECC für Schlüsselaustausch, AES / DES für Daten
- **Mobile Datenverbindungen / 5G**
 - Schutz der Teilnehmer-Identität über Subscription Concealed Identifier
 - OTA Verschlüsselung: AES256
- **Lokale Drahtlosnetzwerke**
 - Bluetooth: (AES-128-CCM oder E0 Cipher)
 - WiFi-Verbindungen: WPA3 -> AES128-GCM
- **Lokale kabelgebundene Netzwerke**
 - Ethernet: IEEE802.1AE MACsec (Hardwareimplementiert!)
 - CAN: Potenzial für zukünftige Verschlüsselung – Protokoll noch in Entwicklung



High level
(z.B. Cloud)

Low level
(z.B. Sensor)

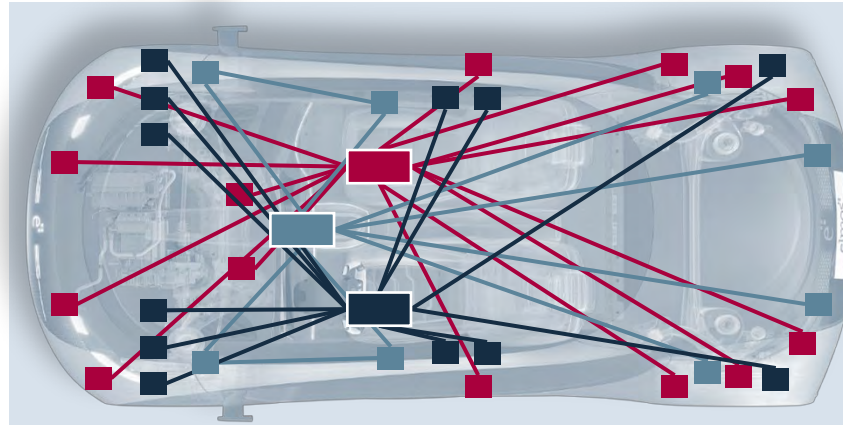


Automotive-QRNG-Anwendungen:

Zonen-E/E-Architektur (ersetzt Domänencontroller-Systeme)

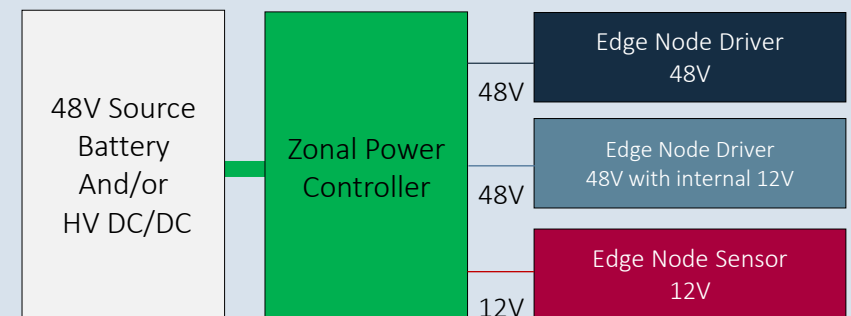
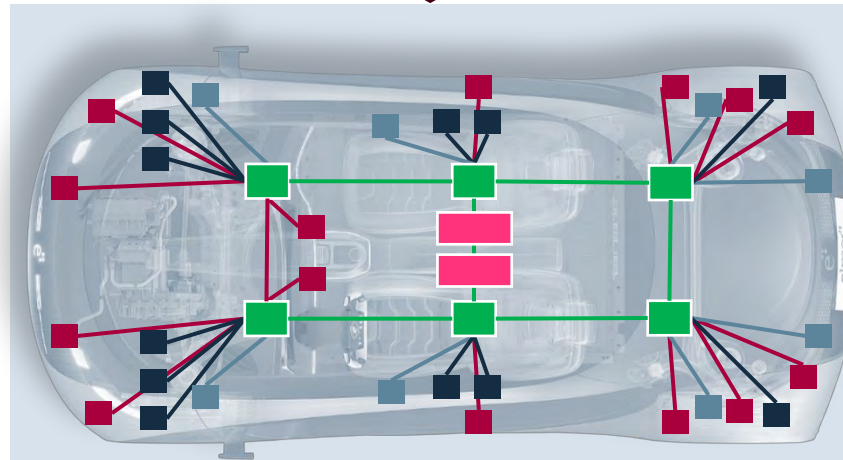
Domänen

- Verteilte kleine Steuergeräte
- Heterogene Netzwerke
- Komplexe Software
- Zentrale Energieverwaltung
- Mehr sicherheitskritische Komponenten



Zonen

- Zentralisierte, gespiegelte ECUs
- Zonensteuerungen, verbunden über 10BASE-T1S / CAN XL)
- Dezentrale Versorgung mit **E-Fuse**
- Mehr sicherheitskritische Komponenten erfordern FuSI / Cybersicherheit mit **RNGs**

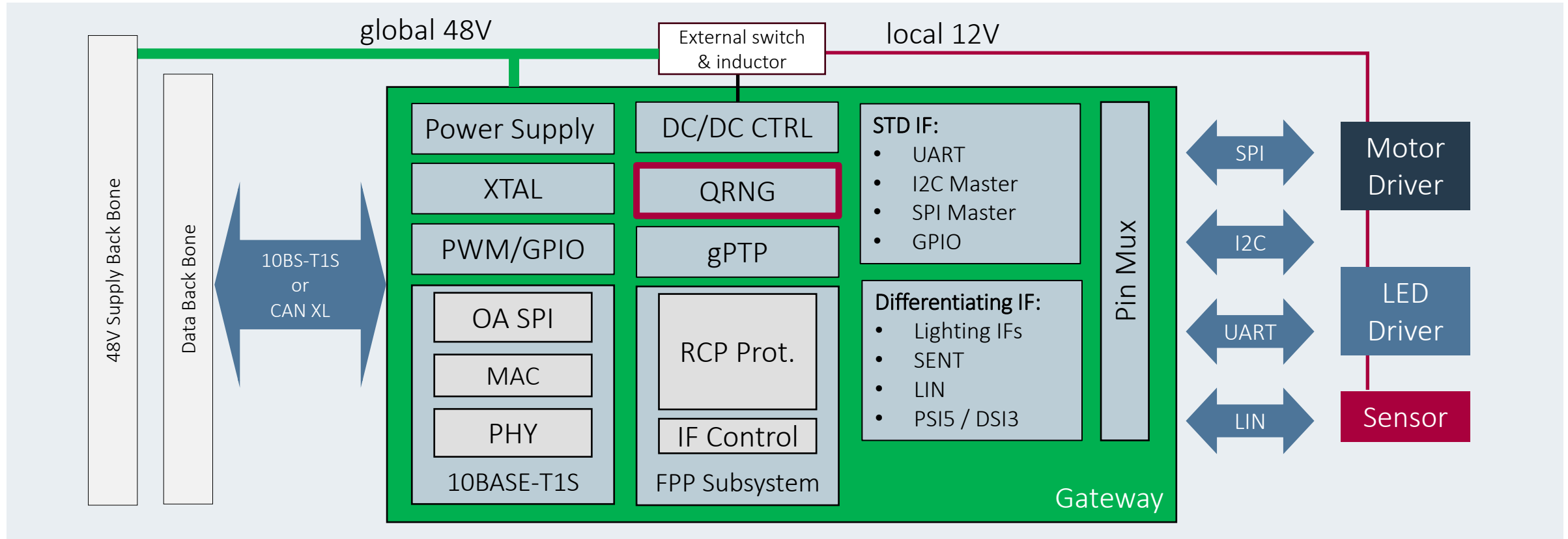


Unsere Vision: Cybersicherheit durch QRNG in jedem Kommunikationsknotenpunkt

Automotive-QRNG-Anwendungen:

Zonales Gateway SBC mit integriertem QRNG (geplant)

elmos[®]



Hauptmerkmale:

- SBC mit 48V -> 12V DC/DC für lokale 12V Komponenten
- 10BASE-T1S oder CAN XL Bus mit Echtzeitprotokoll (gPTP)
- Lokale Standard Bus-systeme: UART, I2C, SPI, GPIO
- Unterstützt verschiedene Schnittstellen zu Sensoren/Aktoren

Next Level Cybersicherheit für modernste Domänencontrollersysteme durch Elmos **QRNG**-Integration



Innovation

Das neue QRNG Konzept

elmos[®]

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

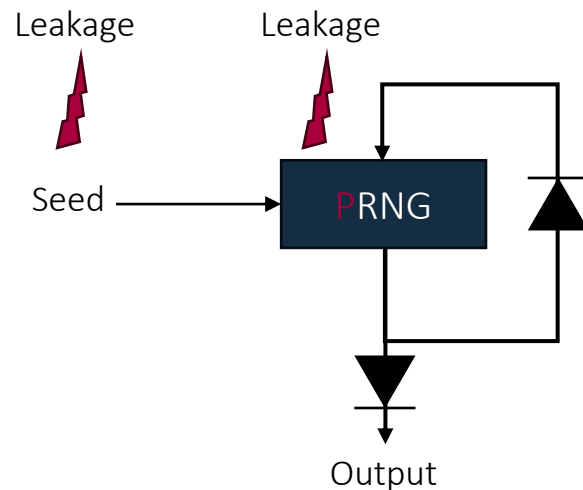
18.02.2026

Evolution von Zufallszahlengeneratoren

PRNG

Pseudo Random Number Generator

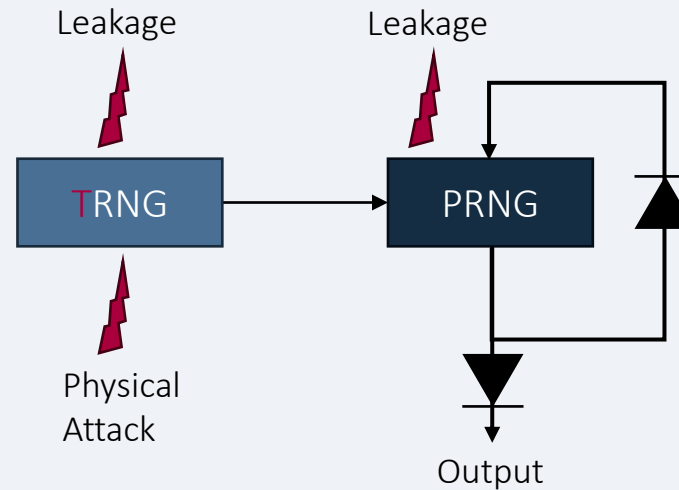
- Basierend auf Algorithmus, der aus einem Startwert eine Sequenz erzeugt
- **Deterministisch**
- **Nicht wirklich zufällig**
- **Vorhersagbar**



TRNG

True Random Number Generator

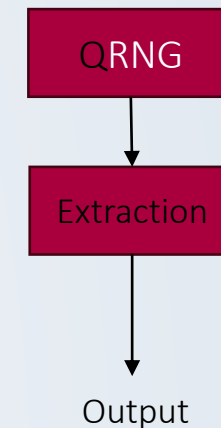
- Basierend auf physikalischen Zufallseffekten
Typisch kombiniert mit PRNG zur Erhöhung der Bitrate
- **Nicht-deterministisch**
- **Zufällig**
- **Vorhersagbar (z.B. KI mittels mathematischer Modelle)**
- **Anfällig für physikalische Angriffe (z. B. Temperatur, EMV)**



QRNG

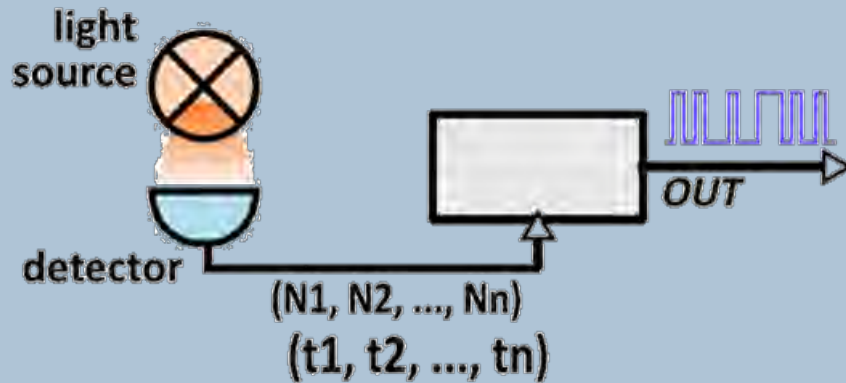
Quantum Random Number Generator

- Basierend auf Quanten-Zufallseffekten
- **Nicht-deterministisch**
- **Zufällig**
- **Nicht vorhersagbar (auch nicht durch QC/KI)**
- **Sicher gegen physische Angriffe**

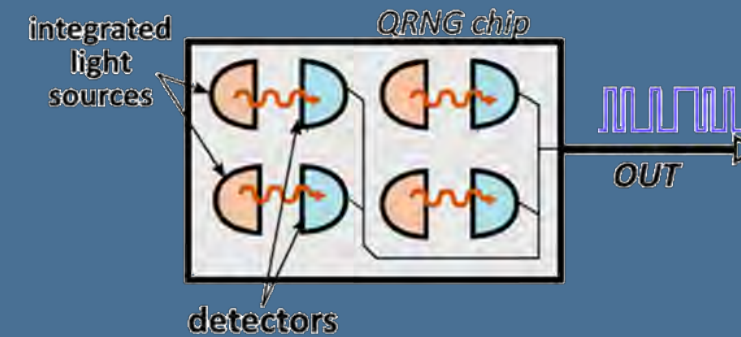


Evolution photonenemissionsbasierter QRNG-Konzepte

Von diskreten Bauelementen...



...zu lateral integrierten Emittlern und Detektoren...



[Acerbi et al., Structures and Methods for Fully-Integrated Quantum Random Number Generators, IEEE J. Sel. Top. Quantum Electron., vol. 26, no. 3, May/June 2020]

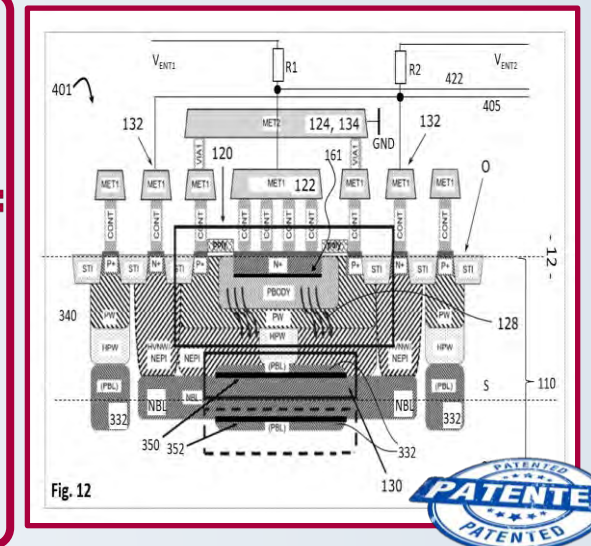
Der neue Ansatz von Elmos

- Vertikale Anordnung von Emittler und Detektor
- Monolithische Integration in Silizium-CMOS
- Basierend auf dem Elmos Automotive LIDAR SPAD Imager Vorteile
 - Extrem kleine Größe für höhere Kosteneffizienz
 - Höhere Bit-Rate durch kurze optische Weglänge
 - Schutz gegen Side Attacks durch zusätzliche Schaltungen
- Patentierte

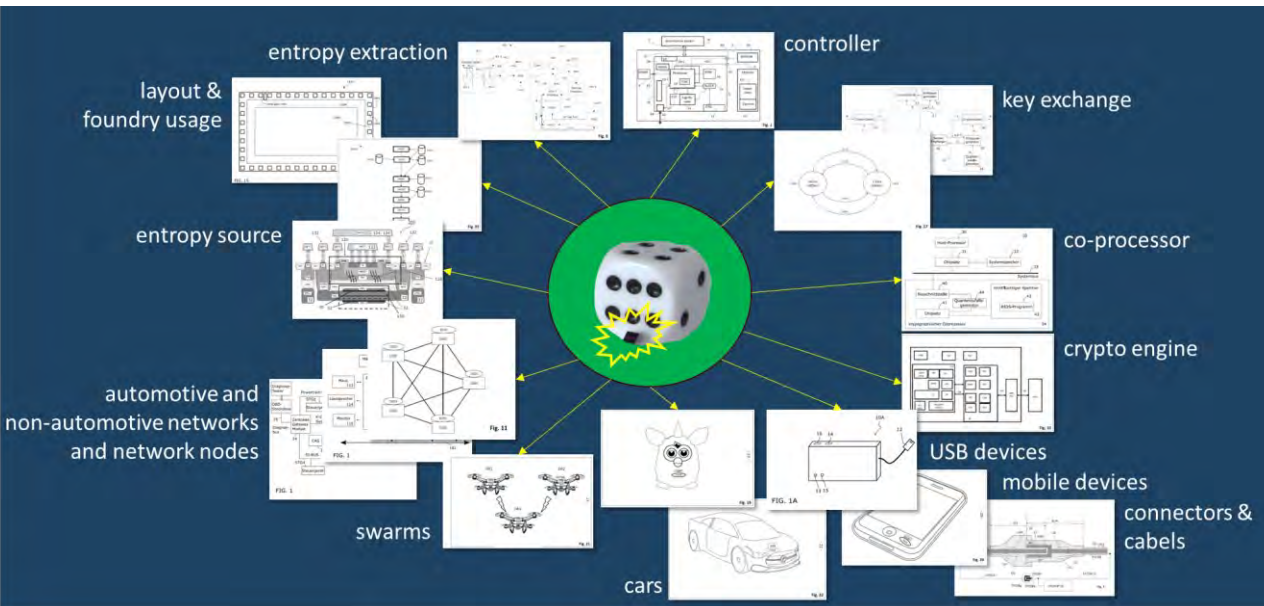
... hin zu einer vertikalen Anordnung von Emittler und Detektor



elmos[®]



Elmos IPs zu QRNG-Technologie (Patentsammlung)



Insgesamt **64 Patentanmeldungen**, darunter:

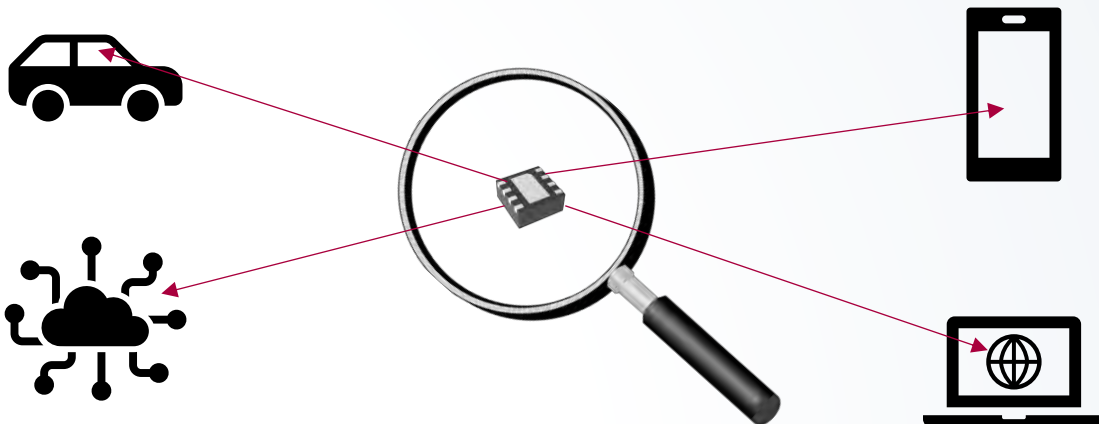
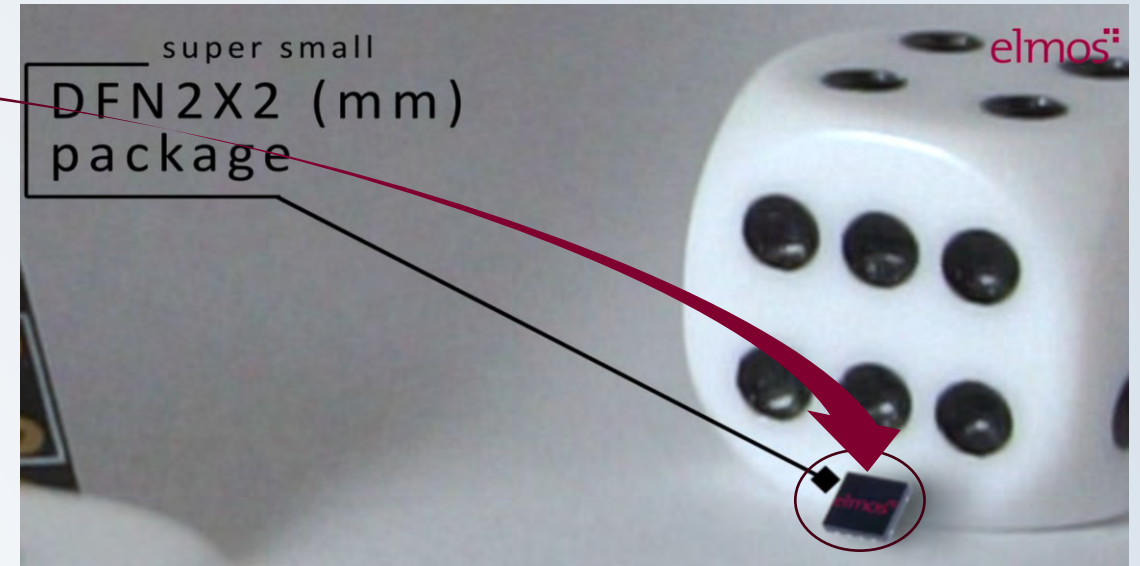
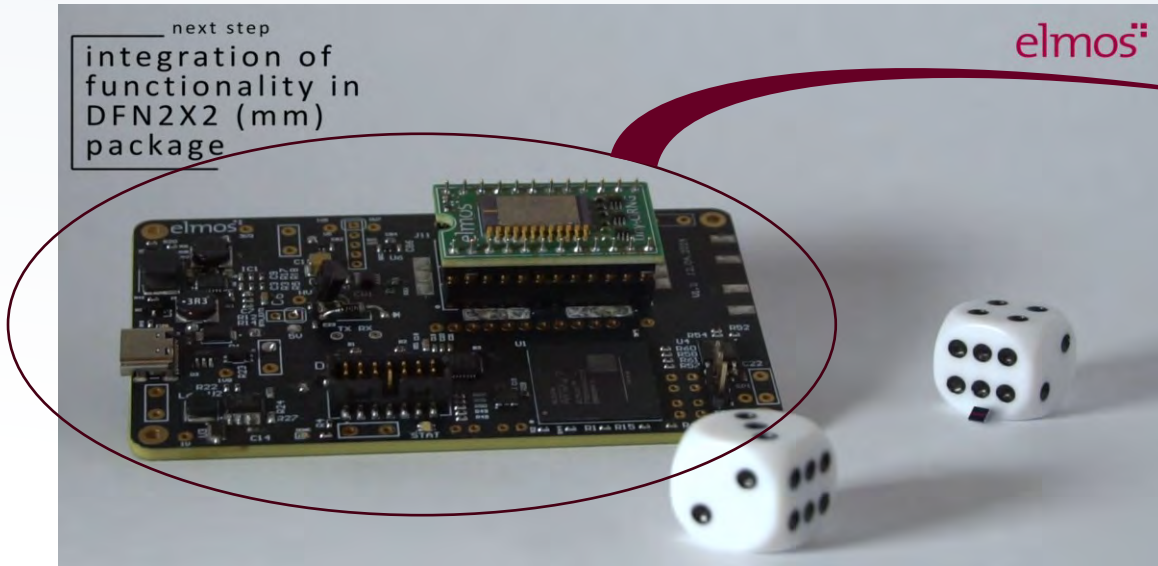
- 12 internationale PCT-Patente (vor Nationalisierung),
- 2 technologische Patente in Taiwan (TW),
- 1 Patent zum Eindringungsschutz (geheim / vertraulich).





simple readout
via COM port

Nächster Schritt: Vollintegration in ein kostengünstiges Gehäuse

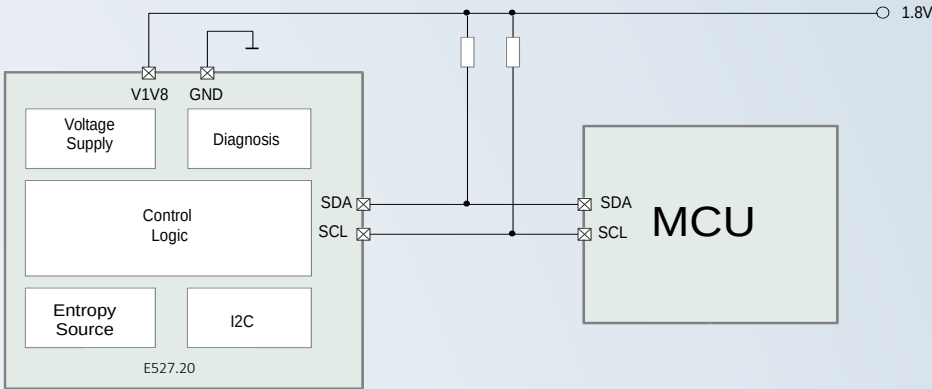


- ✓ Kleinster QRNG auf dem Markt
- ✓ Bestes Kosten-Leistungs-Verhältnis
- ✓ Ultra-niedriger Stromverbrauch
- ✓ Ultra-niedrige Betriebsspannung (geeignet für batteriebetriebene Geräte und IoT)
- ✓ Nachgewiesene Zufälligkeit mit Unterstützung von 
- ✓ Vielseitige Anwendungen: Automotive, Mobile, IoT, Kommunikation
- ✓ Muster ab 12/2025, SOP 2027

Elmos Embedded QRNG IC



Parameter	Elmos 527.20
QRNG Core	
Entspricht dem Standard NIST 800-90A/B/C Zufallstest	JA
AEC-Q100 Automotive Quality	JA
IC Integrationskonzept	monolithisch
Packungsgröße / Packungsvolumen	2 x 2 x 0.55 mm ³ = 2.2 mm ³
Entropiequelle optional skalierbar	500Kbps (basierend auf einer Entropiequelle) Skalierbar bis >>100 Mbps
STROMVERSORGUNG	
Eingangsspannung	1.8V / 3V / 5V
E/A-Schnittstellenspannung	1.8V / 3V / 5V
STROMVERBRAUCH	
Entropie aktiver Zustand	11mW
Energiesparmodus	70µW
BETRIEBSFREQUENZ & TEMPERATUR	
Maximale Nenn-Temperatur	-40°C ... +105°C
INTERFACE PROTOKOLL	
I2C	1MHz
KOSTEN	
USD / Einheit	Deutlich niedriger als bei anderen QRNG-Lösungen



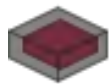
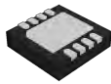
Der neue Elmos QRNG-IC bietet im Vergleich zu bestehenden Lösungen eine höhere Leistung und niedrigere Kosten bei geringerer Größe

Der gesamte Energieverbrauch ist im Vergleich zu TRNGs um bis zu 90 % reduziert

Lizenzoptionen:
Die monolithische QRNG-Lösung kann als eigenständiger IC oder als integrierbarer Funktionsblock für komplexere Designs (z. B. Mikrocontroller, Sensoren, Aktuatoren, Schnittstellenmodule) lizenziert werden

Integration der Elmos-Entropiequelle

Elmos QRNG als
eigenständiger Chip in
DFN2x2



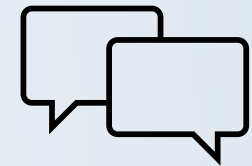
Elmos QRNG
als Chiplet



Lizenzübertragung der
monolithischen Lösung von
Elmos auf geeignete Fremd
(BCD-) Technologie



Andere Technologien
tbd.



A detailed image of a QRNG T809.54A chip. The chip is a square, blue silicon die with a complex circuit pattern. It is mounted on a blue printed circuit board (PCB) with several white surface-mount components. The chip is connected to a blue ribbon cable. A small, white, six-sided die is floating above the chip. The background is a blue, abstract, geometric pattern.

QRNG T809.54A

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

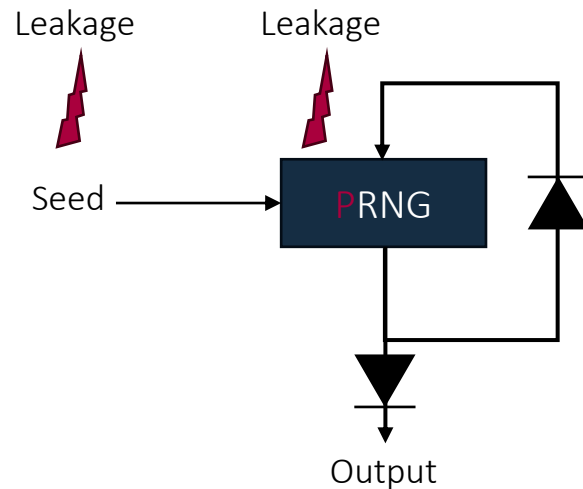
18.02.2026

Evolution of Random Number Generators

PRNG

Pseudo Random Number Generator

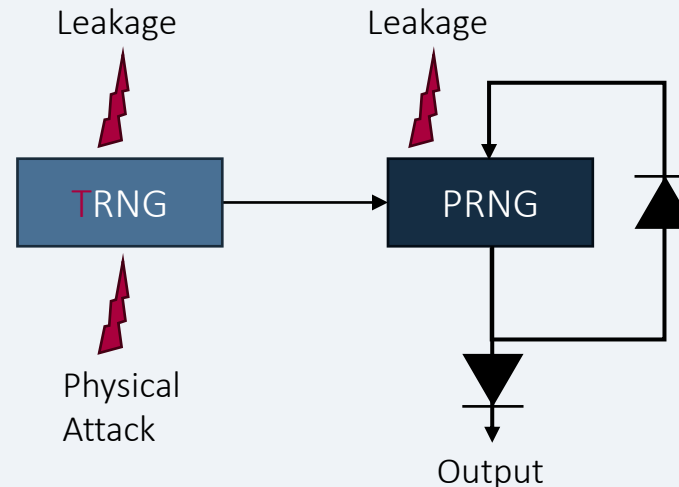
- Based on algorithm generating a number sequence from a random seed number
- **Deterministic**
- **Not truly random**
- **Predictable**



TRNG

True Random Number Generator

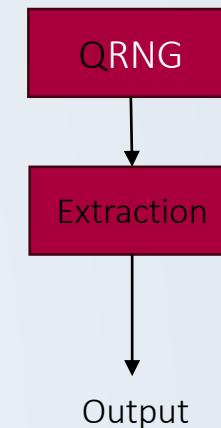
- Based on physical random effects
- **Non-deterministic**
- **Truly random**
- **Predictable (i.e. by AI based on math. models)**
- **Vulnerable by physical attacks (e.g. temp variation)**



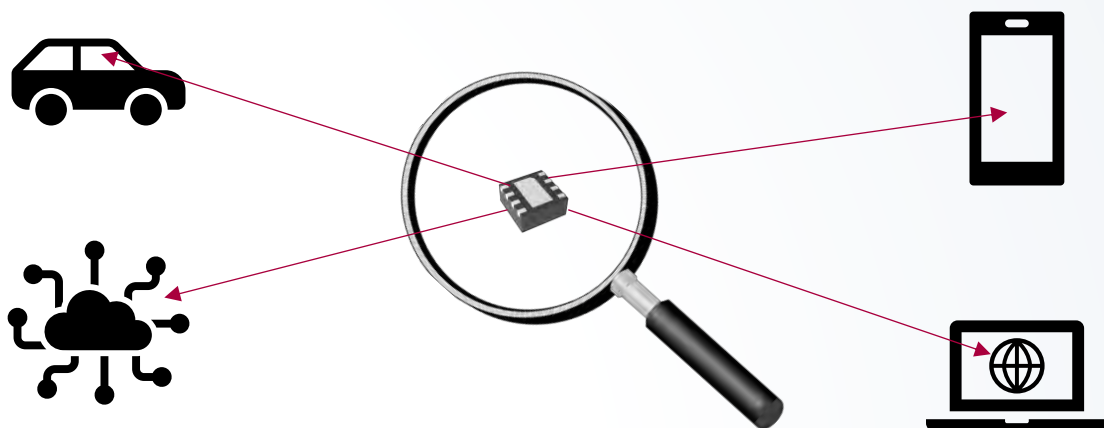
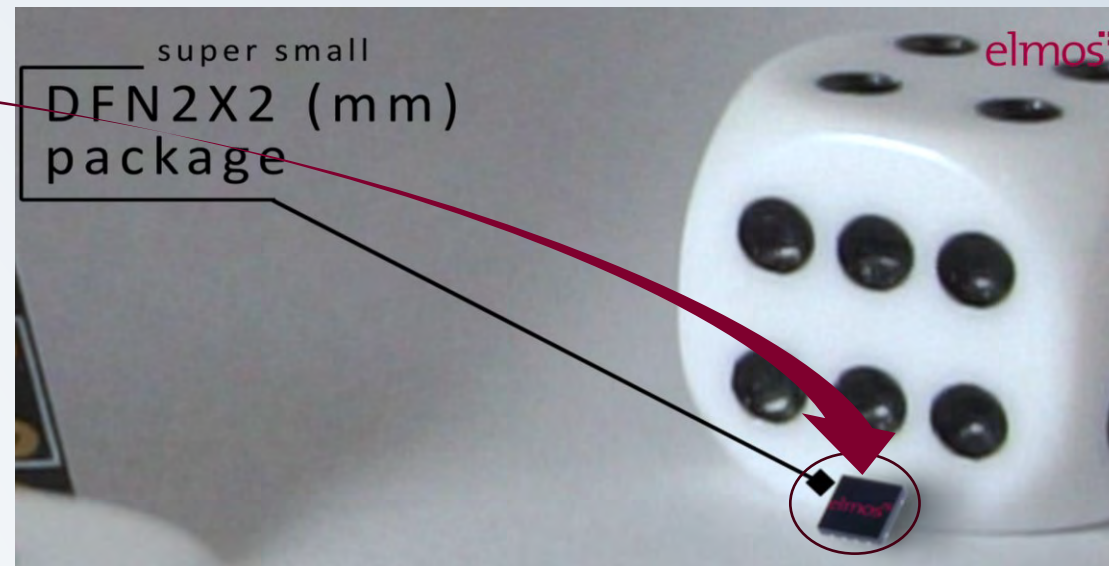
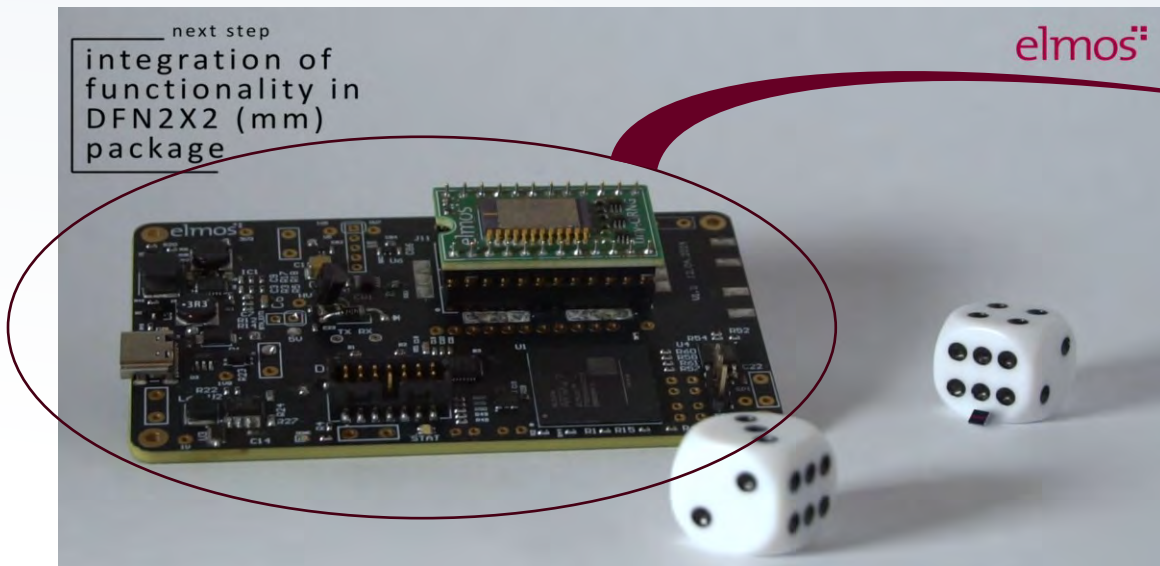
QRNG

Quantum Random Number Generator

- Based on Quantum random effects
- **Non-deterministic**
- **Truly random**
- **Non predictable (not even by QC/AI)**
- **Secure against physical attacks**



Next Step: Full Integration into low-cost package

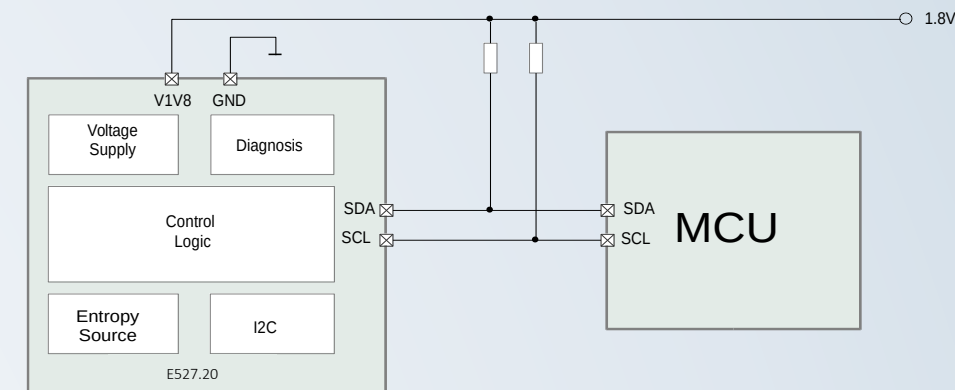


- ✓ Smallest QRNG in market
- ✓ Best cost/performance ratio
- ✓ Ultra low power consumption
- ✓ Ultra low voltage (for battery driven mobile devices / IoT)
- ✓ Randomness proven by IDQ
- ✓ Versatile applications (Automotive/Mobile/IOT/Comm)
- ✓ Samples 12/2025, SOP 2027

Elmos embedded QRNG IC



Parameter	Elmos 527.20
QRNG CORE	
Compliant to the Standard NIST 800-90A/B/C Randomnes Test	YES
AEC-Q100 Automotive Quality	YES
IC Integration Concept	1xComponent (monolithic)
Package Size / Package Volume	2 x 2 x 0.55 mm ³ = 2.2 mm ³
Entropy Source optionally scalable	1000Kbps (based on single entropy source) Scalable to >100 Mbps
POWER SUPPLY	
Single Input Voltage	1.8V / 3V / 5V
I/O Interface Voltage	1.8V / 3V / 5V
POWER CONSUMPTION	
Entropy out active	11mW
Power Down Mode	70μW
OPERATION FREQUENCY & TEMPERATURE	
Absolute maximum rated temperature	-40°C ... +105°C
INTERFACE PROTOCOL	
I2C	1MHz
Cost	
USD / unit	Significantly lower than other QRNG solutions



New Elmos QRNG IC provides higher performance @ smaller size and lower cost compared to existing solutions

The over all power consumption vs. TRNG is expected to be reduced by up to 90%

Licensable:

The Elmos monolithic QRNG can be made available as stand-alone IC or integrable block for higher level Designs (μC, Sensors, Actuators, Interface Nodes...)

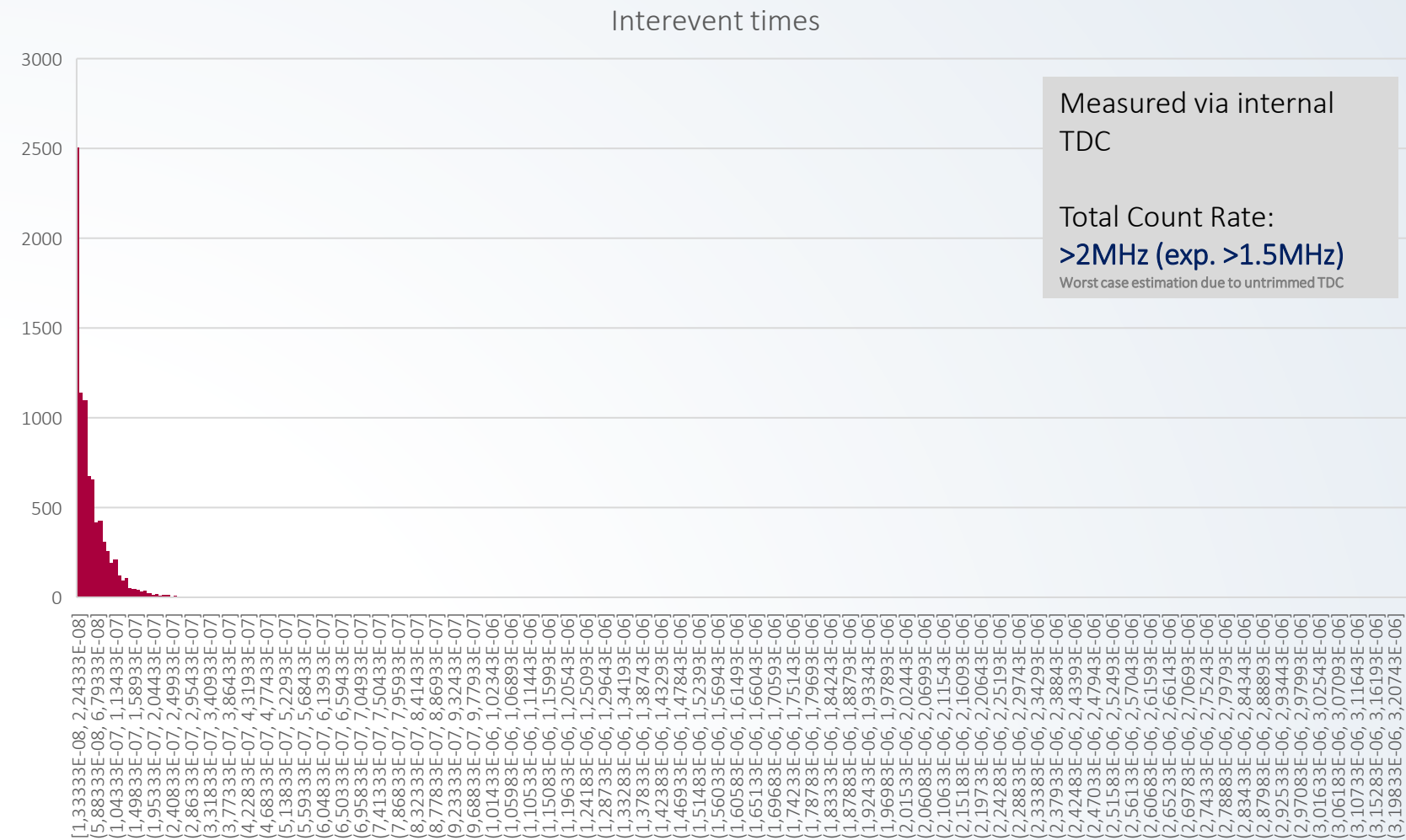
Old Elmos SPAD QRNG – advantages



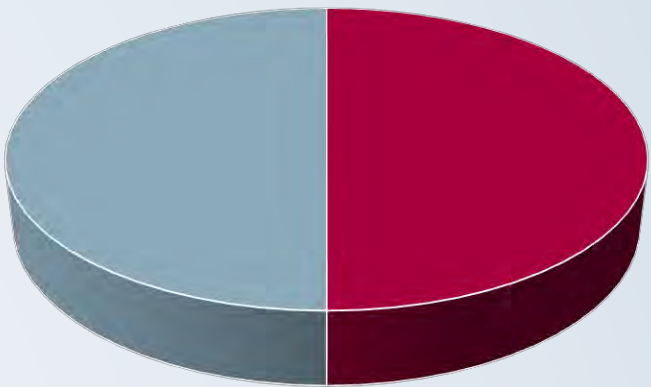
QRNG T809.54A



Initial Data



Distribution of Symbols

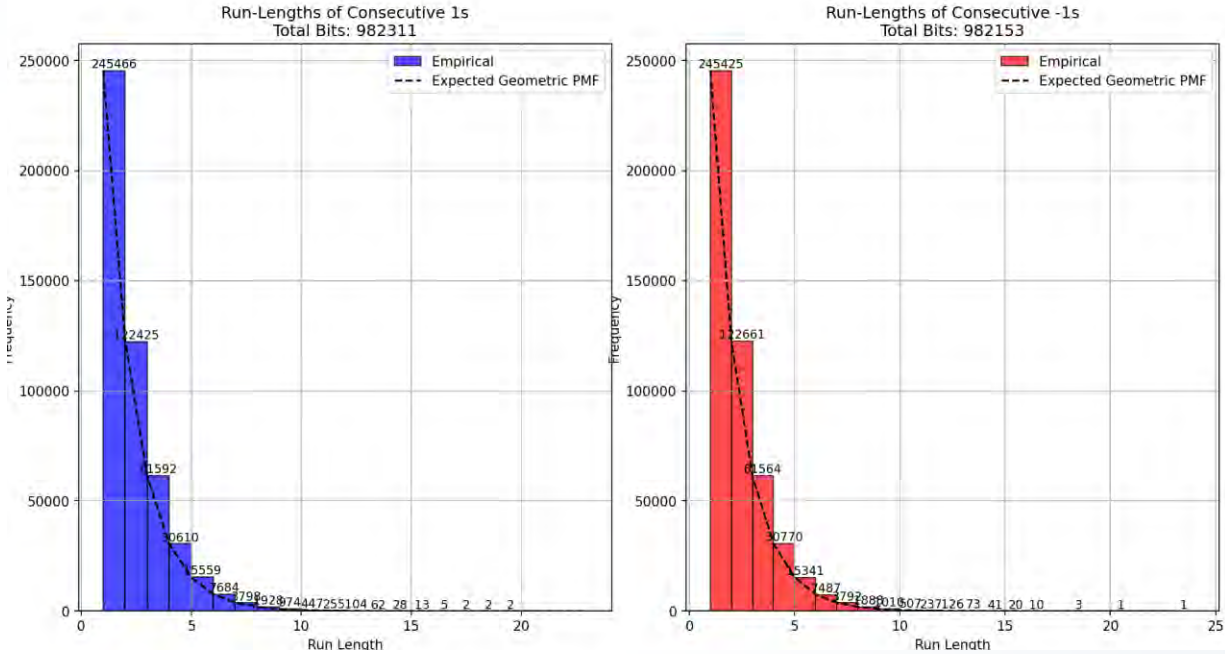


■ Number of 1's ■ Number of 0's

Number of 1's	982311
Number of 0's	982153

Sample #01
Chip-on-board
25°C | 3.3V | 1.5V
Trimmed: no
FFIN

Initial Data



NIST SP800-90A

Randomness Testing					
Test Type	P-Value	Result	Test Type	P-Value	Result
☒ 01. Frequency (Monobit) Test	0.574116019109665	Random	☒ 02. Frequency Test within a Block	0.7166651662080642	Random
☒ 03. Runs Test	0.9216814727831899	Random	☒ 04. Test for the Longest Run of Ones in a Block	0.7218040793381443	Random
☒ 05. Binary Matrix Rank Test	0.7824276572845231	Random	☒ 06. Discrete Fourier Transform (Spectral) Test	0.825684943208663	Random
☒ 07. Non-overlapping Template Matching Test	0.1630697463134299	Random	☒ 08. Overlapping Template Matching Test	0.9309668765596791	Random
☒ 09. Maurer's "Universal Statistical" Test	0.7399111335438552	Random	☒ 10. Linear Complexity Test	0.019625062444357008	Random
☒ 11. Serial Test	0.021572687969757802	Random		0.09923361412538134	Random
☒ 12. Approximate Entropy Test	0.6964951018448887	Random	☒ 14. Cumulative Sums Test (Backward)	0.4918982681199138	Random
☒ 13. Cumulative Sums Test (Forward)	0.17050116173551502	Random			
☒ 15. Random Excursions Test					
State Chi^2 P-Value Result					
-4 2.911489205526148 0.7136294456453369 Random					
☒ 16. Random Excursions Variant Test					
State Count P-Value Result					
-9.0 782 0.6205480473200617 Random					

Min. Entropy Test - IID Test

Dataset	H_original	H_bitstring	Min-Entropy	IID-checks
1Mbit	7.880293	0.998228	7.880293	Passed
2Mbit	7.914982	0.998754	7.914982	Passed
3Mbit	7.925600	0.997951	7.925600	Passed

- H_original
 - How unpredictable is each byte.
 - The closer the value is of 8, the better
- H_bitstring
 - How unpredictable are the bits.
 - The closer the value is to 1, the better.
- Min-Entropy
 - More pessimistic estimation, this should be treated as a conservative response to the tool.

Test Suite:
https://github.com/usnistgov/SP800-90B_EntropyAssessment

Power Consumption



Test sequence after reset to measure event rate								
SET Register	Register	Register description	Current SUP3V3	Current SUP1V5	V_TEST1	V_TEST2	F_TEST1	F_TEST2
Start up			0,65mA	225,2uA	0,1mV	0,1mV	0	0
SET 0x30 0x00	TREF_CTL_OSC8M_TRIM	Sets the 8 MHz oscillator trim to nominal	0,78mA	314,6uA	0,1mV	0,2mV	0	0
SET 0x44 0x03	SUP_REF_CTL_BG_TK_ADJ	Trim 011: 3 steps more positive TK	0,77mA	314,2uA	0,1mV	0,2mV	0	0
SET 0x21 0xD3	QRG_CTRL_QRGC_TRIM_I_ZD	Trims IZD Zener diode current	0,75mA	313,6uA	0,1mV	0,2mV	0	0
SET 0x22 0x0e	QRG_CTRL_QRGC_TRIM_SPAD_OV	Set SPAD overvoltage (VOV)	0,75mA	313,6uA	0,1mV	0,2mV	0	0
SET 0x33 0x07	TREF_CTL_TMR_SEL		0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x70 0x00	TST_CTL_TMR_VAL_ATBMUX_1	Disables all ATBUS connections	0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x23 0x00	QRG_CTRL_QRGC_TMR_ANA1	Disables all analog test muxes	0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x72 0x04	TST_CTL_TMR_VAL_PAD_TEST1	Enable TEST1 output	0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x73 0x04	TST_CTL_TMR_VAL_PAD_TEST2	Enable TEST2 output	0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x75 0x10	TST_CTL_TMR_OUT_TOP		0,50mA	52,61uA	0,1mV	0,1mV	0	0
SET 0x25 0x03	TDC_TMR_OUT	Enables TDC outputs to testbus	1,2mA	53,23uA	3,209V	128,14mV	2,6151Mhz	2,6157Mhz
SET 0x72 0x00	TST_CTL_TMR_VAL_PAD_TEST1	Disables TEST1 output	1,2mA	53,23uA	3,227V	357,74mV	2,588Mhz	2,584Mhz
SET 0x73 0x00	TST_CTL_TMR_VAL_PAD_TEST2	Disables TEST2 output	0,50mA	53,23uA	0,1mV	0,1mV	0	0

Initial Power Consumption
w/o trimming

Extra Load from Test Pins
during trimming

Final Power Consumption:
~1,75mW
@2.5MHz Eventrate, excl.
I2C Communication



elmos[®]

Side Channel Protection

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

18.02.2026

Overview: Signal Path and Side Attack Diagnosis

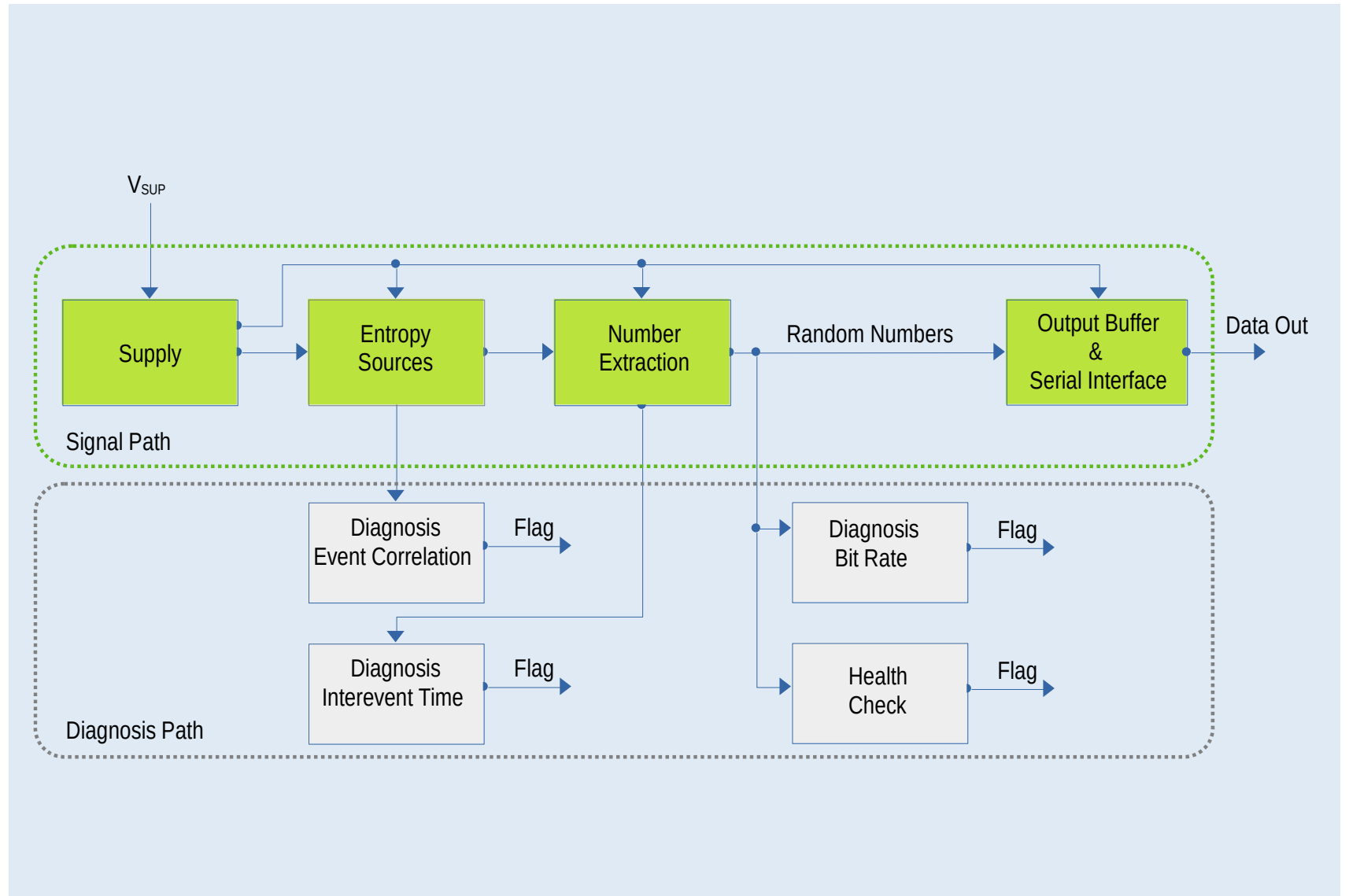
Elmos implements various counter-measures to all potential attacking vectors into:

■ Signal Path

- Separate supply generation of the entropy source digital signal processing
- Entropy source generating random events
- Number extraction generates random bits out of the random events

■ Diagnosis Path

- Dedicated diagnosis start at different points of the signal path



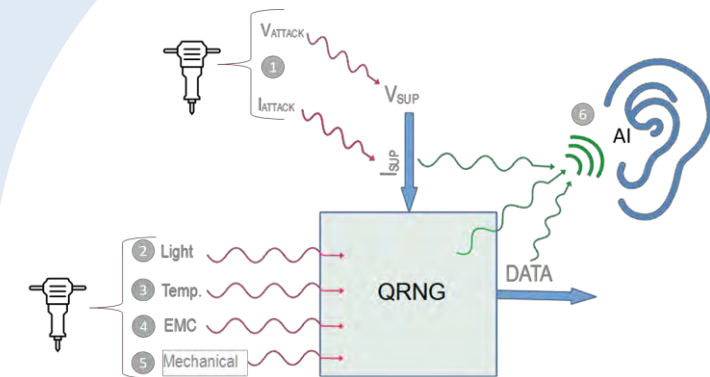
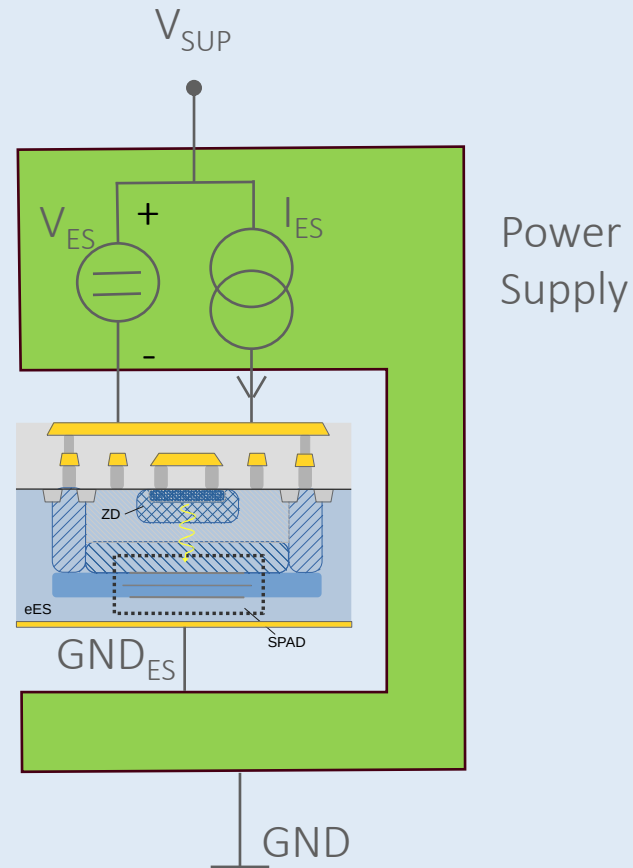
1 Side Attack via Power Supply

Attack

- Variation of supply voltage or current

Elmos QRNG Solution

- Power supply of the entropy source encapsulated by an internal power supply module
- Disturbance of V_{SUP}
 - No impact to the entropy due to decoupling
 - Only influence on the bit rate
 - Diagnosis on bit rate detects effects of V_{SUP} disturbances



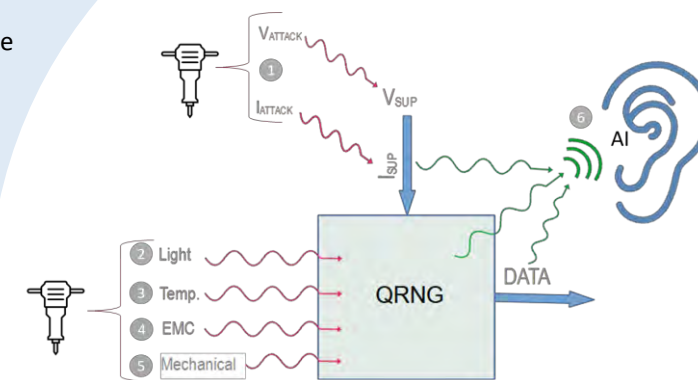
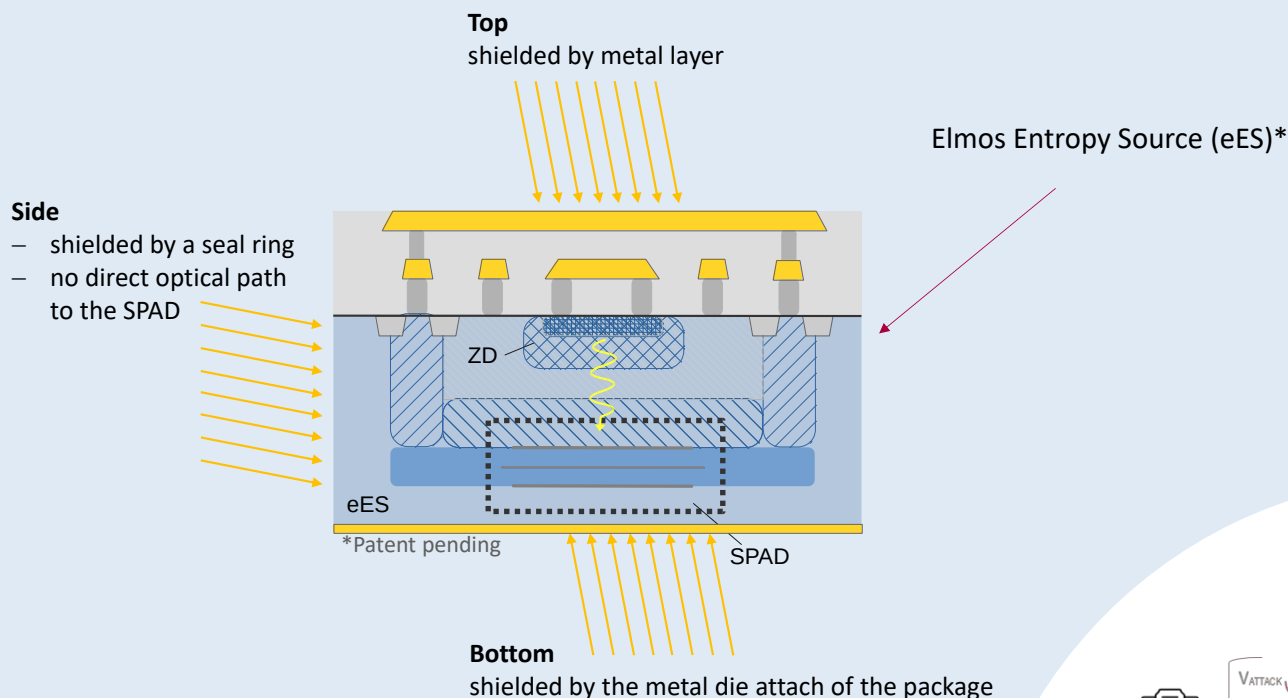
2 Optical Side Attacks on Entropy Source

Attack

- Variation of light by top / bottom or side impact

Elmos QRNG Solution

- Top
 - Metal layer shield
- Bottom
 - Metal die pad package
- Side
 - Seal ring
 - The surrounding circuits will block a direct optical path to entropy source

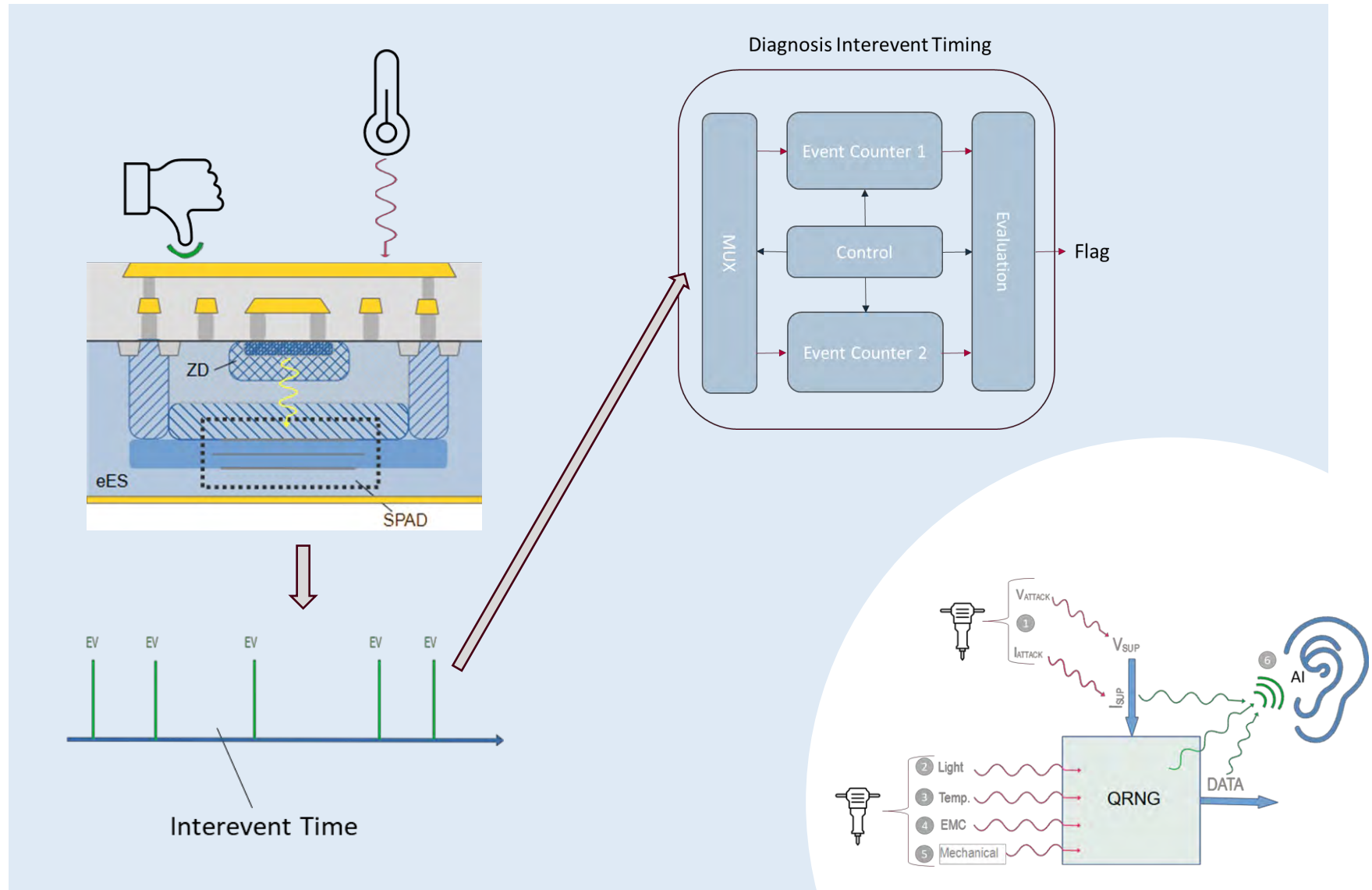


Attack

- Physical impact by variation of:
 - Pressure
 - Temperature

Elmos QRNG Solution

- Calculation the gradient of the interevent times:
 - Comparing the number of events of two or more consecutive, identical time windows



Cybersecurity Robustness Elmos QRNG

Attack

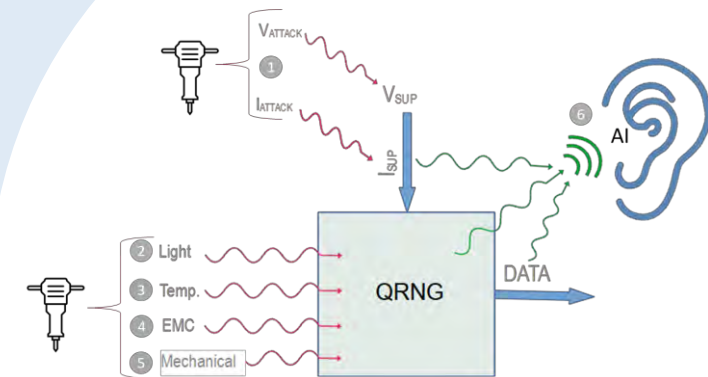
- Manifold physical attack vectors are possible

Elmos QRNG Solution

- Robust measures are integrated to prevent from any possible physical attacks



#	Attack	Bit Rate Monitor	Ambient Light PD	Event Correlation	Inter Event Timing Monitor	Health Check	Embedded Entropy Source	Cybersecurity Robustness
1	Voltage & Current	✓						✓
2	Light		✓	✓		✓	✓	✓
3	Temperature	✓			✓			✓
4	EMC			✓		✓		✓
5	Mechanical				✓			✓
6	Listening (AI)						✓	✓



The background of the slide is a 3D rendering of a blue microchip. The chip has a grid of pins around its perimeter and a complex circuit pattern on its surface. The "elmos" logo is printed in white on the chip. Above the chip, a small white die with black pips is shown in a floating position. Several bright blue light beams emanate from the chip, creating a high-tech, futuristic atmosphere.

Robustheit gegen physische Angriffe

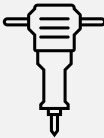
True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

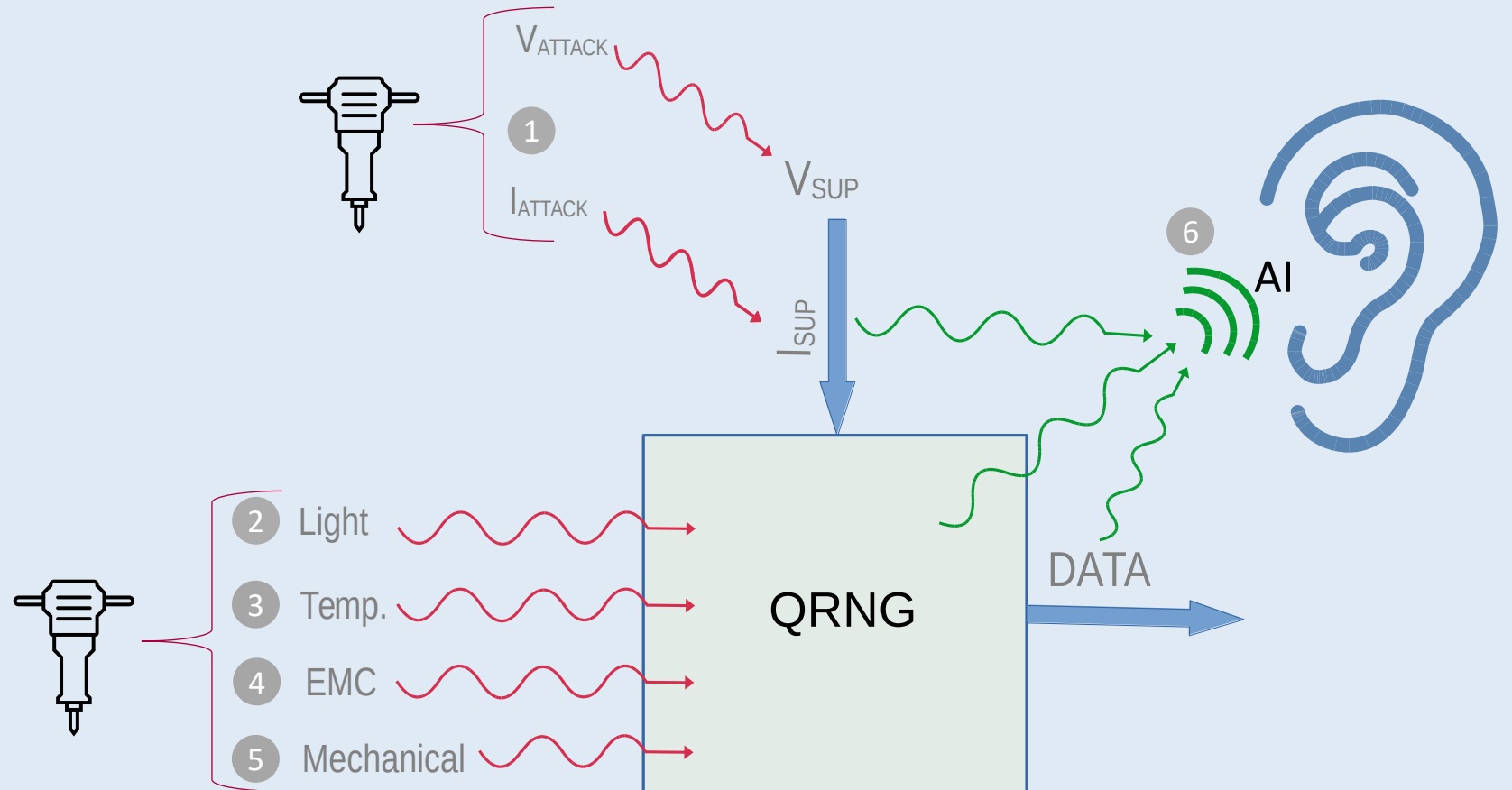
18.02.2026

Szenarien für physikalische Hacker Angriffe

Arten der Manipulation

- Physikalischer Eingriff 
- Vorhersage Output 
- Es gibt verschiedene physische Angriffsmöglichkeiten auf RNG. :

- 1 Stromversorgung
- 2 Licht
- 3 Temperatur
- 4 EMC
- 5 Mechanisch
- 6 KI



Inherent Cybersecurity Robustness Elmos QRNG

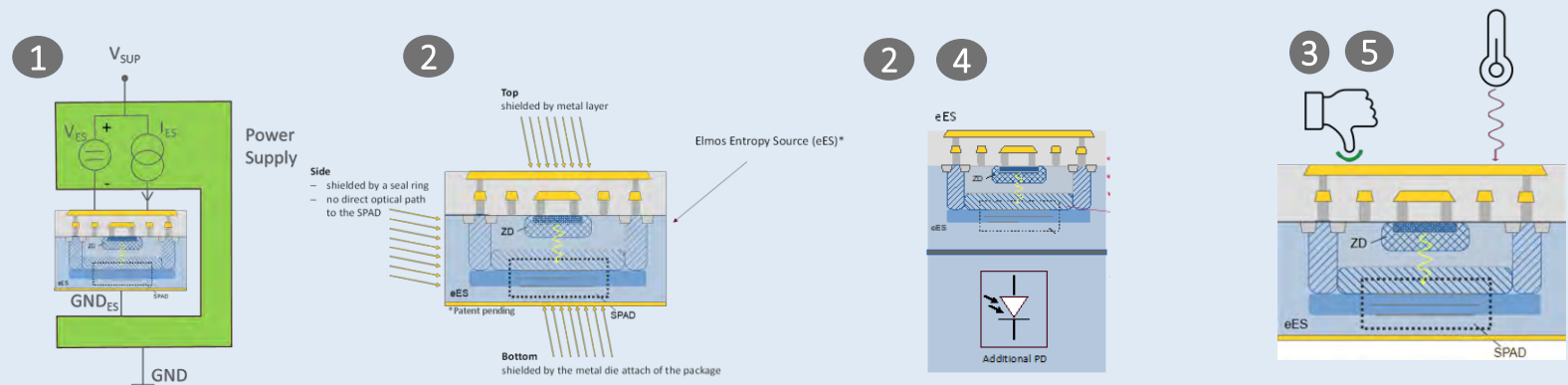
Cybersecurity

- Verschiedenste physikalische Angriffsvektoren möglich

Elmos QRNG Lösungen

- Integrierte Robustheitsmaßnahmen schützen vor möglichen physischen Angriffen
- Dedizierte Diagnoseschaltungen für inherente Robustheit
- Gekapselte Stromversorgung.
- Metall Schirmung und Seal Ring
- Komparator schnell / langsam

#	Attack	Bit Rate Monitor	Ambient Light PD	Event Correlation	Inter Event Timing Monitor	Health Check	Embedded Entropy Source	Cybersecurity Robustness
1	Voltage & Current	✓						✓
2	Light		✓	✓		✓	✓	✓
3	Temperature	✓			✓			✓
4	EMC			✓		✓		✓
5	Mechanical				✓			✓
6	Listening (AI)						✓	✓



Energieeffizienz



elmos[®]

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

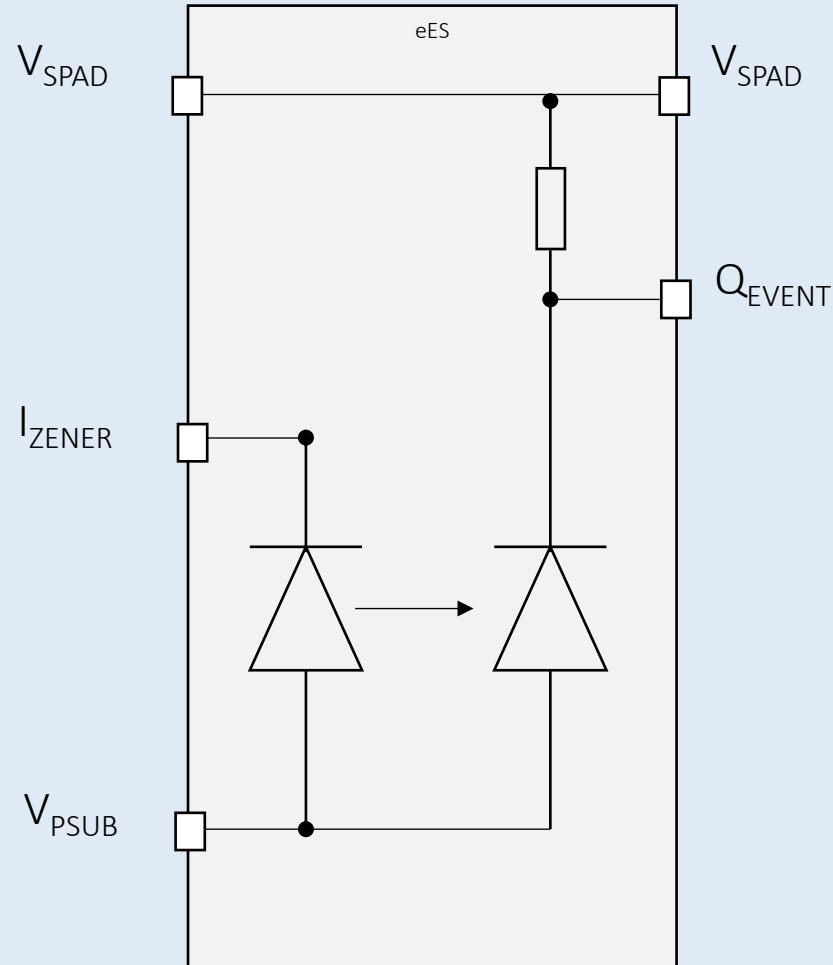
Dr. Bernd Burchard

18.02.2026

Leistungsaufnahme der Entropiequelle

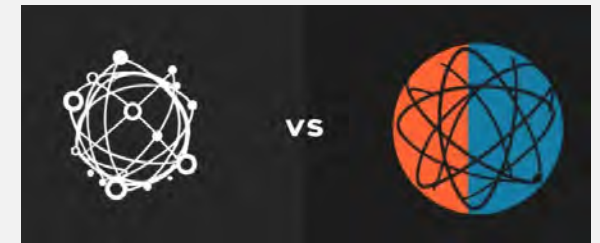
Power Consumption

- Photonenquelle
 - DC stimulus Strom
 - $P_{TX,DC} = U_{Zener} * I_{Zener}$
 - $P_{TX,DC,typ} = 34\mu W$
- Photonen-Detektor
 - AC-Ladung/Entladung der internen Kapazität
 - $P_{RX,AC} = C * U_2 * f$
 - $P_{RX,AC,typ} = \sim 1.5\mu W$
- Gesamt
 - Nur $35.5\mu W$



QRNG vs. TRNG

- Der Energieverbrauch des QRNG liegt im Mittel etwa 10-mal niedriger als bei vorhandenen TRNGs:
 - 100x niedriger als OPTIGATM TPM
 - 10x niedriger als SAKURA-X





elmos[®]

Entropie-Verfügbarkeit

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

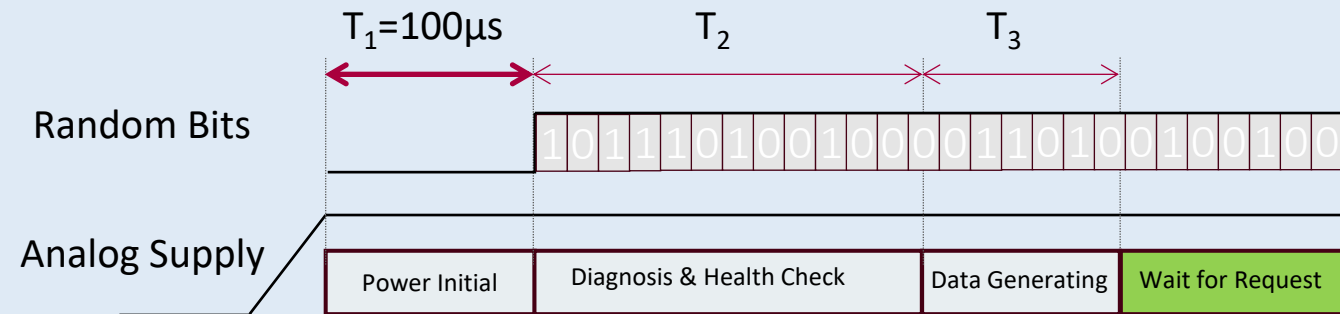
Dr. Bernd Burchard

18.02.2026

Entropie-Verfügbarkeit / Aufwärmphase

Entropiequelle

- Entropie und Bitstrom stehen sofort nach nur **100 μ s** bereit.
- Die Erzeugung zufälliger Bits startet nach T_1
- Zeiten T_2 und T_3 sind implementationsabhängig



Parameter	T_{typ}
Power Initial Time (T_1)	100 μ s
Diagnosis & Health Check Time (T_2)	500 μ s-1ms*
Data Generating (T_3)	50 μ s*

*Timings T_2 and T_3 are depending on the IC implementation

Zertifizierung der Zufälligkeit

True Random, Truly Secure:
Quantum Technology for Next-Gen
Automotive Systems“

Dr. Bernd Burchard

18.02.2026



- Interne Vorabbewertung der Zufälligkeit mit positivem Ergebnis durchgeführt
- Elmos wird die Zertifizierung des Endprodukts durch akkreditierte Stellen (z.B. **TUVIT**) organisiert durch **IDQ**

gemäß den etablierten Standards vornehmen lassen:

- NIST (ESV) IID SP800-90B
- NIST FIPS 140-3 (in integrierten Lösungen) basierend auf ESV #63 unter Verwendung des NIST CMVP
- BSI AIS31
- Für Automobilanwendungen führen wir eine AEC Q 100-Freigabe einschließlich abschließendem PPAP durch
- Während unser QRNG sicherlich die bestehenden (TRNG-basierten) Standards erfüllen wird, sind wir zuversichtlich, dass er auch die zukünftig verschärften Standards in Bezug auf die Quantenbedrohung erfüllen wird.





Zusammenfassung / Q & A

- Cybersicherheit benötigt echte Zufallszahlen
- QRNG ist zukunfts-sichere Lösung
- Elmos präsentiert den weltweit kleinsten und kosteneffizientesten QRNG-IC, der herkömmliche TRNGs deutlich übertrifft :
 - ~10x weniger Leistungsaufnahme
 - ~10x kürzere Startzeit
 - ~10x kleinere Chipgröße

Zusätzlich robuster gegen physische / KI-Angriffe und Alterung

- Muster verfügbar, SOP 2027
- Risikominderung im Bereich Cybersicherheit für die Zukunft + schon jetzt unmittelbare Vorteile

Wir laden Sie herzlich zur Live-Demonstration und weiterführenden Fachgesprächen ein

elmos[®]





IPCEI Microelectronics and
Communication Technologies

elmos[®]

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



**Funded by
the European Union**
NextGenerationEU

Ministerium für Wirtschaft,
Industrie, Klimaschutz und Energie
des Landes Nordrhein-Westfalen



Baden-Württemberg

MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Danksagung

Teile der Arbeit werden im Rahmen des IPCEI Mikroelektronik und Kommunikation vom BMWK auf Grundlage eines Beschlusses des Deutschen Bundestages, von der Europäischen Union im Rahmen von „NextGenerationEU“, vom Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen, vom Senatsdezernat für Wirtschaft, Energie und der öffentlichen Unternehmen, vom Ministerium für Wirtschaft, Arbeit und Tourismus des Landes Baden-Württemberg auf Grundlage eines Beschlusses des Landtags Baden-Württemberg und vom Ministerium für Wirtschaft, Arbeit und Energie des Landes Brandenburg

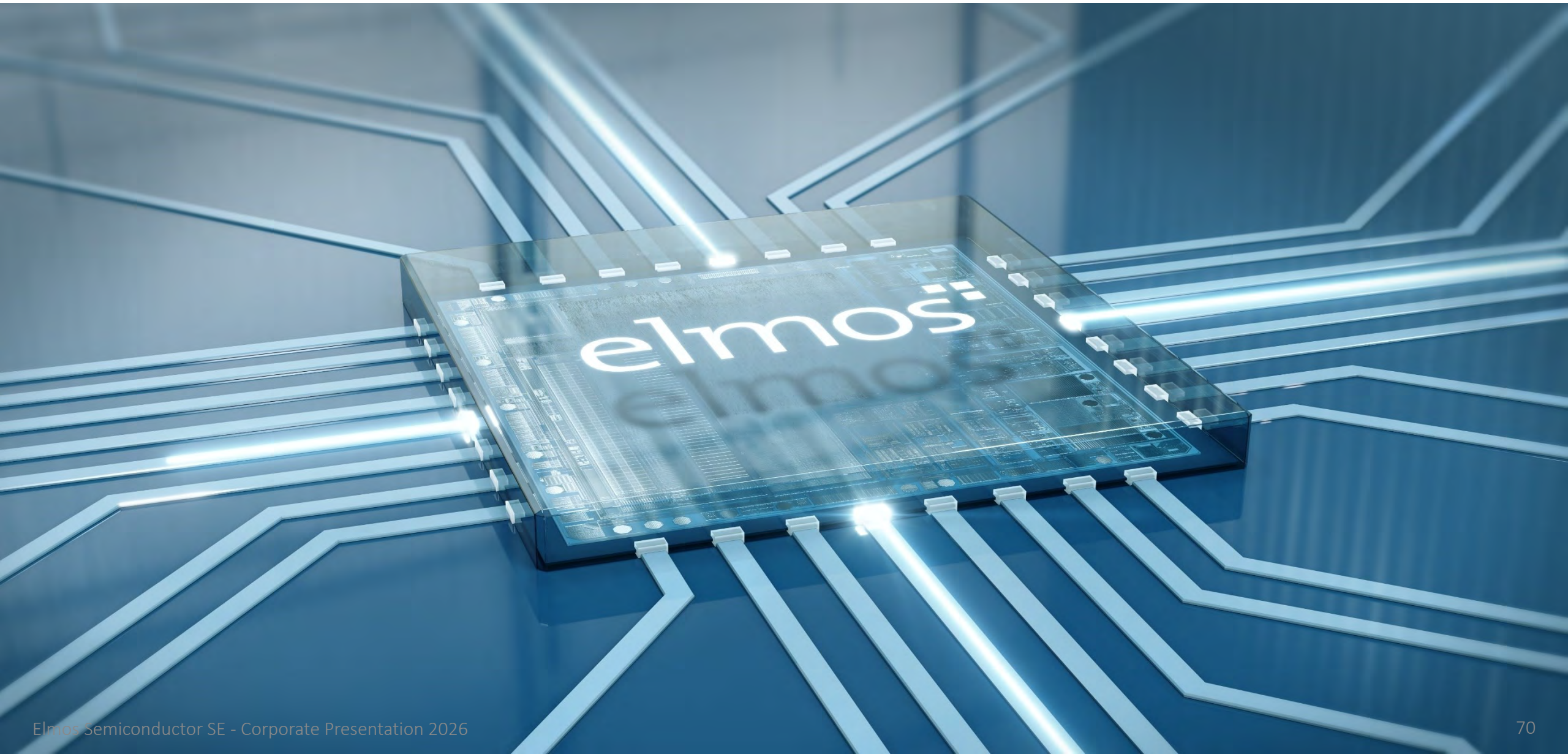
Mit Elmos QRNG für die Zukunft der Cybersicherheit gerüstet

elmos[®]



Thank You

elmos[®]



DISCLAIMER

This presentation contains forward-looking statements based on beliefs of Elmos' management. Such statements reflect the company's current views with respect to future events and are subject to risks and uncertainties. Many factors could cause the actual results to be materially different, including, among others, changes in general economic and business conditions, changes in currency exchange rates and interest rates, introduction of competing products, lack of acceptance of new products or services and changes in business strategy. Actual results may vary materially from those projected here. Elmos does not intend or assume any obligation to update these forward-looking statements.

Elmos Semiconductor SE

Werkstättenstraße 18 | 51379 Leverkusen | Germany | www.elmos.com

elmos[®]

