Cyber-Sicherheit

Schiffsantriebe und -überwachungssysteme

Dr. Stefan Ihmor, Dr. Andreas Pilz

27.06.2018

20. Symposium Verbindungen

„Informations-Sicherheit in Zeiten von WhatsAPP und Co!“

Rolls-Royce

Motivation – MTU Lieferumfang

„Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein.

Sicherheitsexperte Gene Spafford

VERTRAULICH

Rolls-Royce

Sicherheit (Security) Motivation

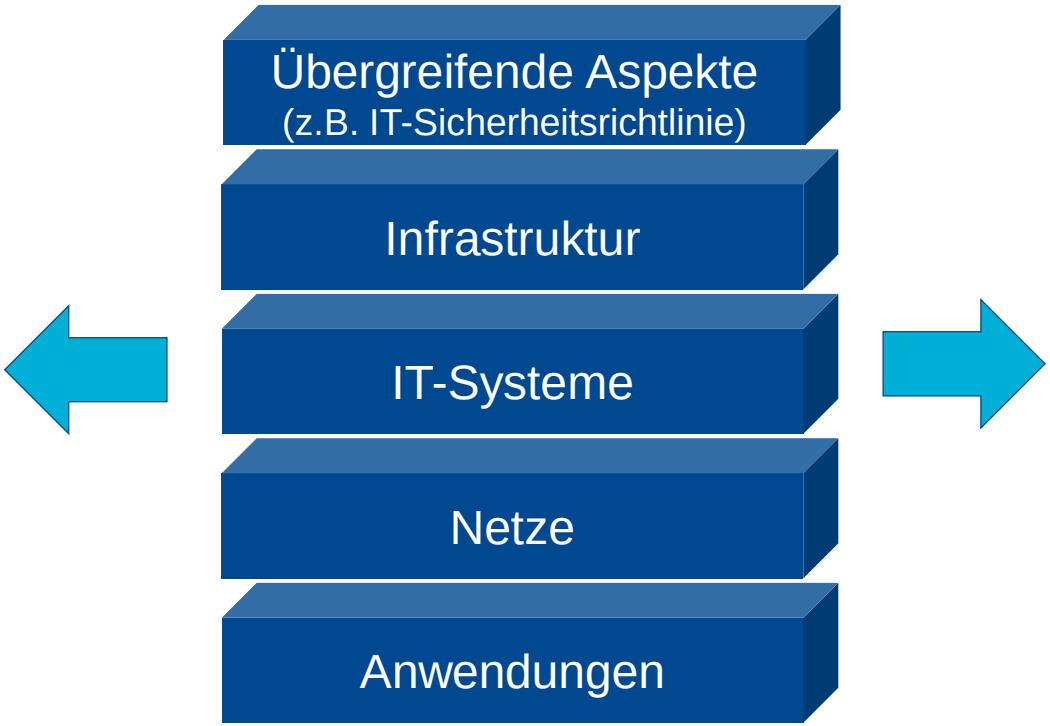
- Motivation
- Sicherheit bei MTU
- IT-Sicherheitskonzepte
- Sicherheit der MTU Produkte
- Sensibilisierung der Mannschaft
- Zusammenfassung

VERTRAULICH

Rolls-Royce

Sicherheit bei MTU
MTU interne Organisation und MTU Produkte

MTU-interne Organisation bzw. Infrastruktur



MTU Produkte inkl. Life-Cycle (MTU Liefer-umfang)

➔ **Keine sicheren Produkte ohne sichere Infrastruktur!**

VERTRAULICH

Rolls-Royce

Sicherheit (Security) Motivation

- Motivation
- Sicherheit bei MTU
- IT-Sicherheitskonzepte
- Sicherheit der MTU Produkte
- Sensibilisierung der Mannschaft
- Zusammenfassung

Orientierungsrahmen

Normen / Standards für IT-Sicherheit

- ISO27001 (IT-Grundschutz ggf. zum Nachweis)
- SANS CSC 20 – CPNI
- CyberEssentials (UK) → aktuell CyberEssentials Plus Zertifikat erhalten
- US Cyber Security Framework
- C5 für Cloud Computing

Cyber Security in der zivilen Schifffahrt

- Rules Klassifikationsgesellschaften
  z.B. DNVGL-RP-0496 “Cyber security resilience management …”
- Gründung **IACS Cyber Security Panel**
- **IEC 62443** Industrial communication networks - Network and system security

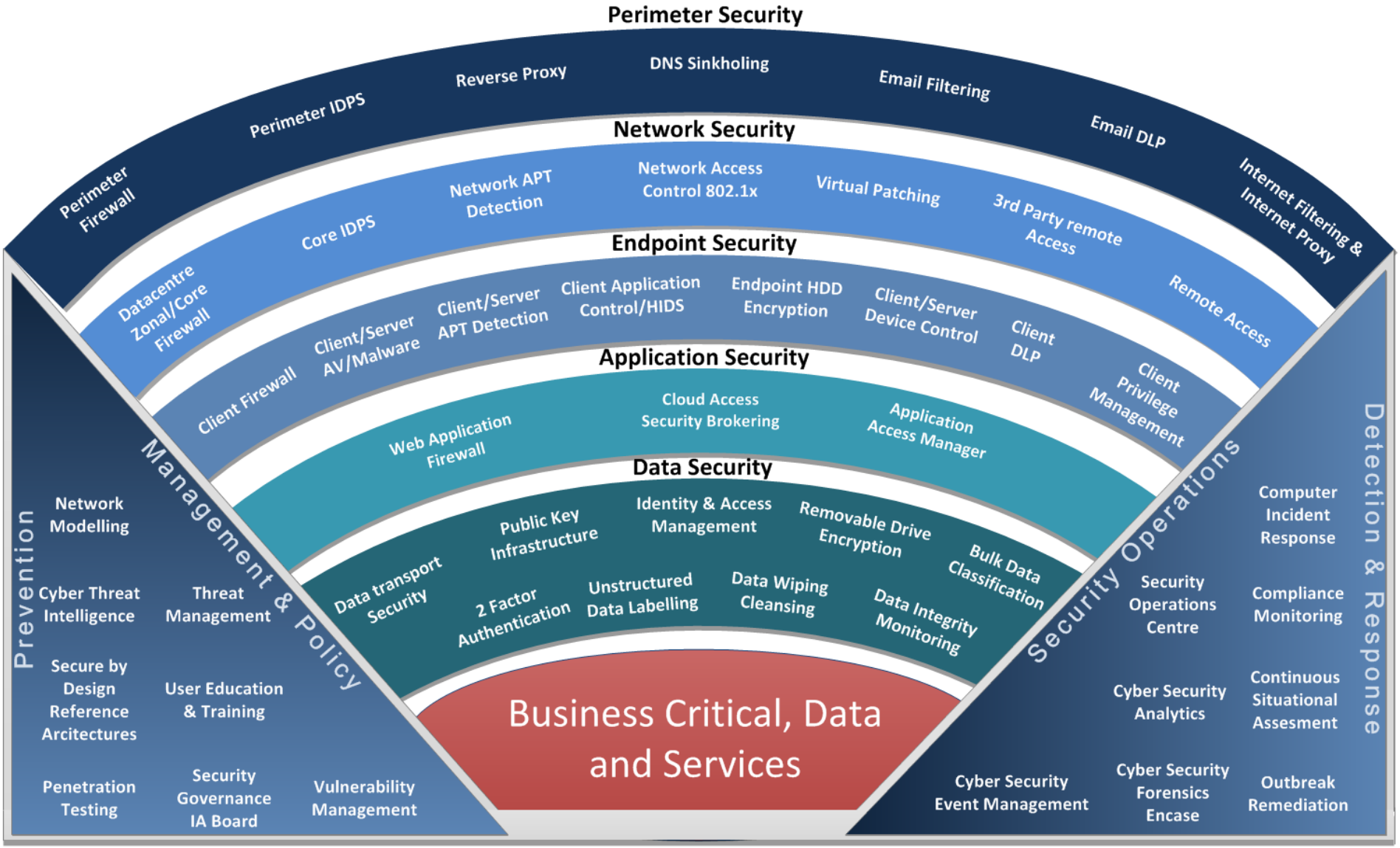
Leitprinzipien der IT-Sicherheit bei Rolls-Royce Power Systems AG

Ansätze für die Sicherstellung der IT-Sicherheit

- Business driven
- Defence in depth
- Assume Breach
- Risiko-basierend
- Kronjuwelen-Ansatz
- Compliance driven
- Continuous improvement

IT-Sicherheit – Technologie, Prozesse, Organisation

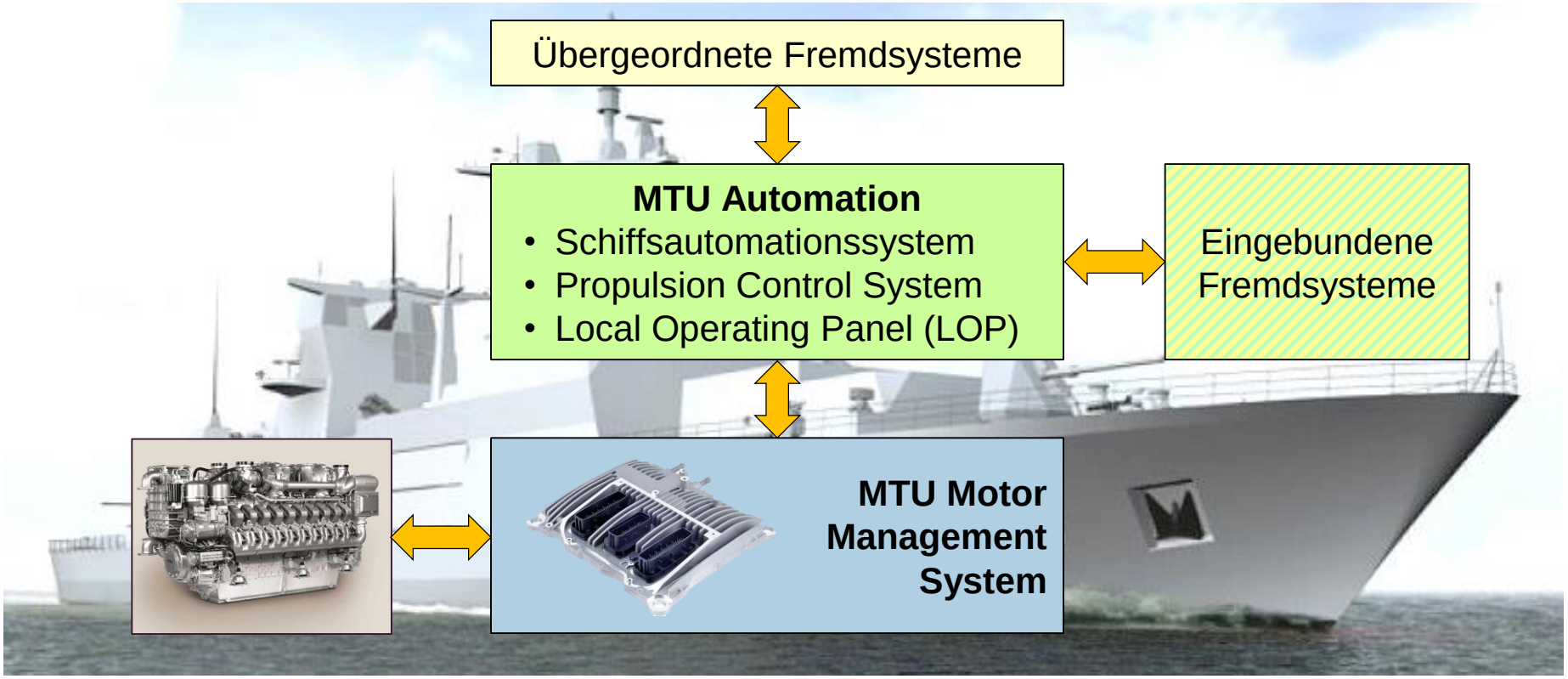
Rolls-Royce Power Systems AG



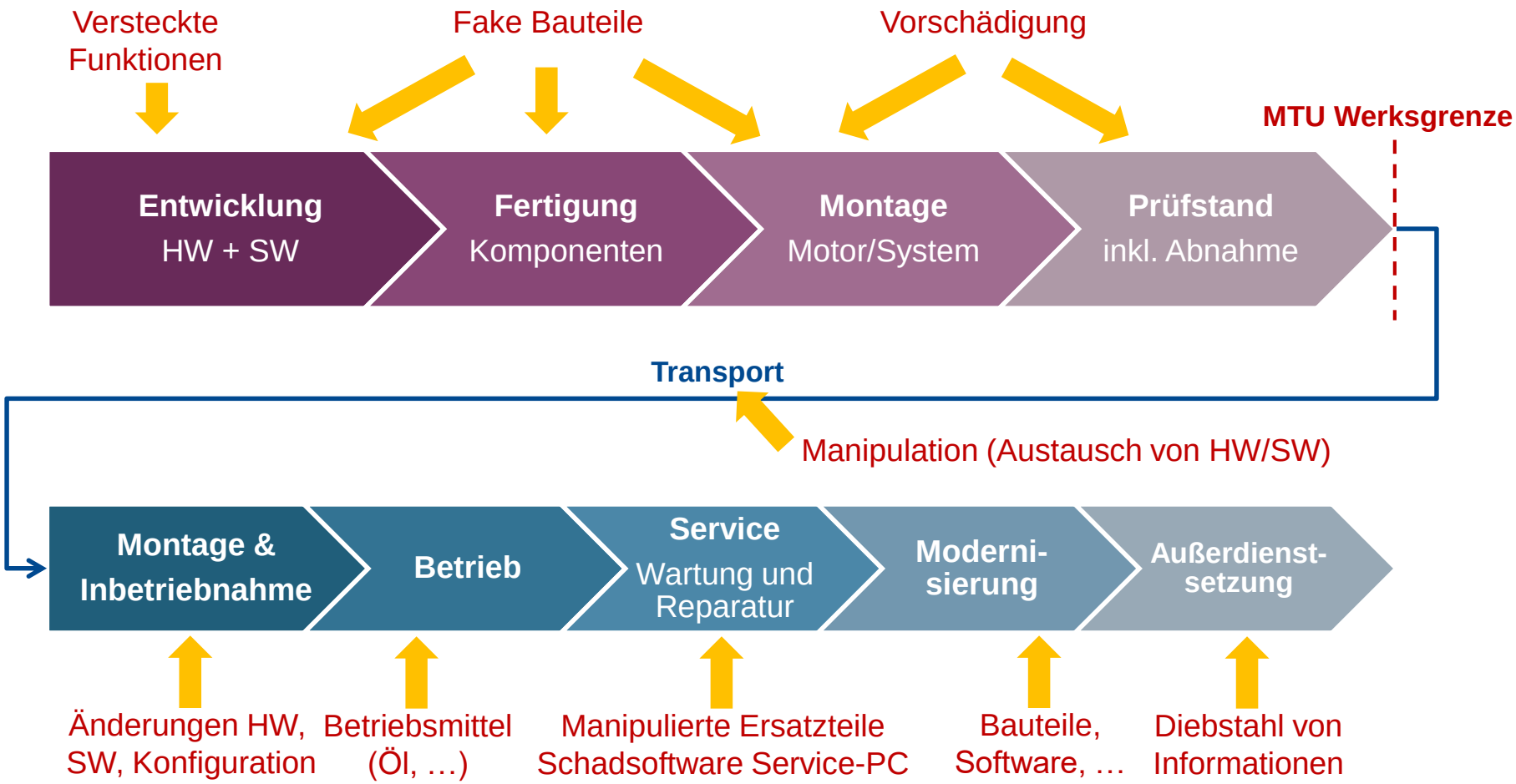
Sicherheit (Security)
Motivation

- Motivation
- Sicherheit bei MTU
- IT-Sicherheitskonzepte
- Sicherheit der MTU Produkte
- Sensibilisierung der Mannschaft
- Zusammenfassung

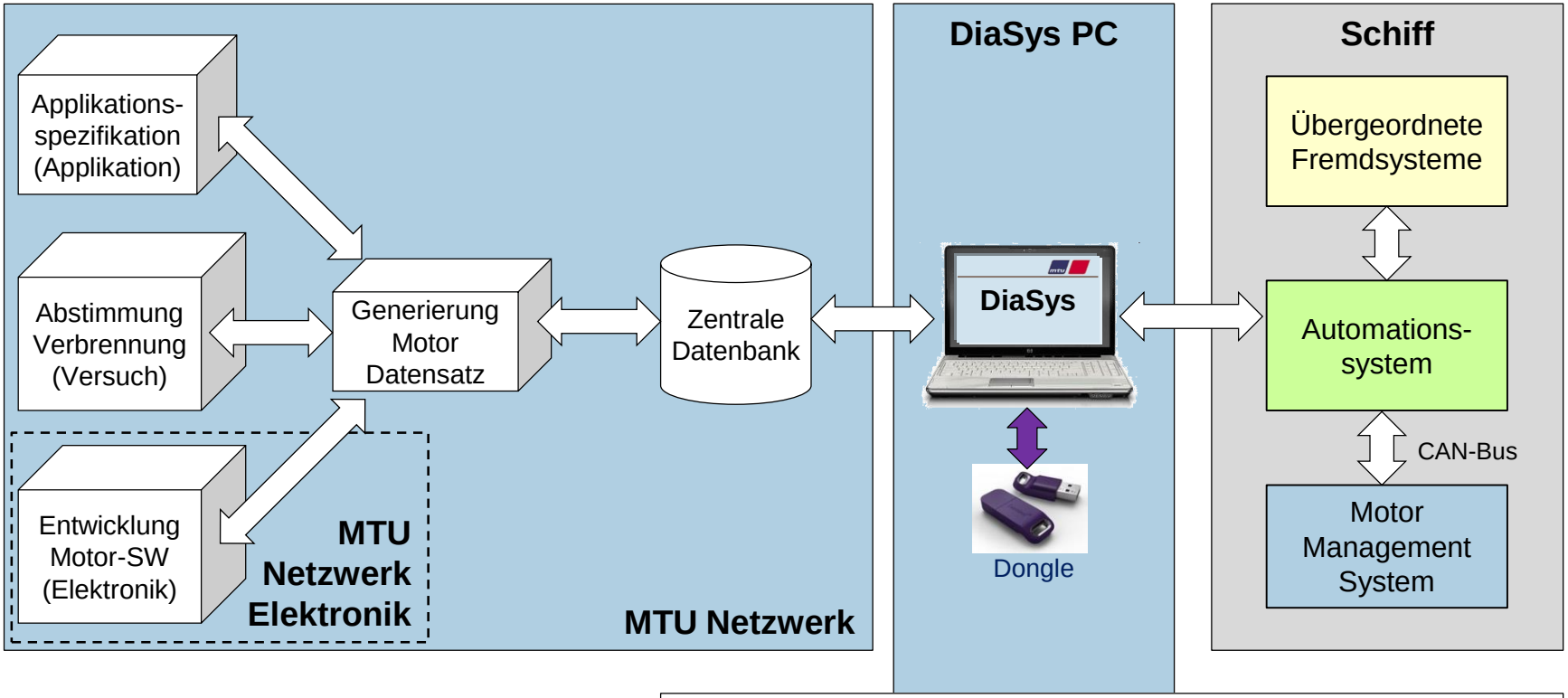
Übersicht MTU Produkte



MTU Produktlebenszyklus
Bedrohung in jeder Phase



Bedrohung bzgl. IT-Systeme
Software Logistik Prozess MMS

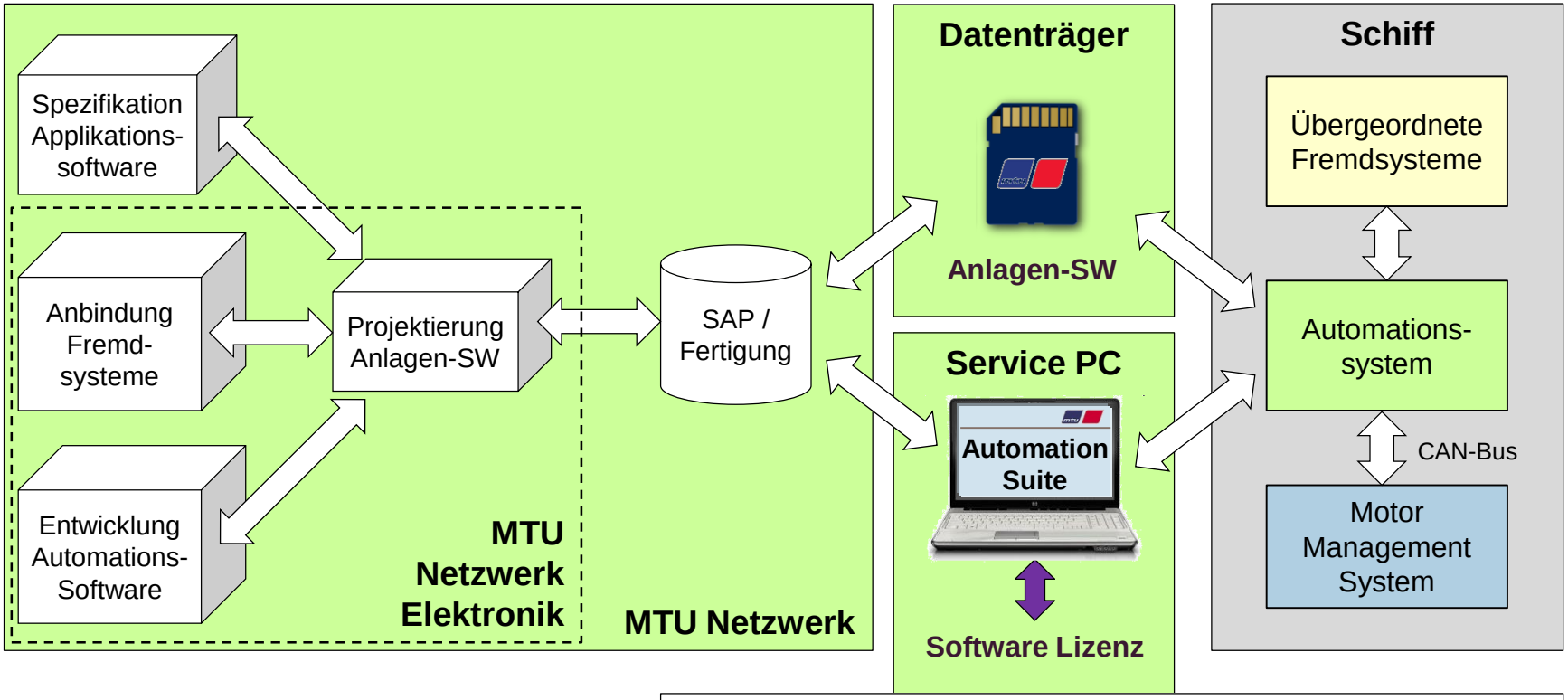


- Darstellung: Software/Datensatz Erstellung und Verteilung
- nicht dargestellt: Fertigung Elektronik, Montage und Prüfstand

Diagnose Software auf PC

- MTU Elektronik (Entwicklung)
- MTU Netzwerk (Service, Applikation)
- Fremd-Rechner (Kunde, Distributor, Service Partner)

Bedrohung bzgl. IT-Systeme
Software Logistik Prozess Automation



- Darstellung: Software/Anlagendaten Erstellung und Verteilung
- nicht dargestellt: Prüffeld

Diagnose Software auf PC

- MTU Elektronik (Entwicklung)
- MTU Netzwerk (Service, Applikation)
- Fremd-Rechner (Kunde, Distributor, Service Partner)

Bedrohung durch Hardware “Fake” Bauteile

Arten von “Fake” Bauteilen

- Bauteile funktionieren nicht
- Bauteile halten die Spezifikationen nicht ein
  - Toleranzen
  - Umweltanforderungen, Temperatur
  - Herabgesetzte Dauerhaltbarkeit
  - Fehlerhafte bzw. falsche Funktionalität
- Versteckte Funktionen
  - Aktivierung verborgener Funktion “innerhalb” des Bauteils bspw. nach Ablauf einer bestimmten Zeitspanne (nur Betriebsstunden/keine RTC) oder Eintritt bestimmter Ereignisse
  - Aktivierung der Funktion von “außerhalb” des Bauteils: Es müssen gezielt Informationen, Signale bzw. Energie von außen eingebracht werden

Bedrohung durch Software Gerätesoftware bzw. Bedatung

Mögliche Auswirkungen von Angriffen auf Software/Bedatung

- Software/Datensatz funktioniert nicht
- Software/Datensatz halten die Spezifikationen nicht ein
  - Fehlerhafte bzw. falsche Funktionalität
  - Herabgesetzte Dauerhaltbarkeit der Maschine durch bspw. erhöhten Verschleiß (Stuxnet), Veränderung der Thermodynamik
- Versteckte Funktionen
  - Aktivierung verborgener Funktion “innerhalb” des Bauteils bspw. nach Ablauf einer bestimmten Zeitspanne (nur Betriebsstunden/keine RTC) oder Eintritt bestimmter Ereignisse
  - Aktivierung der Funktion von “außerhalb” des Geräts: Es müssen gezielt Informationen und Signale von außen eingebracht werden

Rolls-Royce

Generelle Maßnahmen

- Organisatorische Maßnahmen (IT-Richtlinien, …)
- Anwendung IT-Security und IT-Infrastrukturmaßnahmen (Virenscanner, regelmäßige Updates, Zugangsberechtigungen, …)
- Schulung / Sensibilisierung der Mitarbeiter
- Sorgfältige Bauteil- u. Lieferantenauswahl (COTS-Produkte & Fremdsysteme)
- Softwaresicherheitsmechanismen (Authentifikation, Verschlüsselung, Integrität, Plausibilisierung, Diagnose)
- Absicherung der Datenlogistik
- Umfangreiche Tests und Qualitätssicherung: Bauteile, Software, Geräte, Anlagen, “Heißtest” jedes Motors, Inbetriebnahme
- Feldbeobachtung + Analyse von Auffälligkeiten im Feld für MTU Produkte

Bewertung von Schwachstellen mittels OWASP

Bewertung Eintrittswahrscheinlichkeit

Threat agent factors			
Skill level	Motive	Opportunity	Size
5	2	7	1
Vulnerability factors			
Ease of discovery	Ease of exploit	Awareness	Intrusion detection
3	6	9	2
∅ Likelihood: 4.375 (MEDIUM)			

Bewertung technische Auswirkungen

Technical impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	7	5	8
∅ Technical impact: 7.25 (HIGH)			

Bewertung wirtschaftliche Auswirkungen

Business impact			
Financial damage	Reputation damage	Non-compliance	Privacy violation
1	2	1	5
∅ Business impact: 2.25 (LOW)			

Quelle: Systemsicherheit, Prof. Dr. C. Karg (HS Aalen)

Auswertung

Für die Eintrittswahrscheinlichkeit sowie die Auswirkungen wird der Mittelwert gebildet:

0 bis 2 Punkte	LOW
3 bis 5 Punkte	MEDIUM
6 bis 9 Punkte	HIGH

Rolls-Royce

Bewertung von Schwachstellen mittels OWASP

Gesamtrisiko = Wahrscheinlichkeit x Auswirkungen

Auswirkungen				
	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Wahrscheinlichkeit		

Quelle: Systemsicherheit, Prof. Dr. C. Karg (HS Aalen)

Alternativen zu OWASP

- Microsoft Threat Risk Modeling (STRIDE/DREAD)
- Common Vulnerability Scoring System (CVSS)

System-Security gestern und morgen

gestern

- Proprietäre Systeme, Funktionen und Entwicklungsumgebungen
  → MTU OS, Protokolle, HW Build- und Projektierungsumgebungen, Tools, …
- OWASP
  → *positiv* Oportunity, Size, Easy of Discovery, Easy of Exploit, Awareness
  → *negativ* Skill Level, Intrusion Detection

morgen

- Einsatz von Standards, Zukaufkomponenten und -Software, Digital-Produkte
  → z.B. COTS, Linux/Win, Ethernet, Remote Access, WLAN, Cloud, BYOD
  → **zusätzliche Security-Maßnahmen erforderlich**!
  - Virenscanner im Produkt + regelmäßige Virenupdates, Firewalls, …
  - ggf. verschlüsselte Protokolle / HDD, Crypto-Chips, HW-Authentifizierung

Rolls-Royce

Security kostet!

Was darf Security kosten?

• Monetär	Crypto-Chips, Zertifikate, …	vs.	günstige Standard-Bauteile
• Performance	Leistungsstarke CPUs	vs.	Geräte ohne aktive Kühlung (Lüfter)
• Flexibilität	Anlernvorgänge für Geräte	vs.	einfaches ET-Konzept
• Diagnose	Verschlüsselte Protokolle	vs.	einfache Diagnose / Datenlogger
• Server	Verschlüsselte Festplatten	vs.	einfacher Datenzugriff / Service
• Verfügbarkeit	Regelmäßige SW-Updates	vs.	24/7/365 Betrieb

Fazit

- Security ist Herausforderung bzgl. Digitalisierungswünschen der Kunden (WLAN, …)
- Ziel: Trade-off aus Security ⇔ Handhabbarkeit / Bezahlbarkeit / „Digital“ Technologie
- Einmal Safety = Immer Safety; Einmal Security ≠ Immer Security
- SW-Updates ggf. nicht ausreichend → Refit aufgrund Security denkbar
- Firmenübergreifende Security-Standards auf Gesamtsystemebene fehlen aktuell

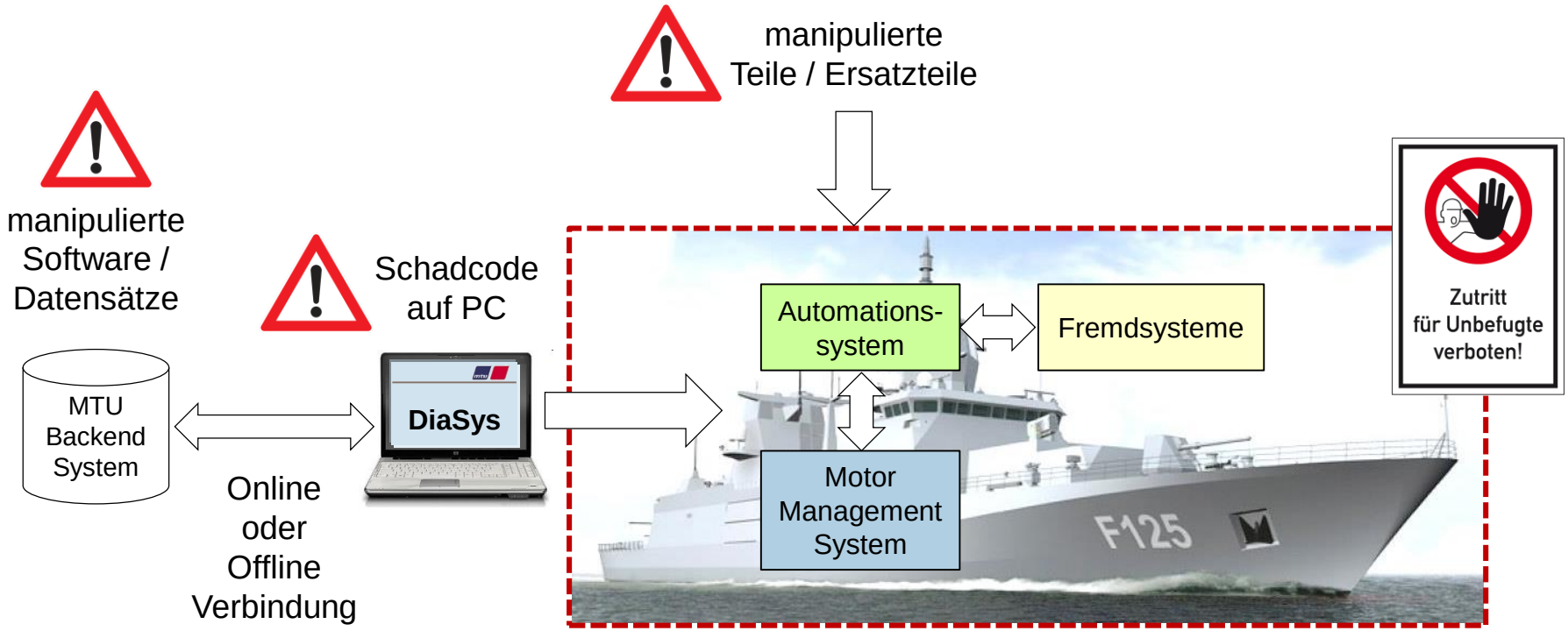
➔ Austausch mit der Deutschen Marine für zukünftige Entwicklungen erwünscht

Rolls-Royce

Sicherheit (Security)
Motivation

- Motivation
- Sicherheit bei MTU
- IT-Sicherheitskonzepte
- Sicherheit der MTU Produkte
- Sensibilisierung der Mannschaft
- Zusammenfassung

… der Weg in die Anlage



Zusätzlich

- → „Digital“ Produkte (Logger, Remote Access, Handys, …)
- → Schnittstellen im System (WLAN, Ethernet, …)
- → Schnittstellen zu Fremdsystemen (FDS, CCTV, …)

Rolls-Royce

MTU Produkte
Sensibilisierung der Mannschaft

- Nur vertrauenswürdiges Service Personal an Bord lassen
- Beobachtung von Veränderungen an Bauteilen / Kabeln / SW-Updates
- Ersatzteile aus vertrauenswürdigen Quellen (Transportweg hinterfragen)
- Service-Schnittstelle
  - Zutrittsberechtigungen für Räume / abschließbare Vorreiber
  - Keine Änderung ohne vorherige Absprache & Zustimmung von Werft / Betreiber
  - Service Personal nicht unbeaufsichtigt lassen
- Service Rechner
  - Ist der Rechner vertrauenswürdig?
  - Werden regelmäßig Sicherheitsupdates eingespielt?
  - Wie wird Datenträgern (z.B. USB-Sticks) umgegangen?
  - Welche Anwendungen sind noch auf dem PC installiert?
  - Für welche Zwecke wird dieser Rechner noch eingesetzt?

Sicherheit (Security)
Motivation

- Motivation
- Sicherheit bei MTU
- IT-Sicherheitskonzepte
- Sicherheit der MTU Produkte
- Sensibilisierung der Mannschaft
- Zusammenfassung

Rolls-Royce

Sicherheit MTU Produkte Zusammenfassung

- Fazit
  - Sicherheit hat viele Facetten und besitzt bei Rolls-Royce Power Systems und der MTU Friedrichshafen GmbH einen hohen Stellenwert
  - OWASP als Methodik für die Bewertung von Schwachstellen
  - Einmal Security ≠ Immer Security und Security kostet!

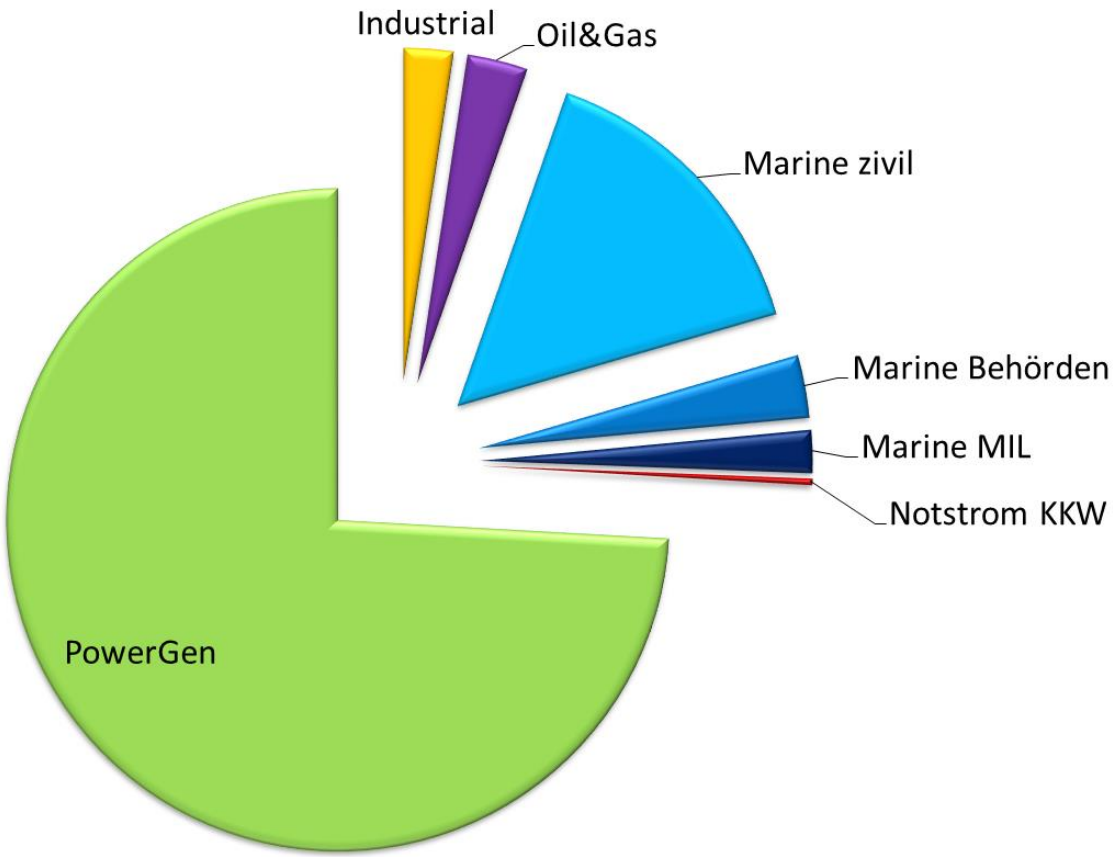
  ➔ **Wieviel IT- und Product-Security müssen und wollen wir uns leisten?**

- Ausblick
  - Firmenübergreifende Security Standards für effektive und effiziente Integration
  - MTU hat Projekt für Entwicklung eines neuen Marine Leitstands gestartet

  ➔ **Intensiver Austausch mit der Deutschen Marine seitens MTU erwünscht**

Rolls-Royce

Maßnahme Feldbeobachtung Motorsteuergerät ECU-7



- Große Stückzahlen im Feld
- Verschiedene Applikationen und Lastbereiche (Standby → Dauerläufer)
- Notstrom KKW extrem hohe Anforderungen bzgl. Feldbeobachtung

Schlussfolgerung
mögliche Auffälligkeiten werden sehr früh in anderen Applikationen aufgedeckt