SECURITY-AUDIT VON MOBILE DEVICES:

WIR HABEN EIN MDM !

UND JETZT ?

Raoul Rumplmayr

ASFINAG

17.10.2019, Konferenz „Secure Mobile & Connected Future“

AGENDA – Raoul Rumplmayr

- ASFINAG Vision – und ihre Grundlage
- Typische Schutzobjekte (Ein Überflug)
- Sicherheit – babylonische Zielkonflikte !
- Was macht Mobiles so besonders ? (Risikoanalyse)
- Was bitte heißt „Mobiles“?

➔ **Gilbert Wondracek**

… Verlässlichkeit auf allen Wegen …

RELIABILITY ALL THE WAY.

Was bedeutet das?

… Verlässlichkeit auf allen Wegen …

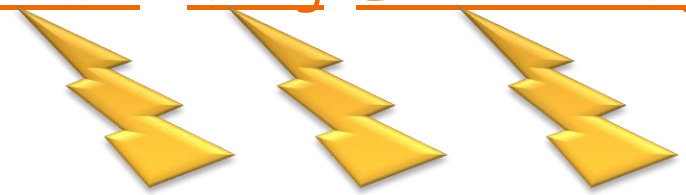
➔ **Mobilitätsbedürfnisse** steigen

➔ Ansprüche an **Service-Verfügbarkeit** und **Vernetzung** steigen

… immer mehr Interne + Externe (Nutzer+Dienstleister)

… mit immer umfassenderem **Zugriff + überall + stets verfügbar**

➔ „Ich will wenig Einschränkungen“ (Funktion + Zugriff + Daten)



Was bedeutet das?

Allgemeine Herausforderung

Zielkonflikte zwischen „universelle Mobilität“
..u.a.…

mit **Mindest-Anforderungen** der **Informations-Sicherheit** **!**

Unsere Vision …

Grundlage der ASFINAG Vision …

… AUSBAU DIGITALER INFRASTRUKTUR + SERVICES !

… Grenzen zw. physischen und logischen Netzen längst aufgelöst …

… ab 2020 ist IP-Infrastruktur fixer Bestandteil einer Autobahn-Strecke.

asfinag.at/.../pressemeldungen/2019/autobahnen-wlan.../

„[..] werden Autobahnen und Schnellstraßen 2020 bis 2023 mit einem speziellen WLAN für die Fahrzeugkommunikation ausgerüstet. [..] 500 WLAN-Stationen österreichweit. [..]
Das System heißt C-ITS und steht für „Cooperative Intelligent Transport Systems“. [..] wird künftig wichtige Informationen aussenden [..] kann von WLAN-tauglichen Fahrzeugen empfangen werden. [..] Auch von den Fahrzeugen können Infos an die ASFINAG gesendet werden, um so andere Verkehrsteilnehmerinnen und Verkehrsteilnehmer noch besser mit Updates entlang der Strecke zu versorgen. [..]
Vorteil: ASFINAG sendet zeitnah Informationen wie Fahrstreifensperren, Baustellen, Tempolimits, Pannen, Unfälle auf der geplanten Strecke ins Fahrzeug.“

Nächste Fahrzeuggeneration:

Teilautomatische Fahrt / Lkw-Konvois (Studie 2018)➔ cms.asfinag.at/.../truckplatooning....pdf

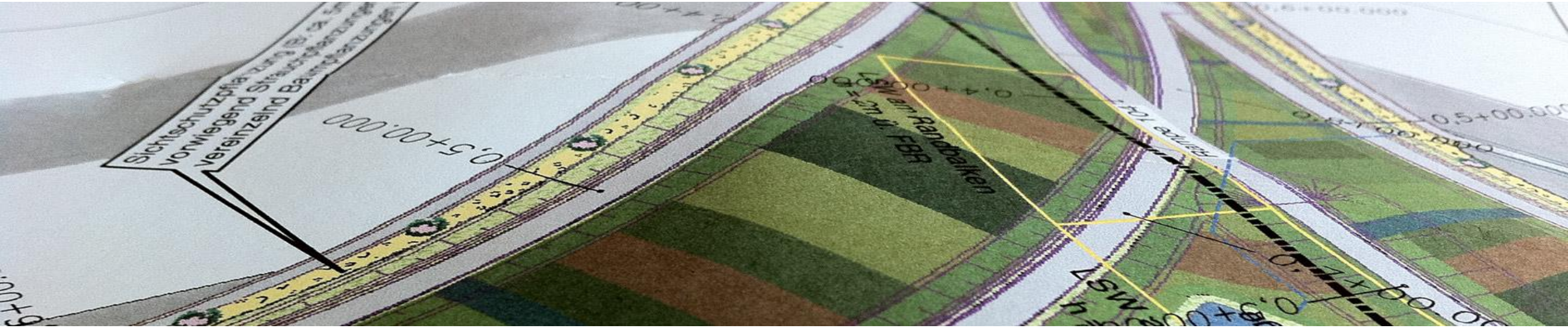
Faktencheck Automatisches Fahren in Ö cms.asfinag.at/.../asfinag_faktencheck.pdf

Konkrete Herausforderungen

- Vielzahl an Services & Service-Partnern
- Innovationsdruck: Funktionsanforderungen steigen
- Anzahl mobiler Angebote + mobil-dezentralen Aktivitäten steigt
- Ansprüche steigen: Service-Verfügbarkeit + Usability
- Mobiles als mittlerweile übliches Angriffsziel (alle OS!)
- Spannungsfeld Corporate vs. Private Nutzung
    - Informationssicherheitskultur vs. „private“ User Behaviour
    - Umgang mit Verarbeitungen und Datensicherheit
    - Lizenzthemen, etc…

AGENDA – Raoul Rumplmayr

- ASFINAG Vision – und ihre Grundlage
- ASFINAG – Typische Schutzobjekte (Ein Überflug)
- Sicherheit – babylonische Zielkonflikte !
- Was macht Mobiles so besonders ? (Risikoanalyse)
- Was bitte heißt „Mobiles“?



Schutzobjekte

durch Anwendung mobiler Services einem erhöhten Risiko ausgesetzt

Schutzobjekte

Einnahmen

- Einnahmen [EUR]: Lkw-Maut 1,4 Mrd. Vignette 501 Mio. Sondermaut: 189 Mio.
- Verkaufte Vignetten gesamt: 25,400 Mio. Stück
- Gesamterlös 2018: 2,58 Mrd. Euro
- Periodenergebnis 2018: 824 Mio. Euro
- Ausgaben für Infrastruktur-Investitionen 2018 gesamt: 1 Mrd. Euro

Schutzobjekte

Anwendung mobiler Dienste erhöht Risiken

Beispiele !

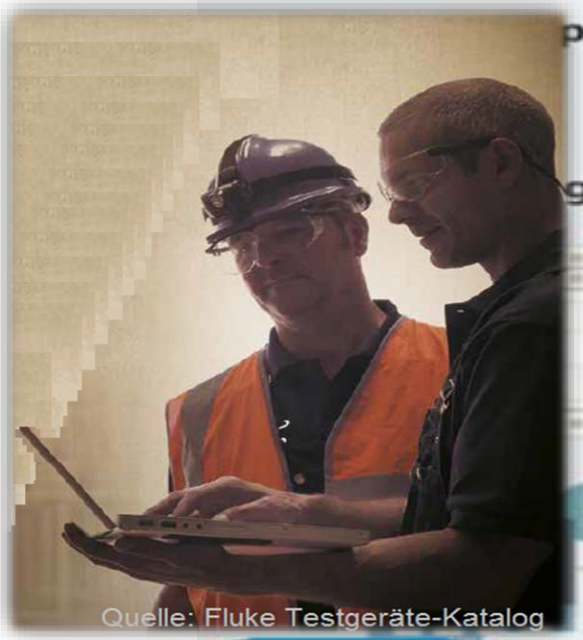
- Tunnelsteuerungen
- Nationale Verkehrssteuerung

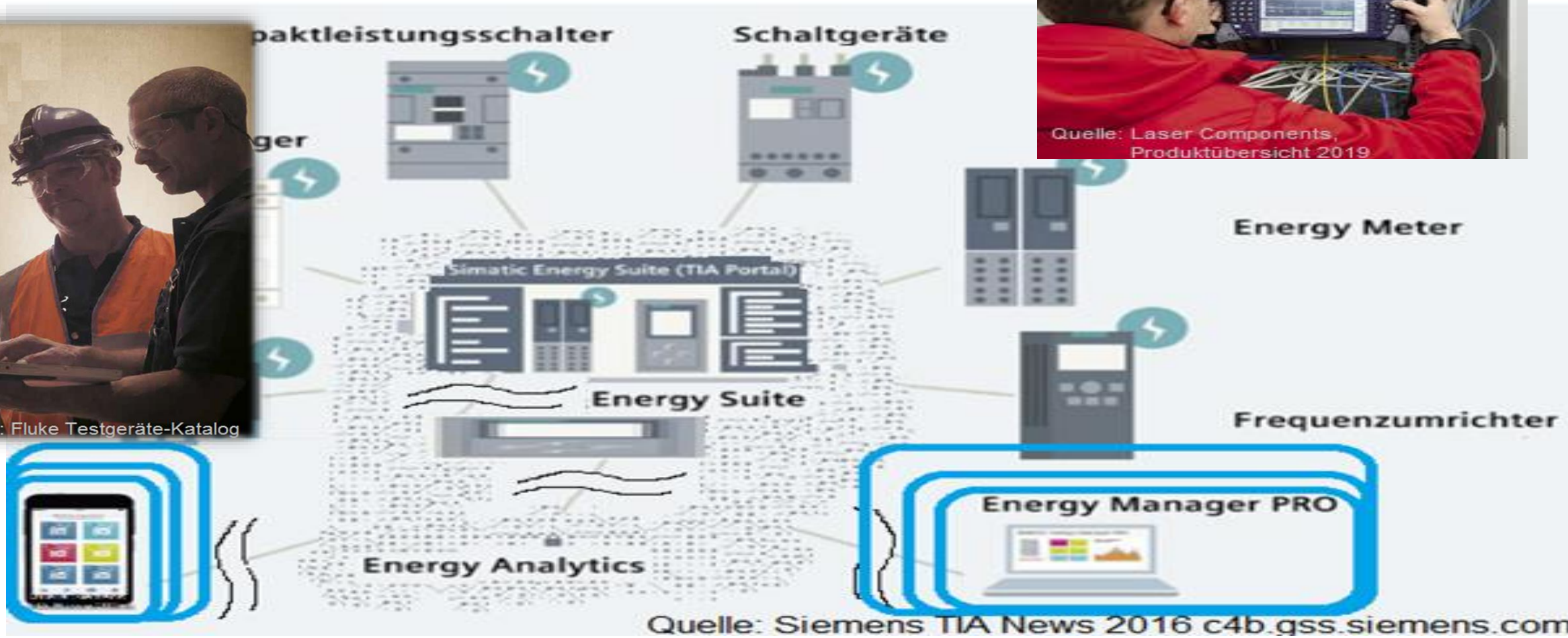
Nationale Netzsteuerung

Verkehrsmanagementzentralen (VMZ)

Schutzobjekte

Mobile Services

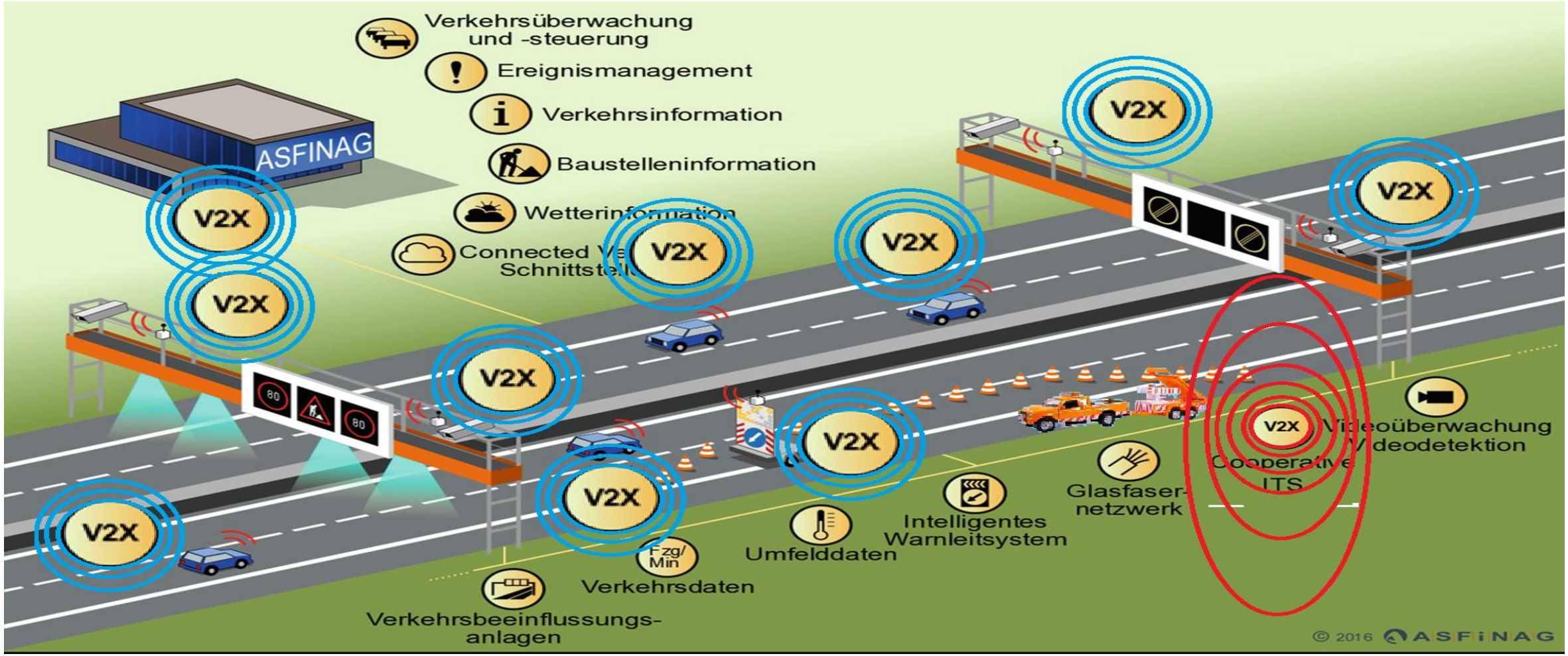




Risikoanalyse

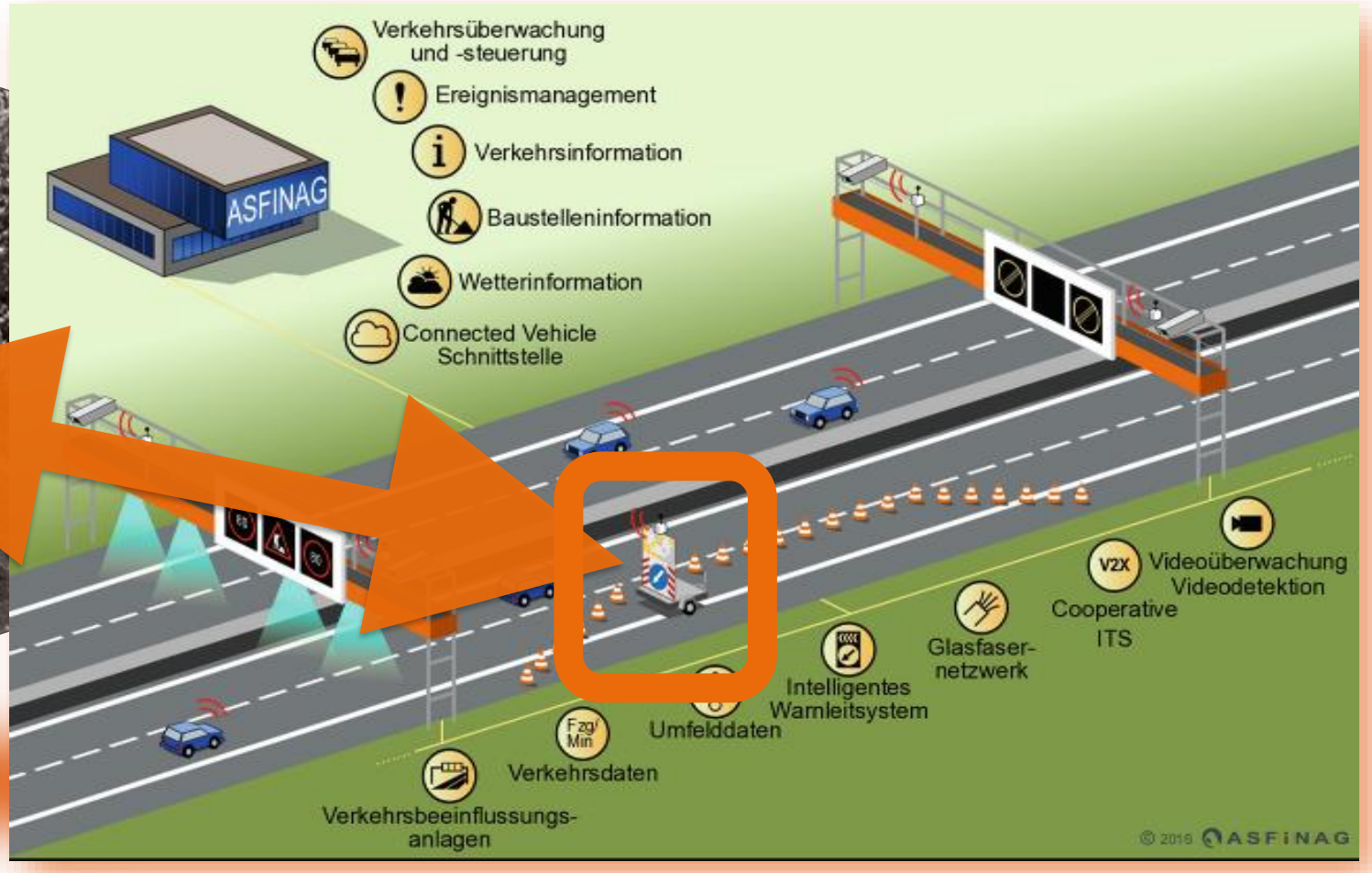
4G hat jedenfalls 4 “ L“ – Risiken!

➔…Risikoanalyse…!



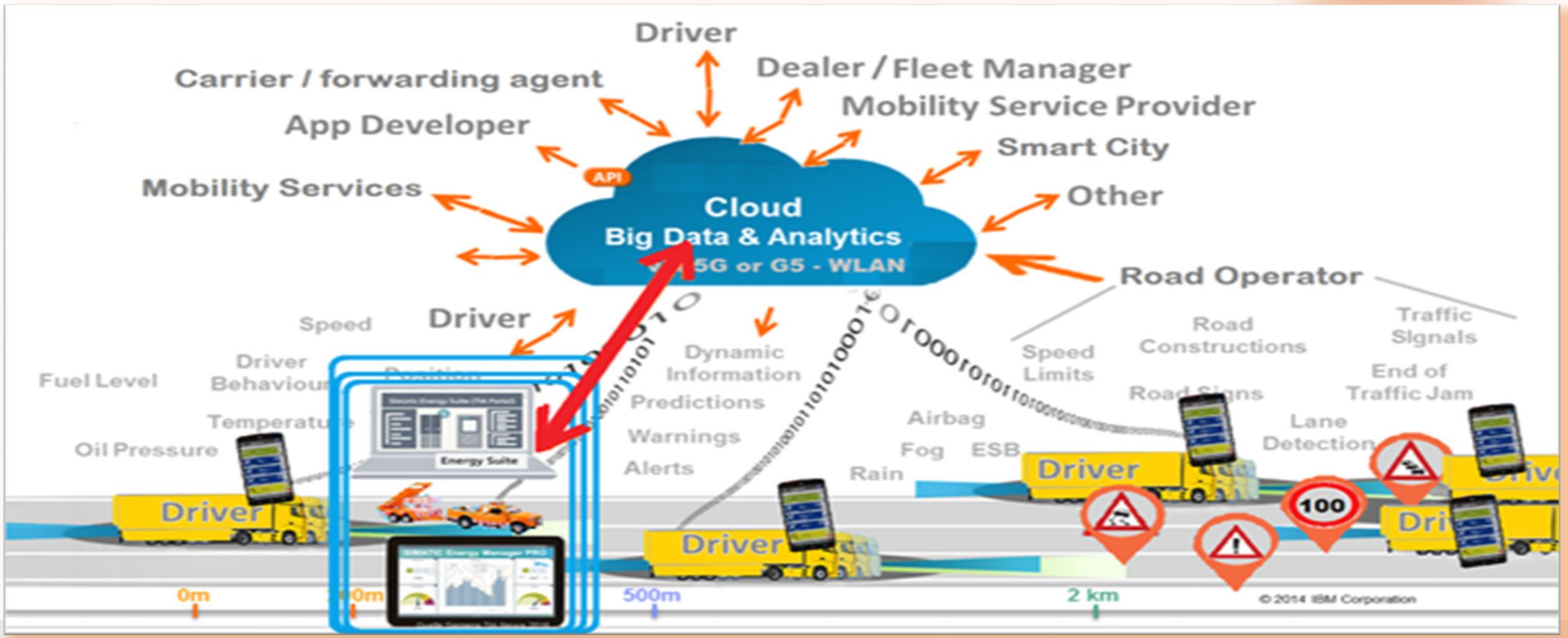
Schutzobjekte

Infrastruktur für das autonome Fahren … Unsere „größten Mobiles“



Schutzobjekte

Infrastruktur für das autonome Fahren … Unsere „größten Mobiles“



Schutzobjekte

Ressourcen und Infrastruktur (z.T. „wD“) (Stand Geschäftsbericht 2018)

- Mitarbeiter: 2.822
- Netzlänge in Betrieb: 2.223 km
- 11 Mio. Kunden mit Jahresfahrleistung: 32,5 Mrd. KFZ-km/Jahr (A+S)
- Kundenkontakt / Webpräsenz / Marken-Image / kommerzielle Angebote (Webshop, Terminals, GoMaut)
- Kundenkontakt: App „Unterwegs“ >>500.000 Installationen, Social Media-Auftritte (Facebook, Twitter, Blog, Chatbot) mit > ½ Mio. Einzelkontakten
- Raststationen: 87 Video !
- Rastplätze: 51 Video !
- Park & Drive Anlagen: 47 Video !
- Gesamt Stellplätze: ca. 18.300 Pkw- und ca. 7.500 Lkw-Stellplätze) Video !
- Tunnel in Betrieb: 165
- Brücken: 5.735
- Anschlussstellen: 371
- Autobahnmeistereien: 43
- Mautstellen: 6
- Verkehrsmanagementzentralen: 9

Schutzobjekte

Marken-Image ASFINAG

ASFINAG als Mobilitäts-Provider auf A+S ist

- Verlässlich
- Sicher
- Nachhaltig
- Innovativ

» „Wir tun was“

Schutzobjekte

Mobile Services

„kleine“ mobile Units für den Einsatz in IT

Schutzobjekte

Kunden-Services

ASFINAG Kompagnon: Eine App als digitaler Beifahrer

https://blog.asfinag.at/technik-innovation/kompagnon/

Schutzobjekte

Kunden-Kommunikation

„ASFINAG Blog“

https://blog.asfinag.at/hinter-den-kulissen/irrtuemer-winterdienst/

Schutzobjekte

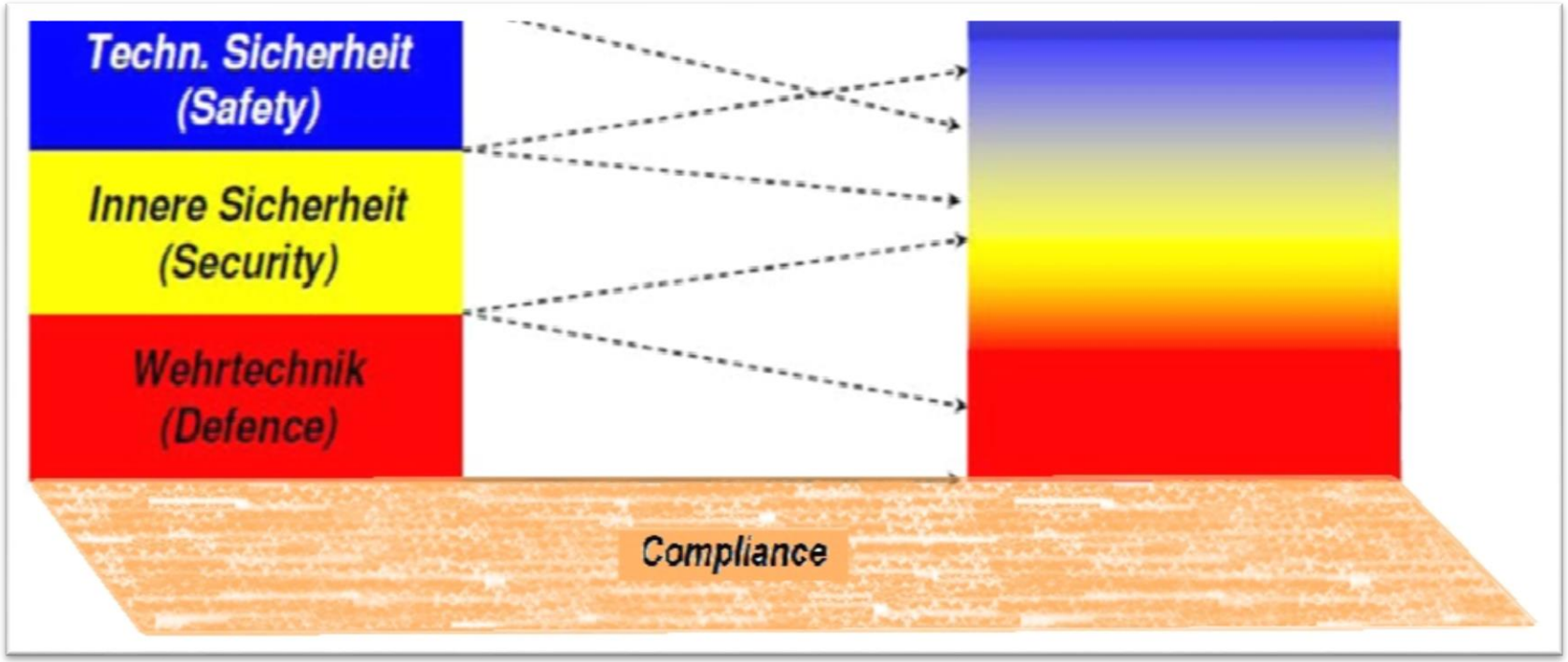
für mehr Kunden-Sicherheit und Kunden-Komfort

(beispielhaft)

AGENDA – Raoul Rumplmayr

- ASFINAG Vision – und ihre Grundlage
- Typische Schutzobjekte (Ein Überflug)
- Sicherheit – babylonische Zielkonflikte !
- Was macht Mobiles so besonders ? (Risikoanalyse)
- Was bitte heißt „Mobiles“?

Von Betriebs-Sicherheit zu Informations-Sicherheit



➔ **Informationssicherheit** ➔ kurz: „InfoSecurity“

„SICHER“ ? … Für Laien babylonische Sprachverwirrung!

- „**SICHER**“ aus Kundensicht = hochverfügbare, belastbare Straße und Services
- „**SICHER**“ aus Compliance-Sicht = def. Anforderungen an Betreiber wesentlicher Dienste > NISG (InfoSec) + als „Verantwortlicher“ für Datenverarbeitung > DSGVO (Datensicherheit) + Netz-Bereitsteller > TKG (InfoSec + Datensicherheit)
- „**SICHER**“ für den Eigentümer = Verkehrssicherheit, „sicherer“ Einnahmenfluss, „sichere“ Verkehrsträger-Vernetzung

➔ **Informationssicherheit** ➔ kurz: „InfoSecurity“

„SICHER“ ? … Für Laien babylonische Sprachverwirrung!

- babylonisch unterschiedliche Perspektiven ➔ unterschiedliche Ziele! ➔ Typisch in Prüfbereichen mit hohem Innovationsanteil
-
- ➔ **Unterschiedliche Anforderungen**
- ➔ erkannte + gelöste **Zielkonflikte ?**
- (…Revision zeigt dies mit dem Prüfbericht auf …)

➔ **Informationssicherheit** ➔ kurz: „InfoSecurity“

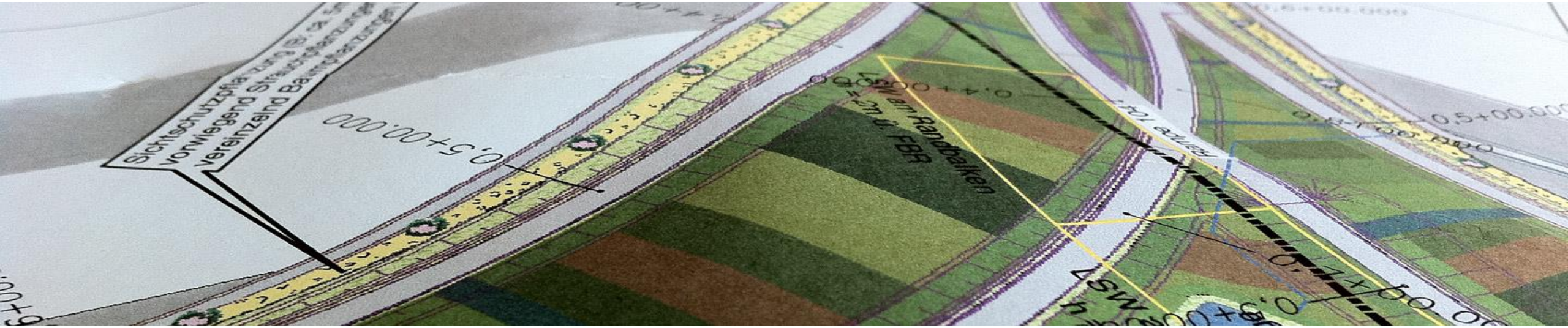
„SICHER“ ? … Für Laien babylonische Sprachverwirrung!

Konflikte zwischen

- **Verfügbarkeit / Performance** vs.
- **Usability / User Experience** vs.
- **Informationssicherheit** vs.
- **Datensicherheit**

AGENDA – Raoul Rumplmayr

- ASFINAG Vision – und ihre Grundlage
- Typische Schutzobjekte (Ein Überflug)
- Sicherheit – babylonische Zielkonflikte !
- Was macht Mobiles so besonders ? (Risikoanalyse)
- Was bitte heißt „Mobiles“?



Risiko-Analyse

Risikoanalyse

Was macht Mobiles so besonders?

Warum ein eigenes Prüfthema?

Im „Prüfuniversum“ eigentlich nur ein Nebenthema

(zugehöriges Services / Infrastruktur)

Risikoanalyse

Was macht Mobiles so besonders?

Warum ein eigenes Prüfthema

- schlanker – leichter – kleiner
- überall (und „nirgends“…)
- immer dabei
- hohe Rechenleistung + großer Speicher
- hohe Konnektivität
- umfassende Zugriffsrechte auf Daten, Dienste, Systeme und Anlagen

➔…Risikoanalyse…!

Risikoanalyse

Was macht Mobiles so besonders?

4G hat **jedenfalls 4 “ L“ – Risiken!**

- Loss
- Leaks
- Loose Behaviour
- Least expected

➔…Risikoanalyse…!

Risikoanalyse

4G hat jedenfalls 4 “ L“ – Risiken!

Loss

Diebstahl, Vergessen, ..

Leaks

„Over the shoulder“, „in der U-Bahn“, „kurz unbeaufsichtigt“

Loose Behaviour

„Sorgloses“ Userverhalten, als Device schwerer zu managen, Daten am Gerät, potentiell unsichere App-Installation / App-Nutzung, leichteres+schnelleres Phising und Malware-Infektion (z-B. kein Hovern) durch unsicheres „Klickverhaltenen“ / „Bestätigen“, privates Nutzen (WhatsApp & Datenfresser), nicht lizensierter Content ➔ **AWARENESS** als Top-Thema!

Least expected (sog. „Aha – Asoo“-Effekt)

Ist ja nur ein „Handy“, also nicht so gefährlich „Hat doch eh einen Virenschutz“,
Zugriffsmöglichkeiten und Rechte werden stark unterschätzt &
Unerwünschter Zugriff über deutlich schwerer zu kontrollierende Wege

Beispiele „zu prüfende Risiken“

Sicht = Konzernebene

Beeinträchtigung der Informations- oder Betriebssicherheit
in Teilbereichen des Konzerns , z.B.:

Technische Infrastruktur / IP-Netze,
Mautbereiche,
Kundenkontaktbereiche (virtual, reallife),
kommerzielle Transaktionsbereiche (Webshop, Lieferantenzusammenarbeit) und
Kundenservicebereiche (virtual, reallife)

oder

nur der MOBILE SERVICES selbst

durch…

➔…Risikoanalyse…!

Risikoanalyse

Beispiel „zu prüfende Risiken“ (Gesamtsicht = Konzernebene)

… durch …

(1) **Unerwünschter remote network access**

(2) **Data loss**
Informationssicherheitsrisiko
Datenschutzaspekte
Produktivitätsverlust (Daten- oder Funktionsverlust)

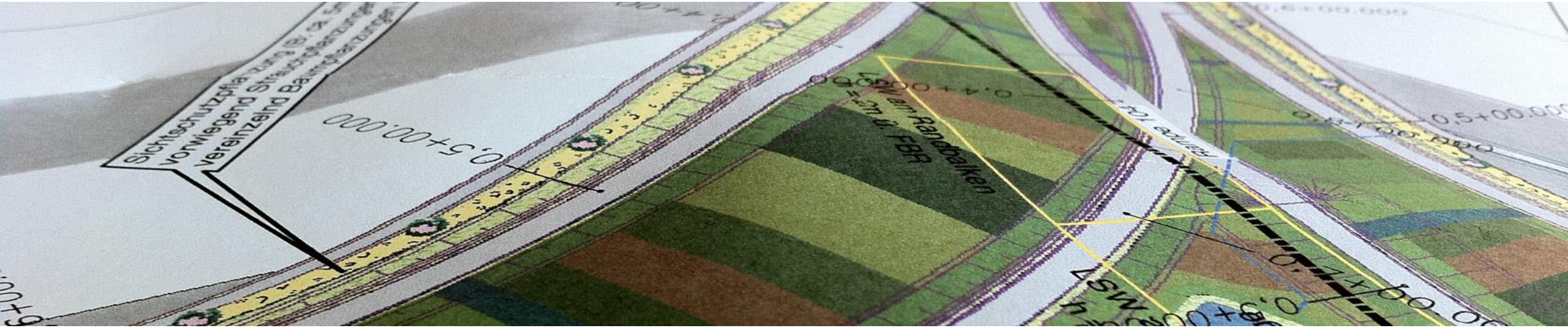
(3) **Betriebsunterbrechung (Incidents)**
risk of operational disruption inkluding malfunction, data loss, malware

➔…Risikoanalyse…!

AGENDA – Raoul Rumplmayr

- ASFINAG Vision – und ihre Grundlage
- Typische Schutzobjekte (Ein Überflug)
- Sicherheit – babylonische Zielkonflikte !
- Was macht Mobiles so besonders ? (Risikoanalyse)
- Was bitte heißt „Mobiles“?

➔ **Gilbert Wondracek**


Sichtschutzpflanzung
vorwiegend Straucheplanzungen
vereinzelnd Baumpflanzungen
0,5+00.000
Randbalken
FBR

Mobiles ?

„Mobiles“?

Allgemeine Definition für die Prüfung

„An ein ASFINAG-Netz

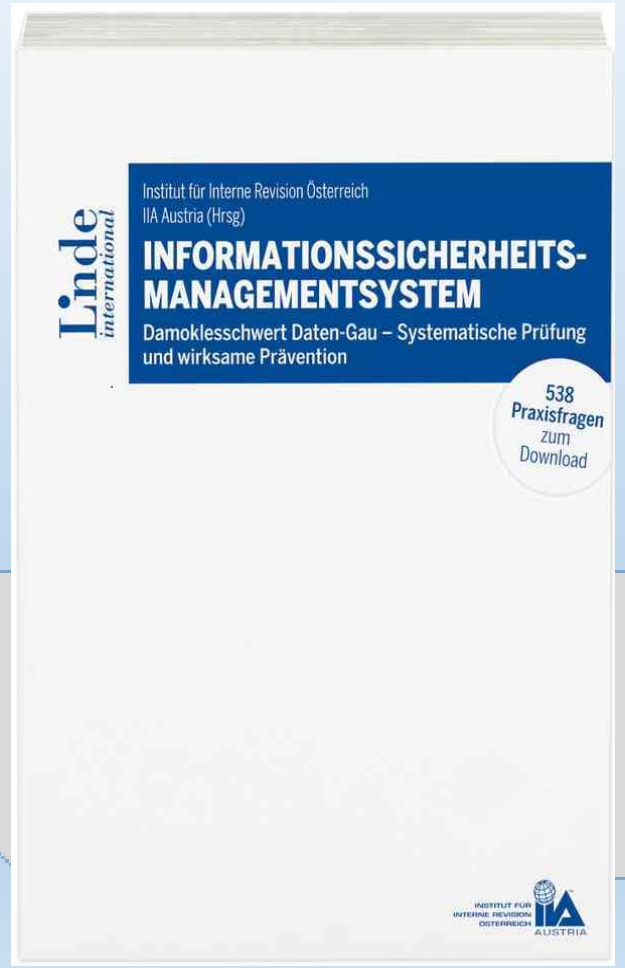
- *drahtlos angebundene*
- *mobile Geräte*
- *mit universeller Datenverarbeitungsfunktionalität*
- *und weit verbreitetem Betriebssystem,*
- *nicht fix in einem schützenden Umfeld verbaut (z.B. nicht auf einem fixen Standplatz in Gehäuse, in Fahrzeug, in Räumlichkeit).*
- *Insbes.: Smartphones, Laptops/Netbooks/rugged Notebooks, PDA/Tablets.“*

➔…CMDB + ITSM-Service-Liste ➔ konkret zu prüfende Geräte-Stichprobe identifizieren…!

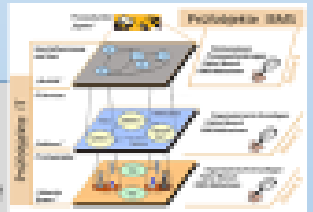
„Mobiles“?

Was macht Mobiles so besonders?

Das „Technik“-Kapitel im ISMS-Buch



- Risiken / Übersicht
- Prüf-Checkliste je Kapitel (Excel)
- Interne / externe Prüfung
- Verweis auf Prüfnormen
- Kap.5 = Unterkapitel IT-Infrastruktur
  … „Mobiles Arbeiten“

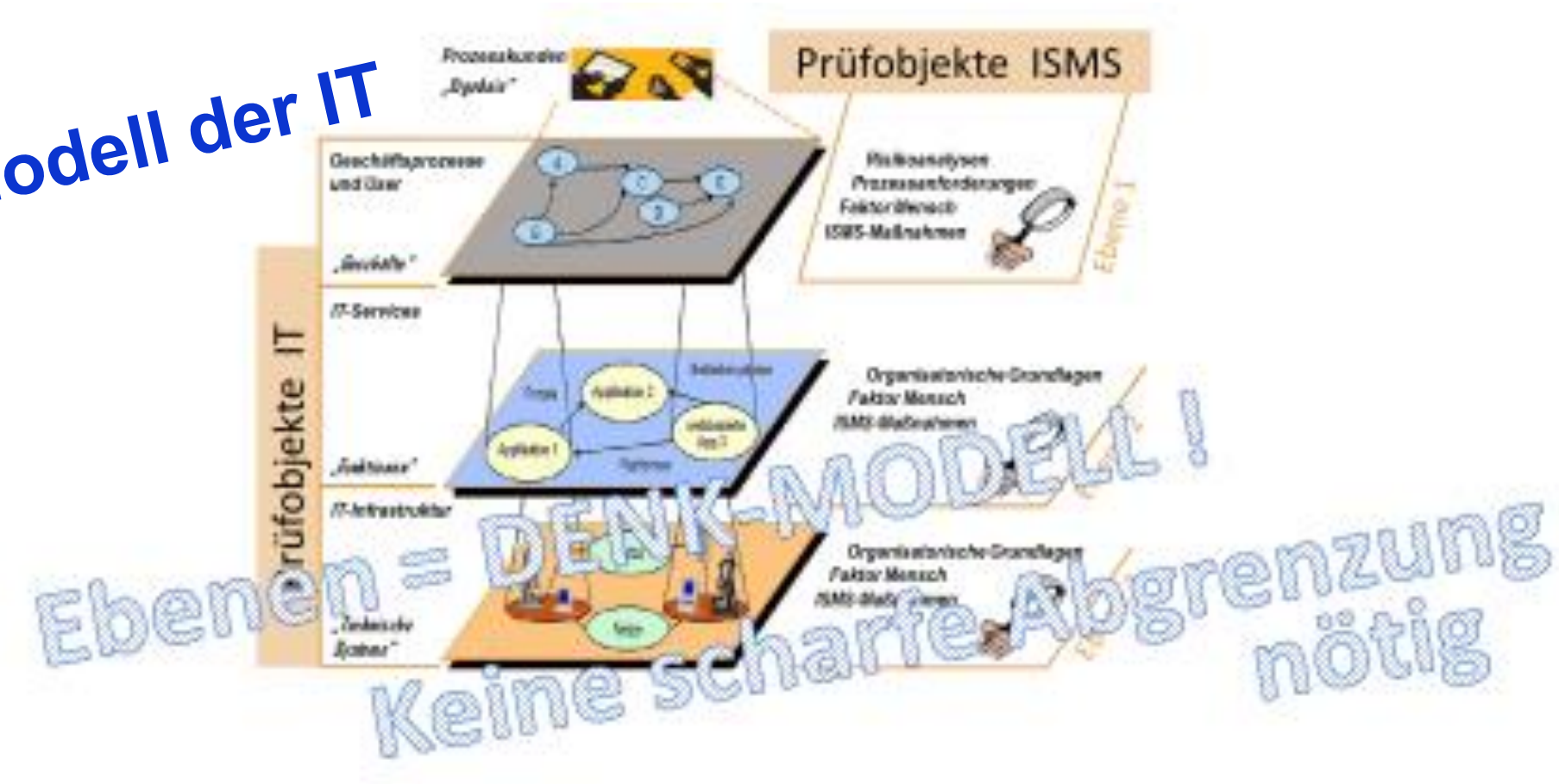


- 3-Ebenen-Modell der IT als Grundlage für Prüfuniversums- & Prüfungs-Konzeption
  ➔In Google nach dem Schlagwort „Informationstechnik“ suchen, oberster Link auf de-wikipedia-org

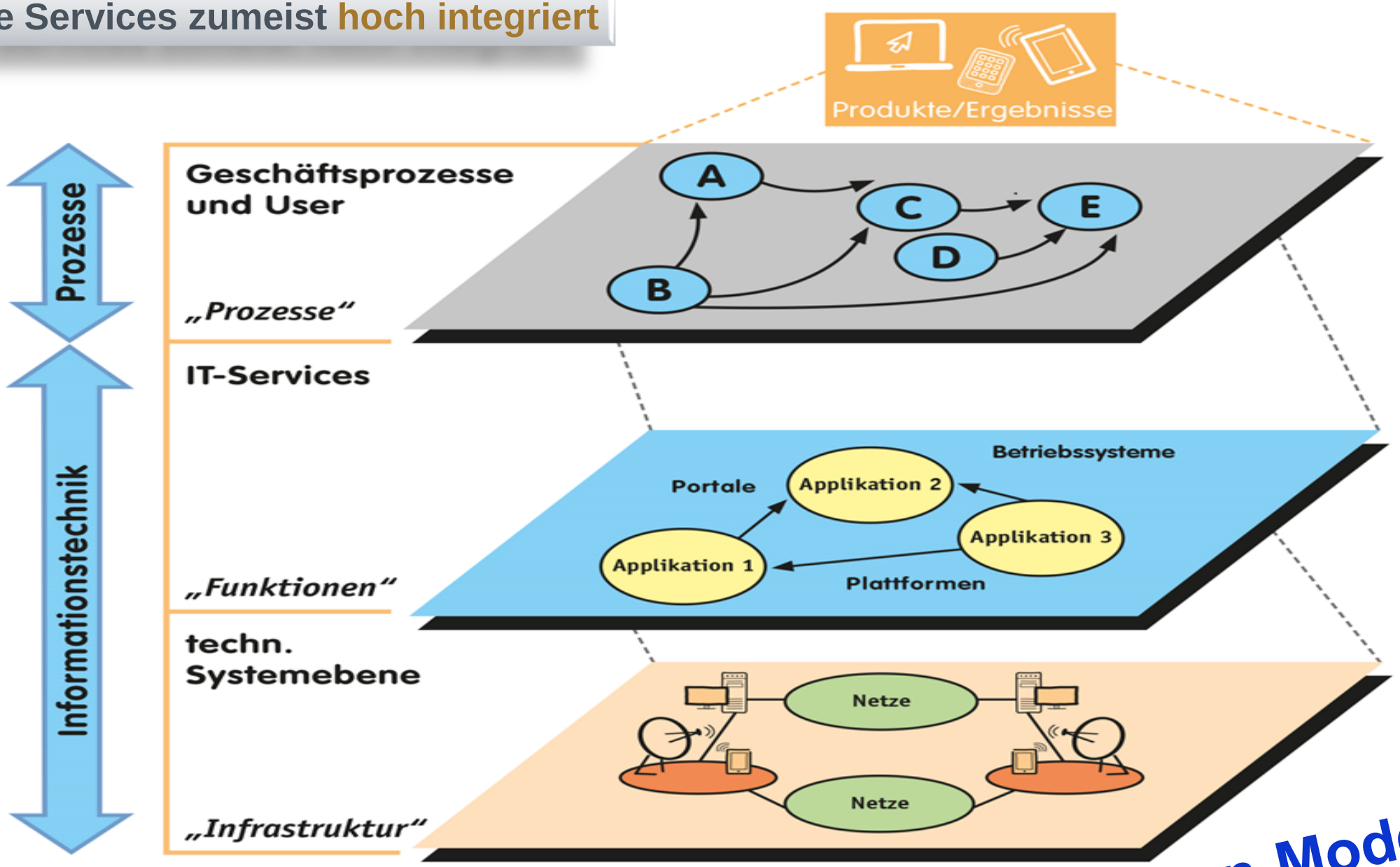
Quelle: IIRÖ

„Mobiles“?

Was macht Mobiles so besonders?



Mobile Services zumeist hoch integriert



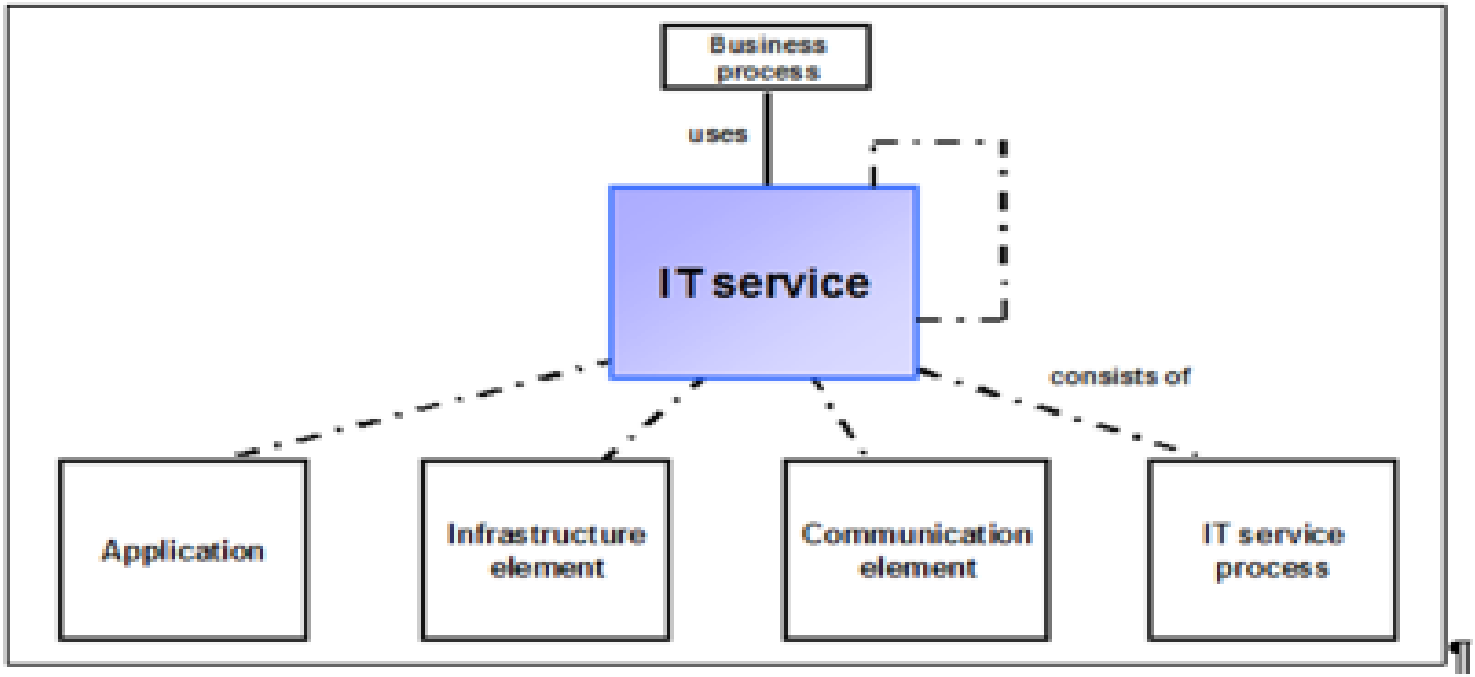
3-Ebenen-Modell der IT

„Mobiles“?

Mobile Services zumeist hoch integriert

Service-Kaskadierung

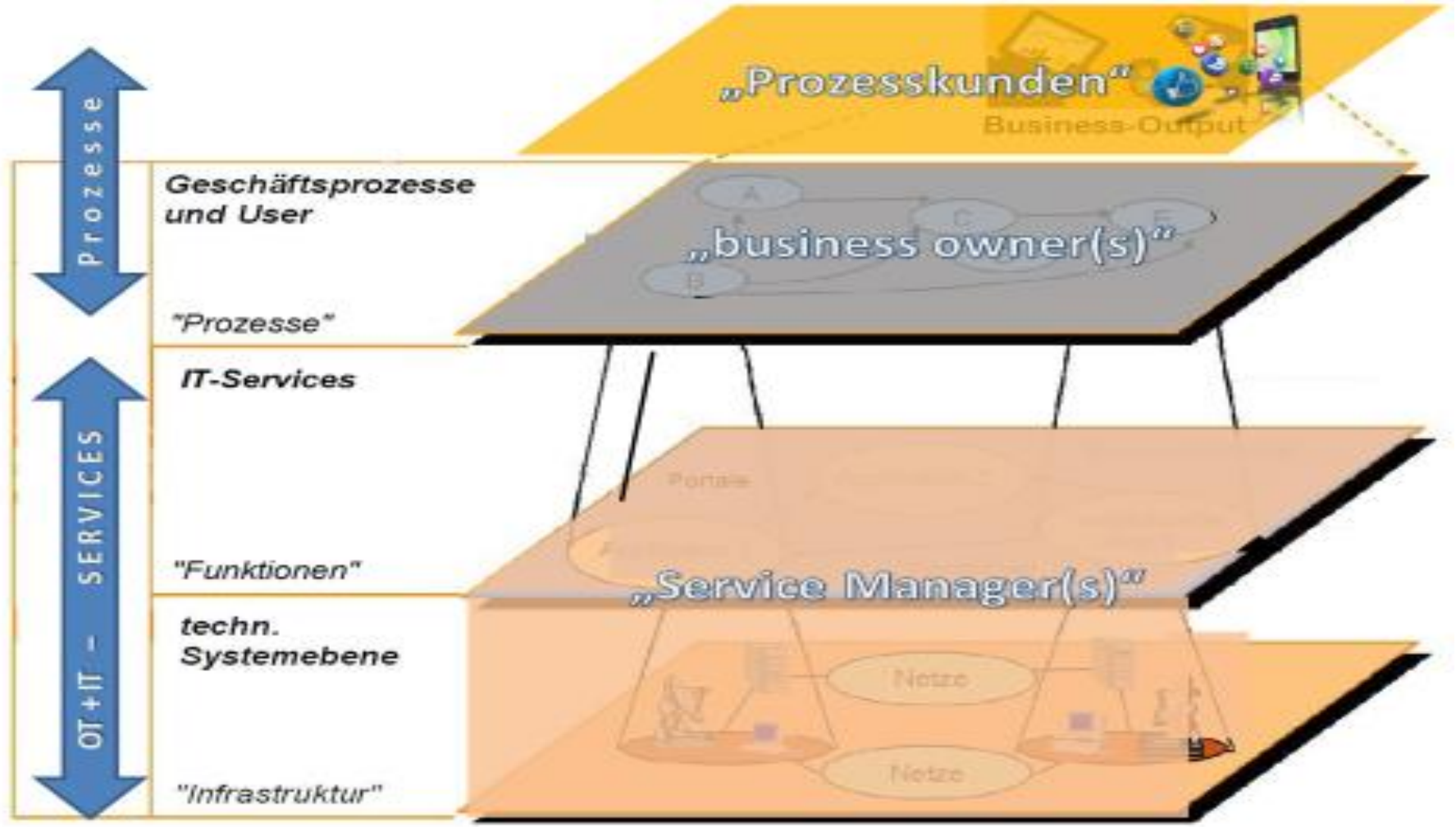
- **IT-Services:** IT-Produkte oder Funktionalitäten, die Geschäftsprozesse mittelbar oder unmittelbar unterstützen



Quelle: ISACA

„Mobiles“?

Mobile Services zumeist hoch integriert



„Mobiles“?

Mobile Services zumeist hoch integriert

(IT-Service-Kunde)

Prozesskunde
hat „alles“ in der Hand ➔

4 “ L“

ASFINAG REVISION

Ing. Mag. Raoul Rumplmayr
raoul.rumplmayr@asfinag.at

ASFINAG Service Center
➔ **0800 400 12 400**
➔ ***200**

info@asfinag.at
asfinag.at

➔ … WILL GEPRÜFT SEIN …

www.asfinag.at