salzburgresearch

Prof. Dr. Ing. habil. U. Hofmann

Secure Communication in the Smart Grid

Secure Internet Integration, Wien 10.5. 2012

Gliederung

1. Salzburg Research

2. Use Cases ergeben Anforderungen an Security Standards, Erkennen von Gaps

2.1 EU Mandate 490, VDE-ITG AG Smart Grid Sec

2.2 Beispiel: Risiko-Bewertung TimeSync -> Reporting

3. Gap: Risiko-Bewertung Internet-Infrastruktur

4. SRFG MINER Tester und Monitor für Secure Integration of Smart Grid Communication

4.1 Motivation

4.2 Einsatzfälle

4.3 2012/2013: SRFG MINER Einsatz in *Securing SG Com Integration*

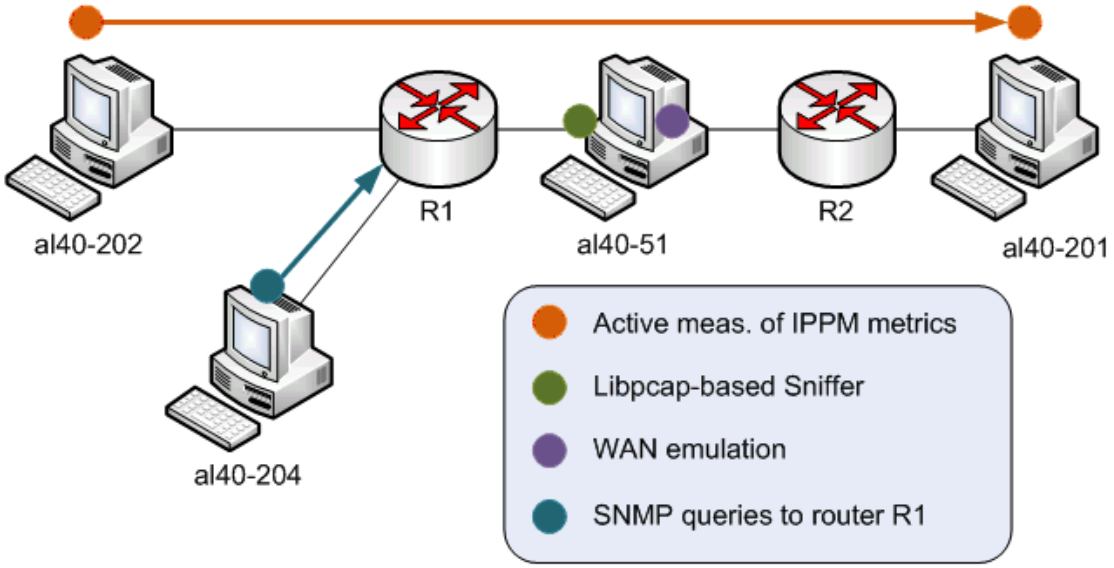
1. Salzburg Research GmbH

- **Forschungsgesellschaft des Landes Salzburg**
  - Gegründet 2000
  - 70 Beschäftigte (2011)

- **Bereiche**
  - Advanced Networking Center
  - Computational Logistics Lab
  - Knowledge and Media Technologies
  - Mobile and Web-based Information Systems
  - Innovation Lab
  - K-Zentrum NewMediaLab
  - Kompetenzschwerpunkte
    - Tourismus
    - E-Health
  - ITS Austria West

LNdF 2012
für alle
Altersgruppen

- **U. Hofmann**
  - bis 1995 Entwicklungsingenieur X.25.-IBM-PAD-Implementierung, Uni Dozent F&E Computernetze
  - ab 1995: Lehre und Forschung Internettechnologien FH Salzburg und Salzburg Research
  - Nationale (FIT-IT, FH-Impuls, **KIRAS**, COIN) und EU (FP6, FP7, Coord. INTERMON, 2011-2015: **SEC** IDIRA) Projekte
  - Schwerpunkt: Monitoring Architekturen, Tools http://miner.salzburgresearch.at



2. Use Cases (UC) ergeben Anforderungen an Security Standards

2.1. EU manadate 490, VDE-ITG Fokusgruppe

- **2011 Gründung der VDE/ITG Fokusgruppe 1.5 Energie-Informationsnetze und – Systeme, AG Security**
  - Unterstützung int. Gremien (IEC, ETSI, CENELEC)
  - Normung in IEC62351/TC57 WG15 (EU Mandate 490)

- **M/490 Standardization mandate for Smart Grid Information Security SGIS**

  SGIS toolbox definition and application
  - 20 Primare Schutzziele/Forderungen: C.I.A., Privacy, non repudiation…auditable…exchangeability of products (EU), availability,…

- **SG information**
  - **=** “dangerous goods” needs to be protected … whenever it is handled or transported on streets (incl. signature)

- **Warum Mitarbeit wichtig ?**
  - Wirtschaft setzt Standards voraus
  - angewandte F&E ist den Standards vorgelagert (kein Internet EU Projekt ohne IETF draft)
  - SRFG Projektentwicklung auf allen Ebenen (regional, national, EU)

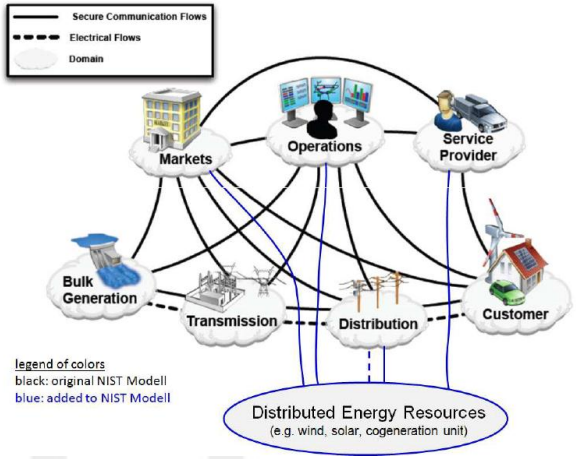
Toolbox, Vorgehensweise:
Gaps in Standards zu gefordertem Security Level finden

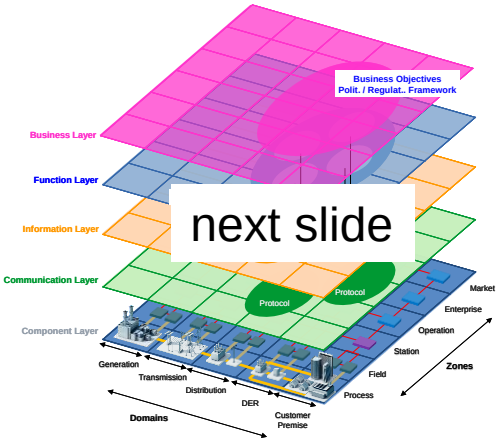
- Vergleiche mit internationalen Standards NIST, IEC
- rein technisch aber auch Risikobewertung

- **Schritt 1**: UC Erfassung => schreibe UC gemäß „WG SGIS report template“

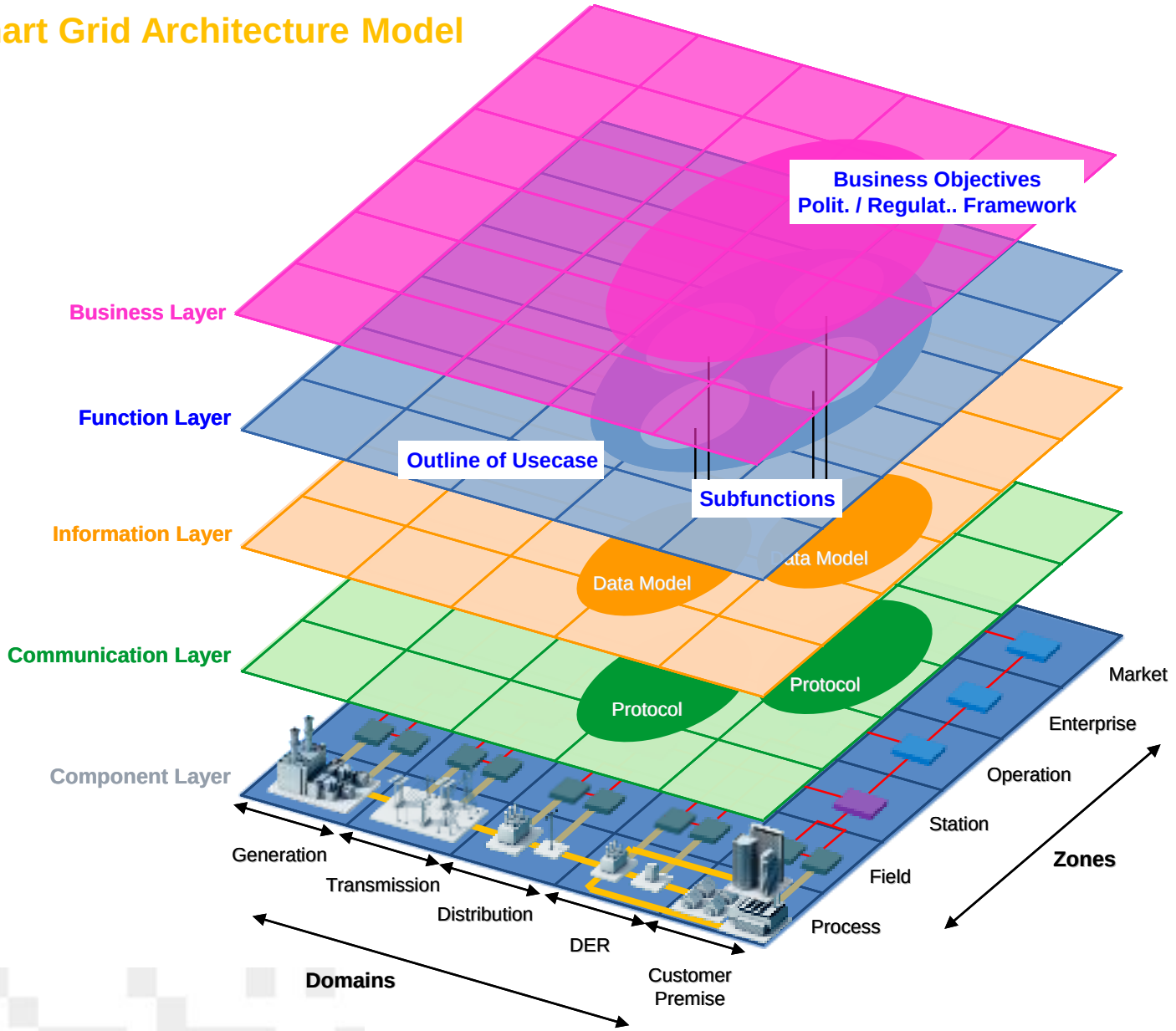
- **Schritt 2**: Einordnung => Bilde die UCs ab auf Smart Grid Architecture Model (SGAM) suggested by the WG Reference Architecture

EU-extension of NIST-Modell

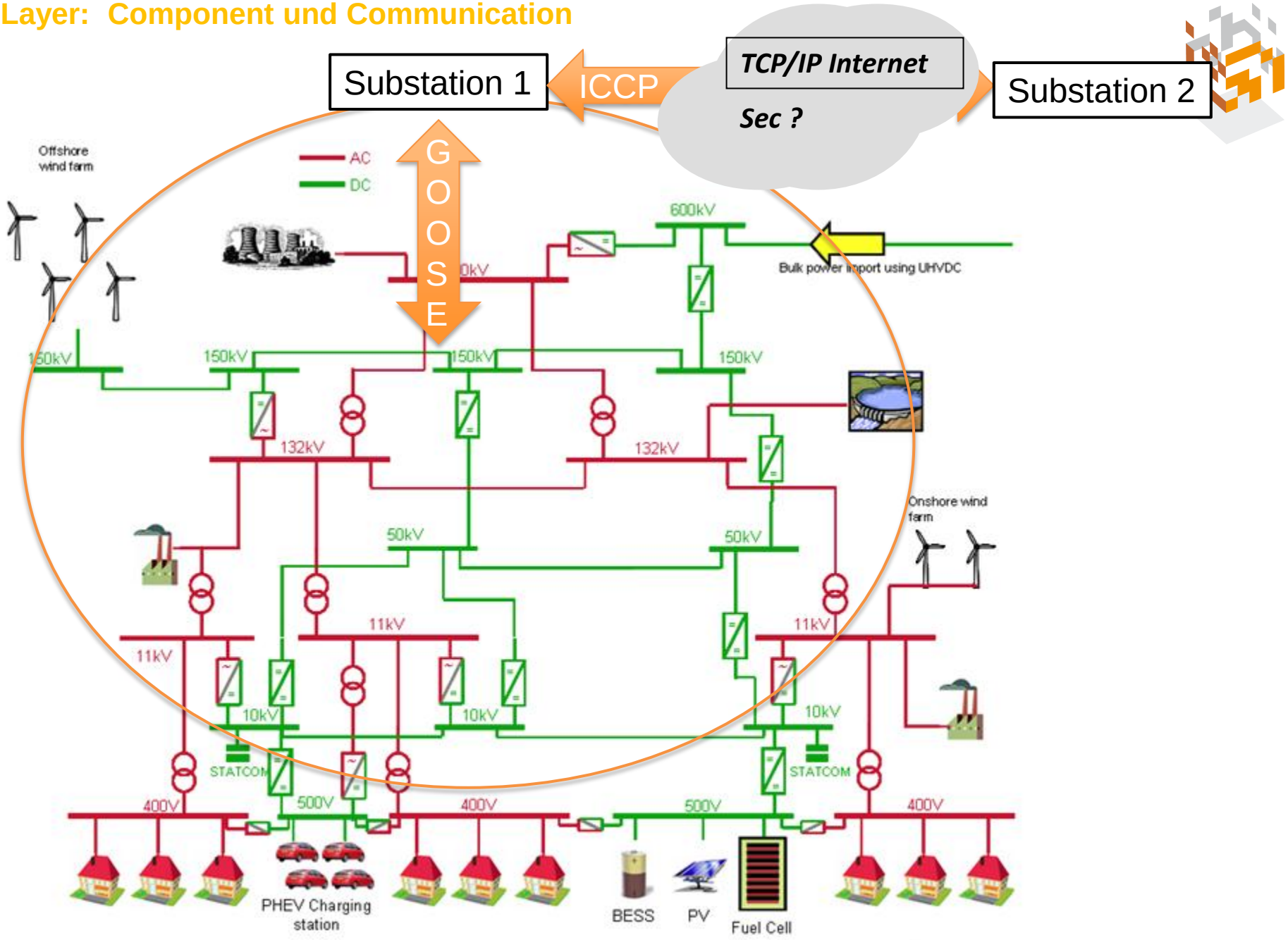




SGAM Smart Grid Architecture Model



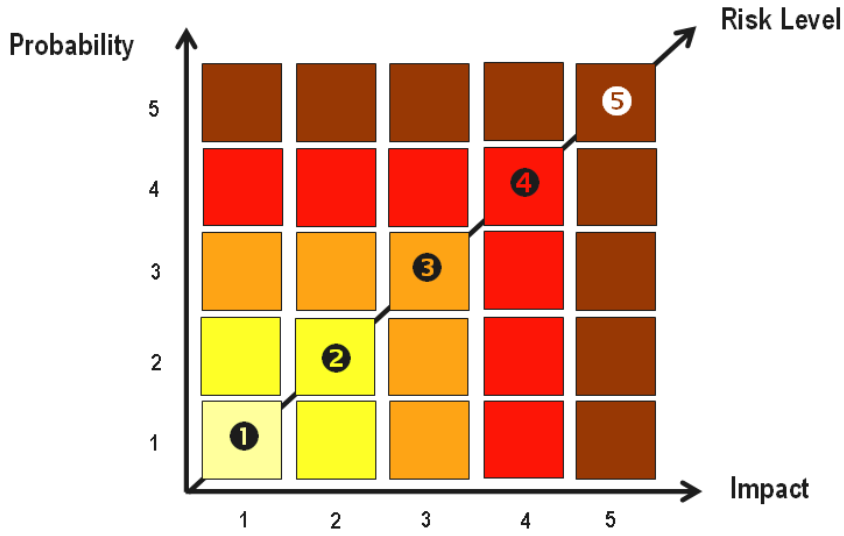
Layer: Component und Communication



- **Schritt 3**: welche Sec Anforderung ? => nimm Toolbox und identifiziere Security Level SGIS-SL

REQUIRED SGIS-SL						
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	MARKET	ZONES
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	ENTREPRISE	
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	OPERATION	
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	STATION	
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	FIELD	
5 - 4	5 - 4	5 - 3	4 - 3	4 - 2	PROCESS	
GENERATION	TRANSMISSION	DISTRIBUTION	DER	CUSTOMER		
DOMAINS						

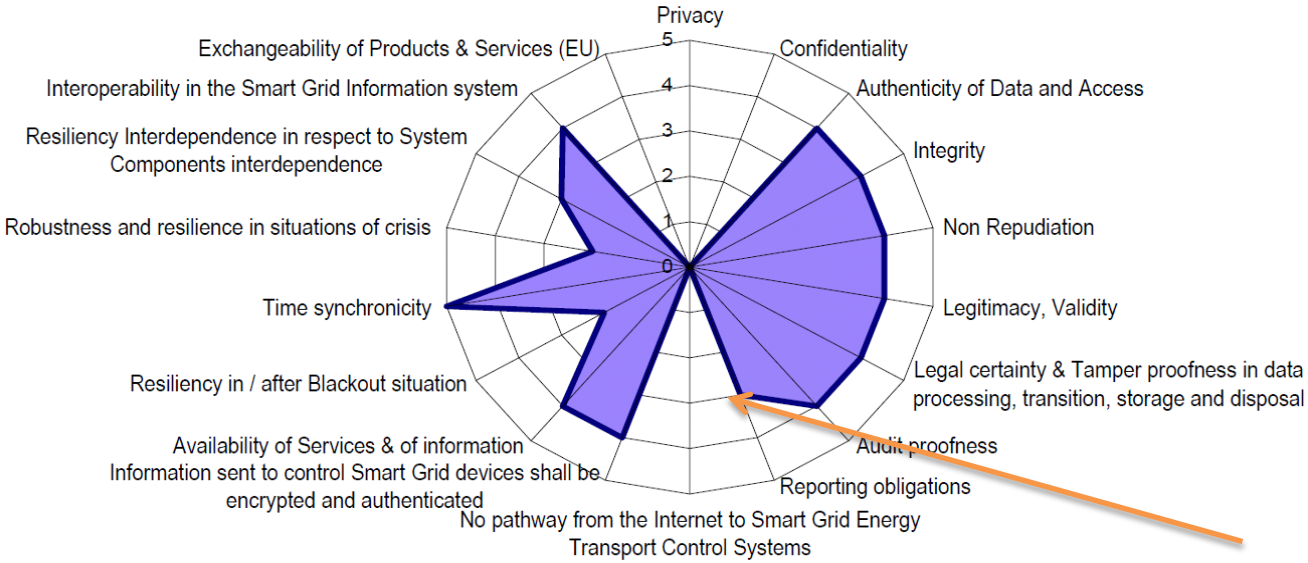
- **Schritt 4** : Ist das SGIS-SL mit den vorhandenen Standards zu ermitteln ?
  Oder fehlen Standards ?



- <u>Normalfall komplexe Systeme</u>
- Subsystem ergeben SecLevel
- Anwendung Max_Methode „Worst Case“
  - Risk_Subsystem = Max. {Probability, Impact}
  - nimm von allen Subsystemen max. Risk
  - = SGIS-RIL Risk Impact Level
  - ? im erlaubten „grünen“ Bereich

2.2. Beispiel: System Time Sync mit 2 Subsystemen

- Anforderungen erfüllt ?
  - **Angenommen** wir kennen: Impact substation time sync auf (reporting=3)



- dazu: Probability Threat:

LEVEL	VALUE	DESCRIPTION OF CLASSIFICATION
Daily	4	A threat occurs at least **daily**.
Weekly	3	A threat occurs at least **weekly**.
Monthly	2	A threat occurs at least **monthly**.
Annual	1	A threat occurs at least **annually**.
Rare	0	A threat occurs **less than once a year**.

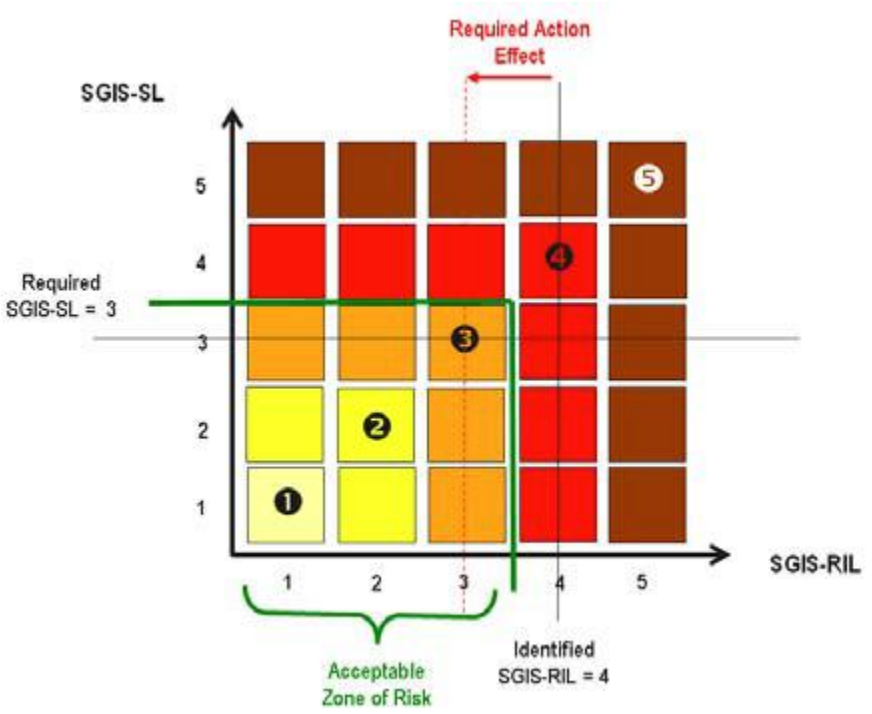
Zahlenbeispiel SGIS_Sec_Level für System Reporting für Windfarm (DER)

- Zone = alle
- Domain = Distributed Energy Resources DER
- Substation S1: Time_Sync: impact = 3, Probability = Daily = 4 => Risk_Subs. = max{3,4}=4
- Substation S2: Time_Sync: impact = 3, Probability = Weekly = 3 => Risk_Subs. = max{3,3}=3

- => SGIS_Risk_Level = max{3,4}=4

- Anforderung s. Tabelle DER = 4...3

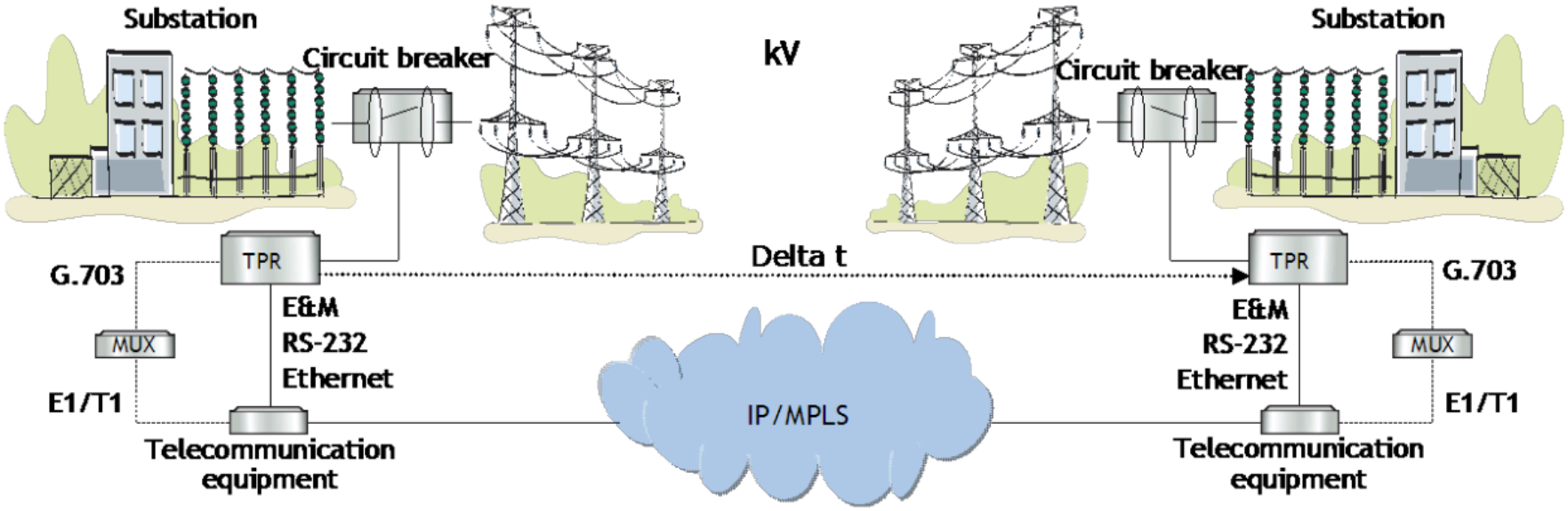
- **=> Risiko gerade noch akzeptabel**
- *Sonst z.B. SL=3:*
  Handlungsbedarf Required Action =>



3. Was fehlt: Risiko-Bewertung Internet-Infrastruktur Availability of QoS

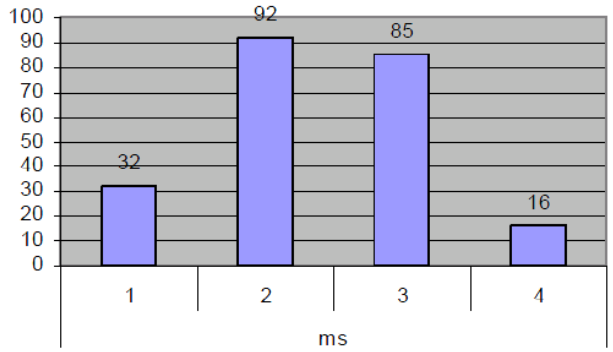
- **Nehmen: Use Case Teleprotection „***…quickly and reliably detecting a (power) network fault and then ensuring the faulty equipment is isolated before the fault has a greater effect on the grid.“*

- Security Level := Garantie Übertragungsdauer < 1/50…60 = 20 …16 ms



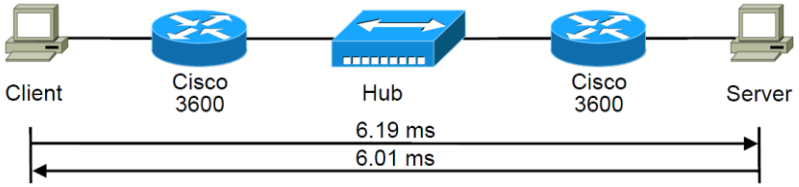
End-to End Delay ist Summe

- Zeit für Sensor- und Schaltungssysteme (Tester: OMICRON)
- Zeit für Übertragung in Substation (SCADA): GOOSE (Generic Object Oriented Substation Events) Protocol (ABB,..)



- Zeit für Übertragung Inter-Substation /SANDIA 2007 Secure ICCP Integration Considerations and Recommendations/
  - Software Stack: Sec, UnSec: 0.8 … 1.2 ms
  - IPSec

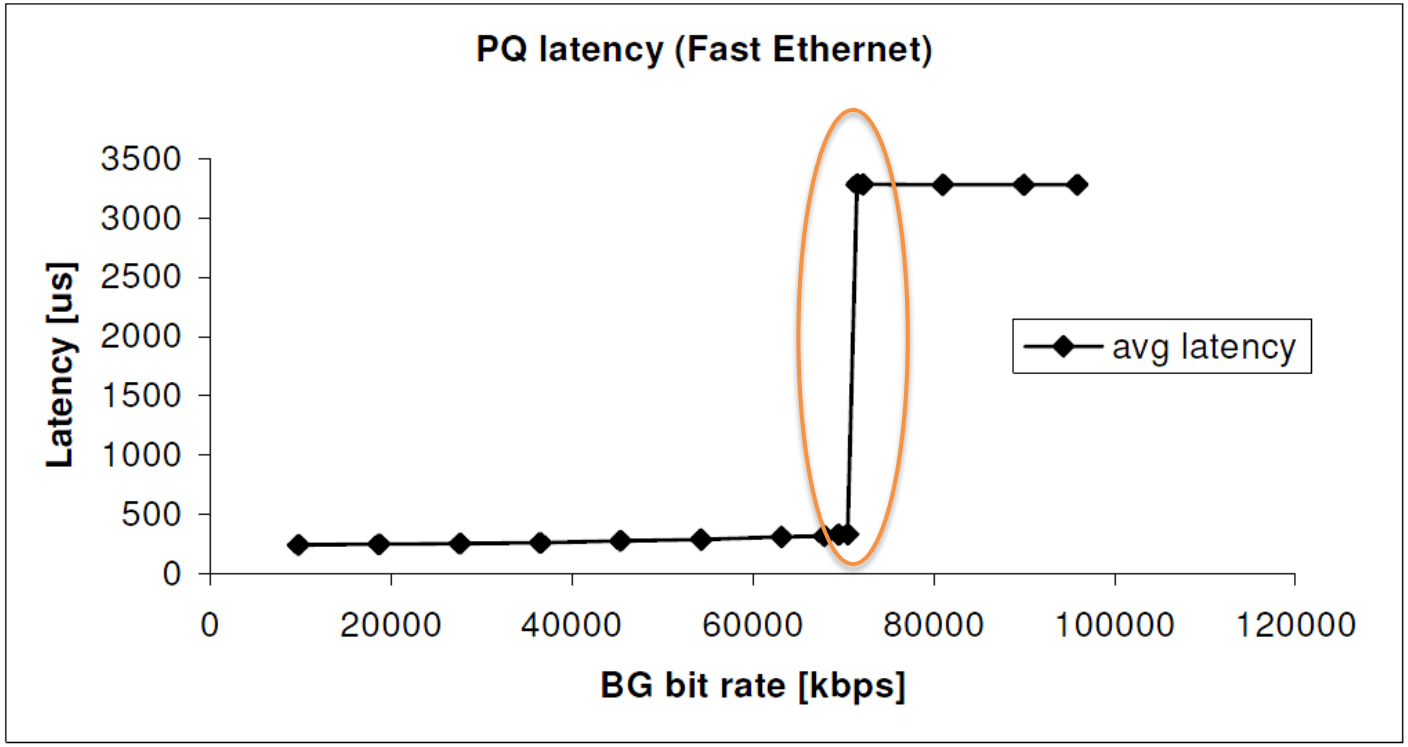
5 + 1 + 6 = 12 **< 16 ms**
(ohne Querlast*)



- *=> DiffServ/BestEffort für **NIST Availability:** *A requirement intended to ensure that systems work promptly and service is not denied to authorized users.*

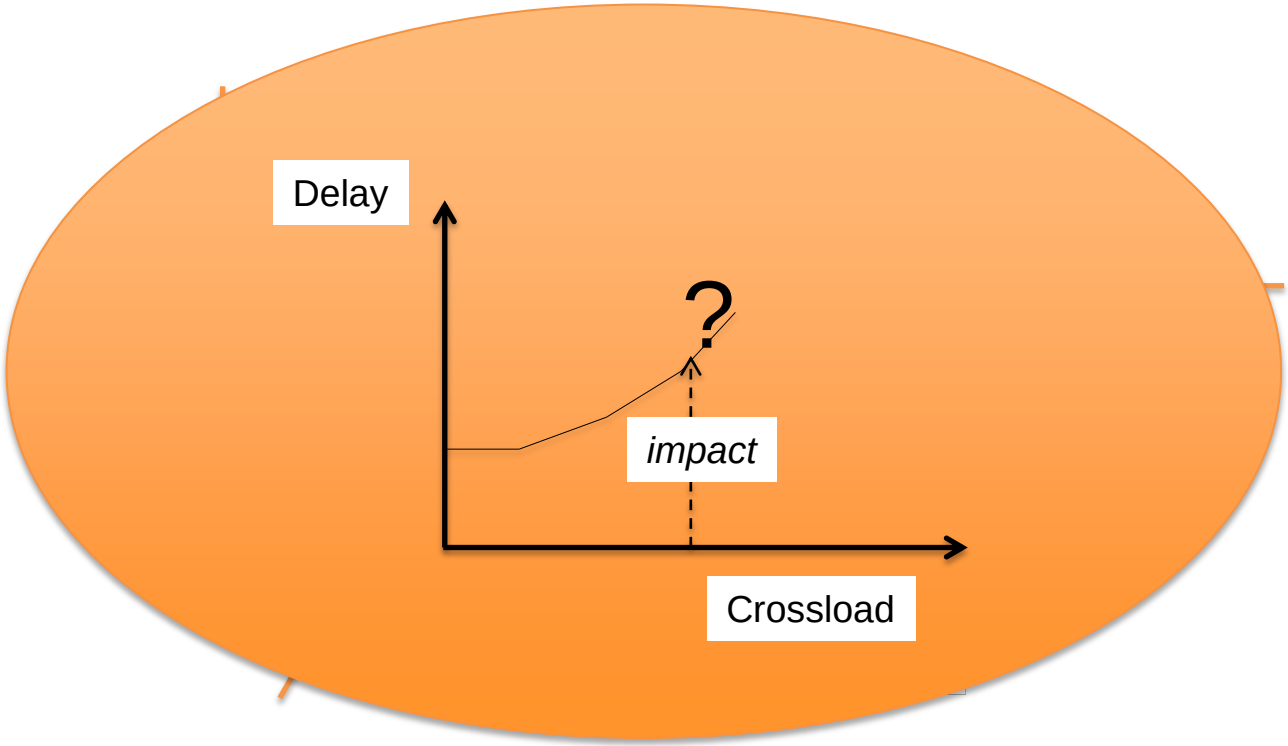
Wie groß ist Risiko für Delay > 16 ms ?

1 Subsystem: 1 Router



Erhöhung der Verzögerung für autorisierten priorisierten Paketstrom
bei Erhöhung Intensität nicht autorisierter Paketstrom

Und dies nicht nur für ein Subsystem, sondern für Netze



SGIS-SL :=

- 2 if P(delay >16 ms) = 0 !
- …
- 5 if P(delay > 16 ms) = 0.001 !

4. SRFG MINER Testen und Monitoren für Secure Integration of Smart Grid Communication

- **Testen und Monitoren kritischer Internet-Infrastrukturen**

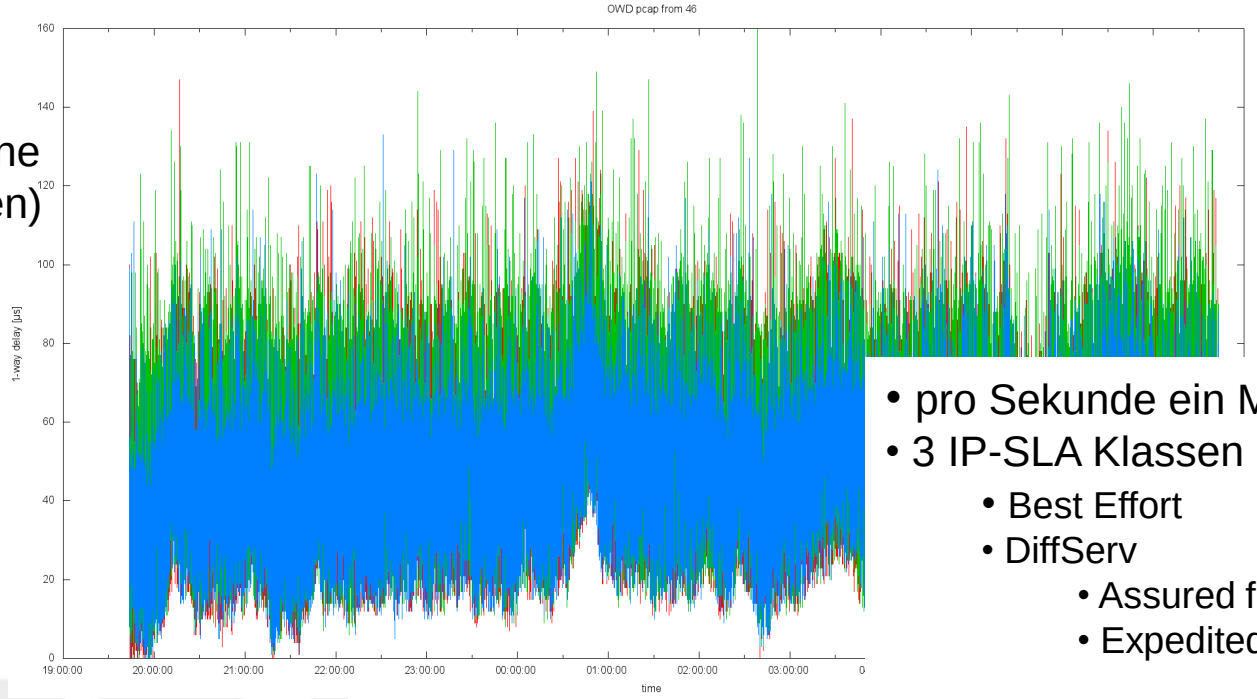
- **Motivation:**
  - Robustheit autorisierter Traffic gegen DDoS = Load Test
  - Komponenten-Test Metriken + Verfahren von IETF BMWG abgedeckt
  - Netztest nur Metriken von IETF IPPM, keine Verfahren
  - Unklar: harte Netztests
  - wenig: verteilte Tests im operationellen Netz
  - Integration in Netzprotokolle (z.B. MPLS-TP OAM-Pakete) ?
    - Ja für private Netze SLA
    - Nein, wenn Third-Party-Netz z.B. Telekom‘s (Wer trägt Verantwortung am Ende = Nutzer des Netzes ! = Energie-Provider)

Einsatzfall kritische Infrastrukturen

- **dyn. Evakuierungssystem**
  - Broadcaststurm zu Evakuierungstafeln legt Netz lahm, mit Messungen entdeckt

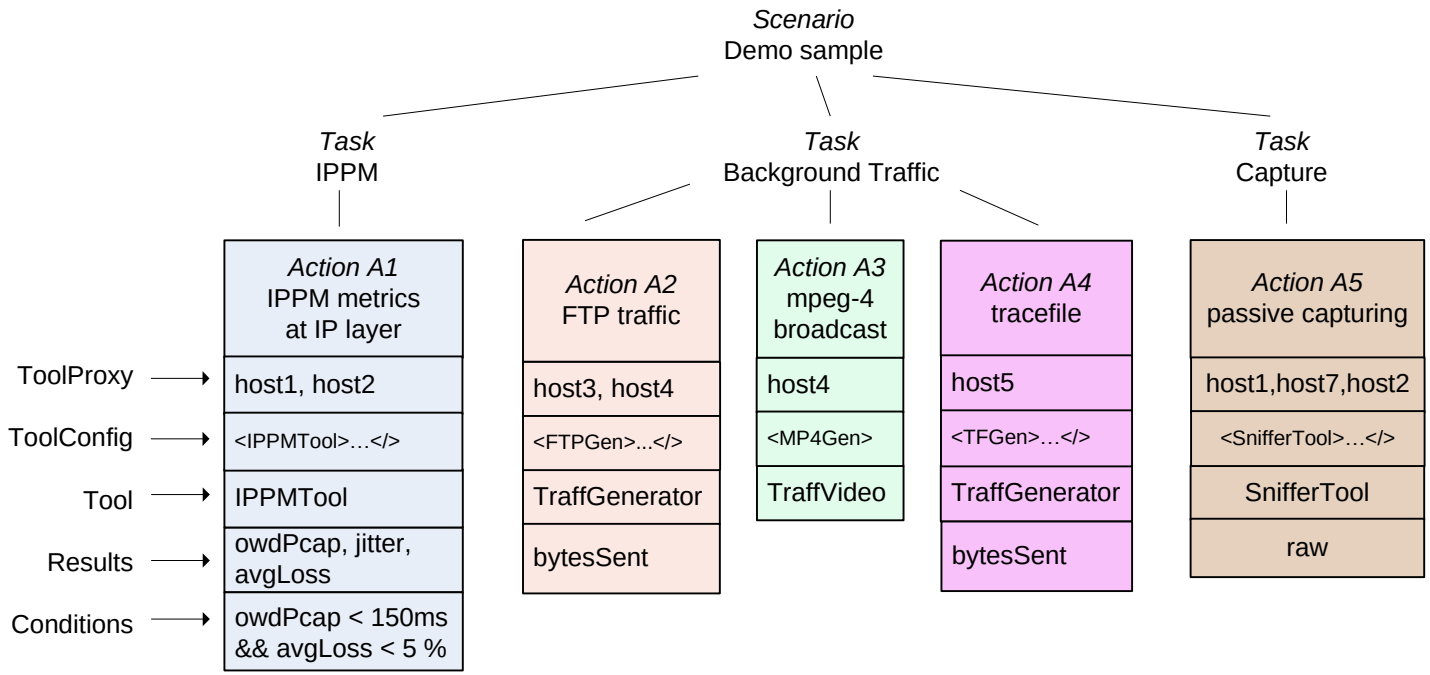
- **Polizeinetz Hessen:** Umstellung von ISDN auf IP-Technologie
  - Sicherung der Availability mit 2-Jahres-Test
  - Testen Stabilität „authorised user“ vs. „non authorised user“

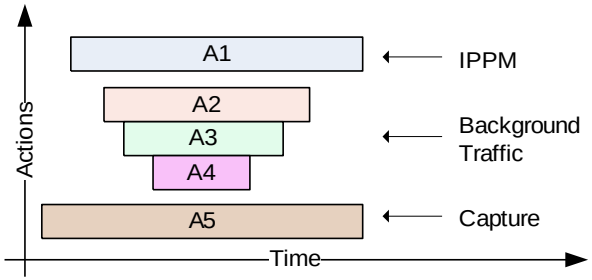
140 µs
(noch keine
Querlasten)



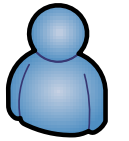
- pro Sekunde ein Messpaket
- 3 IP-SLA Klassen
  - Best Effort
  - DiffServ
    - Assured forwarding
    - Expedited forwarding

SRFG MINER Scenario (Christof Brandauer)





Phase 1: Specification

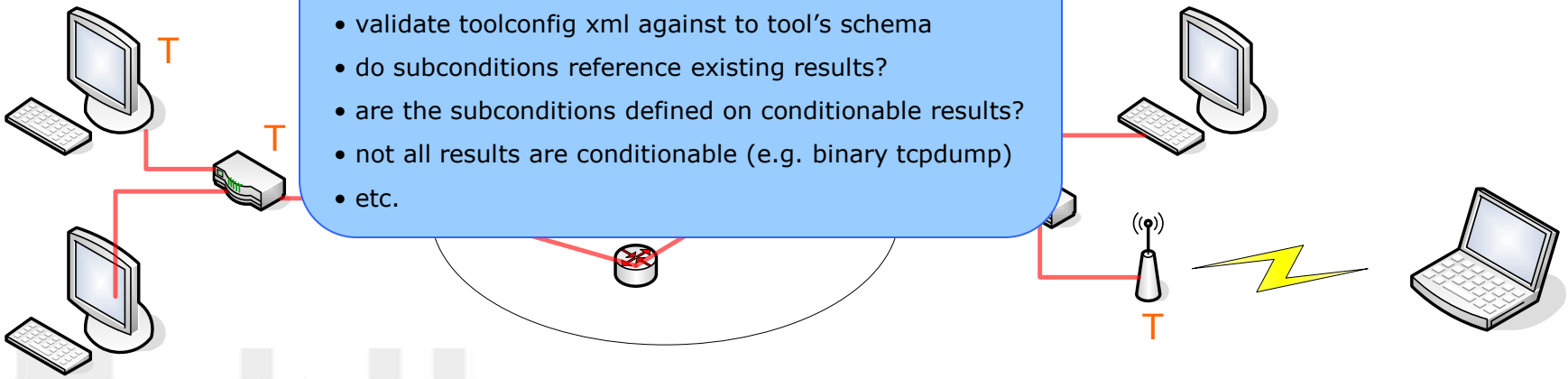


schedule

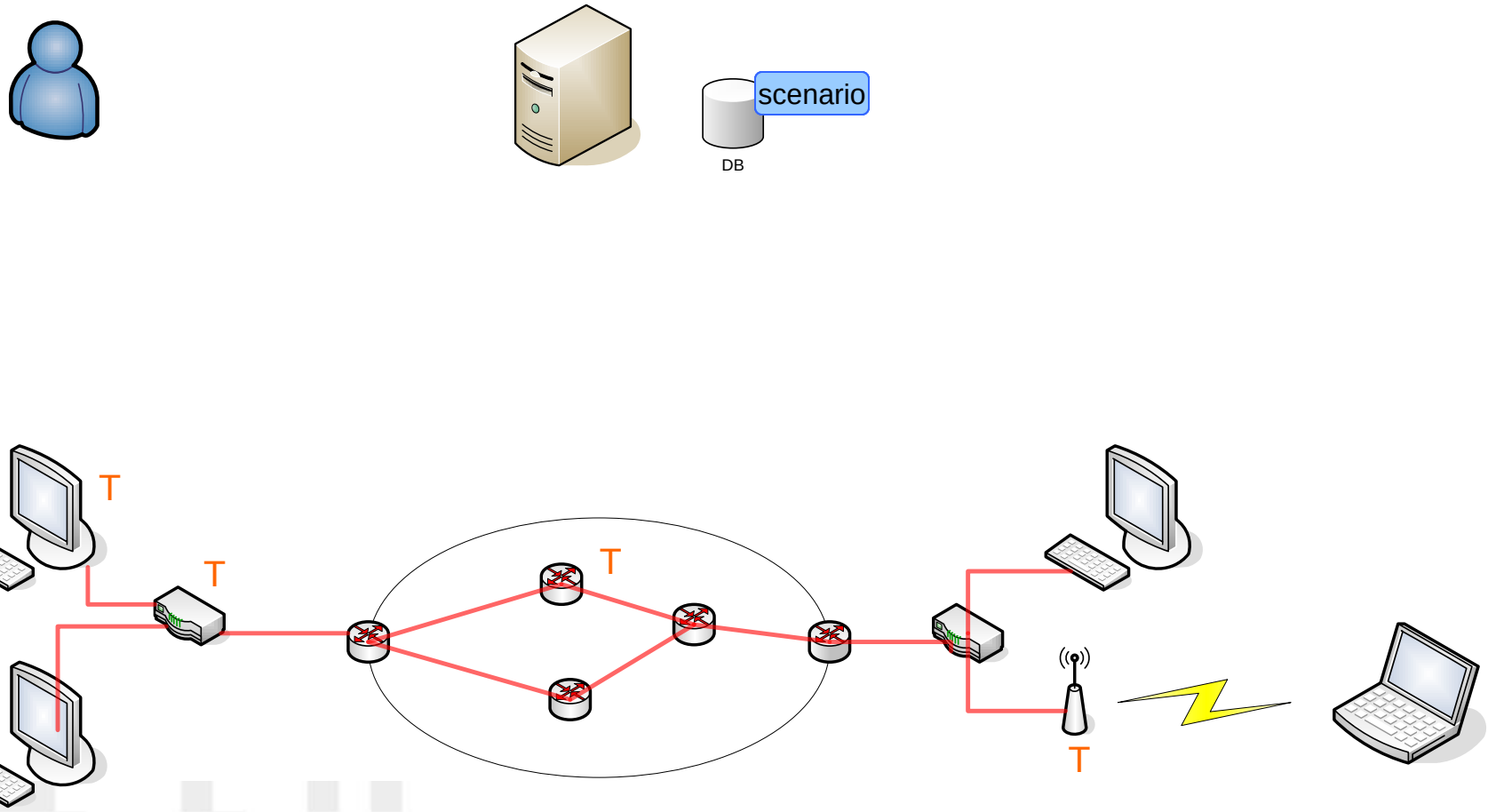
DB

Verification

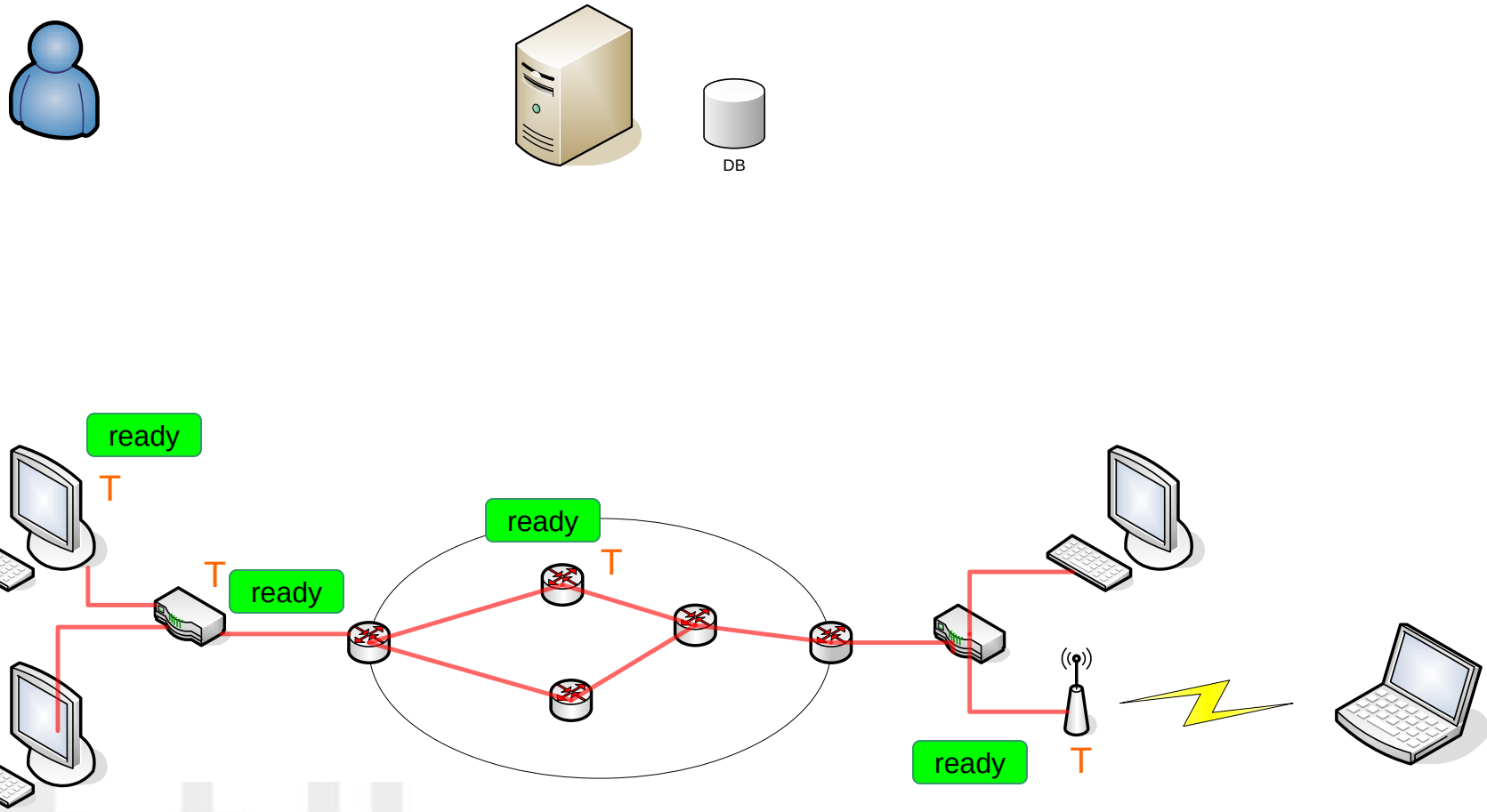
- for each tool: is the config valid?
- validate toolconfig xml against to tool's schema
- do subconditions reference existing results?
- are the subconditions defined on conditionable results?
- not all results are conditionable (e.g. binary tcpdump)
- etc.



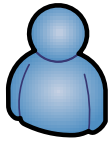
Phase 2: Deployment



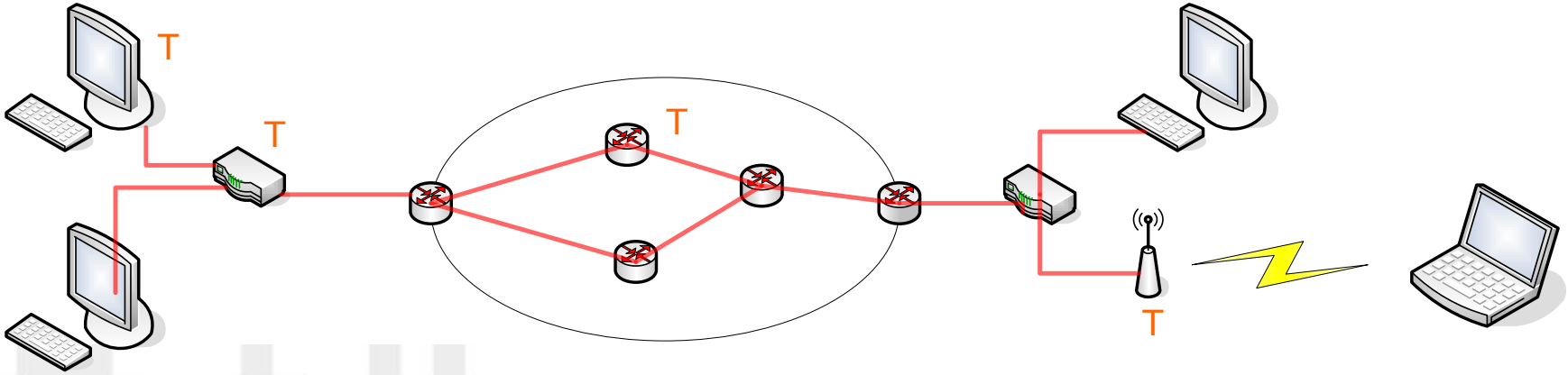
Phase 2: Deployment



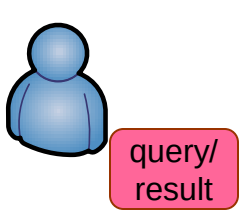
Phase 2: Deployment

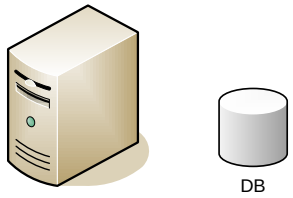


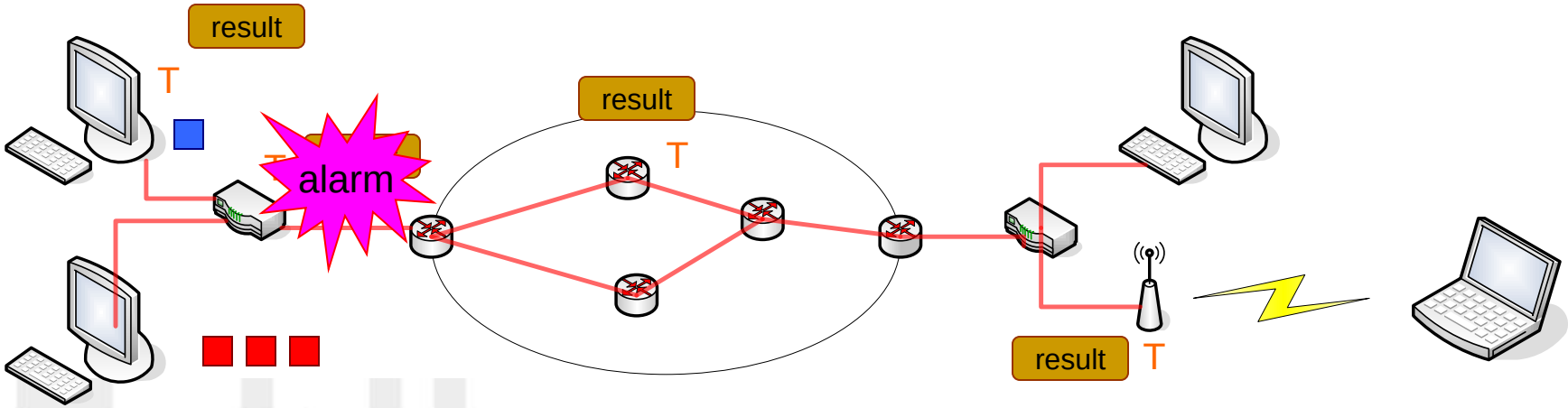
all ready



Phase 3: Execution







4. 2012/2013: SRFG MINER Einsatz in Securing Integration SG Com

- **Beiträge in VDE-ITG 2012**
- **Österreich: über Modellregion Salzburg => bmvit**
- **Cross-Layer Kopplung MINER**
  - Nach „oben“ zu IEC Protokoll-Tester:
    - Um wieviel langsamer wird ICCP bei Querlast ?
    - Optimierte DiffServ Konfiguration (ICCP = Multimedia !)
    - ICCP Lastgenaratoren
  - Nach unten zu Hardware-Tester
    - Um wieviel langsamer wird Reaktion von Leitungsbruch-Sensor zu Trafo, Leitungs-Switch bei Netzlasten

Vielen Dank für Ihre Aufmerksamkeit!

salzburgresearch

U. Hofmann
Salzburg Research Forschungsgesellschaft m.b.H.
Jakob-Haringer-Straße 5/III | Salzburg, Austria
Tel. +43 662 2288-000 | Fax +43 662 2288-222
ulrich.hofmann@salzburgresearch.at