anapur AG

SITUATION-ADAPTIVE MACHINE COMMUNICATION CONTROL IN INDUSTRIAL NETWORKS

KRITISCHE PROZESSE IN SICHEREN HÄNDEN

Sicherheit und Qualität liegen uns am Herzen

Seit mehr als 20 Jahren steht anapur AG für Automatisierungstechnik, OT, produktionsnahe IT, Cybersicherheits- und (GxP-)Qualitätsmanagement für operative/physische Prozesse – v.a. in den Branchen pharmazeutische und chemische Industrie, Gesundheitswesen, Energiesektor, Bahn – und arbeitet mit führenden Unternehmen der Industrie & öffentlichen Hand zusammen.

GMP-Consulting

Functional Safety

OT-Security

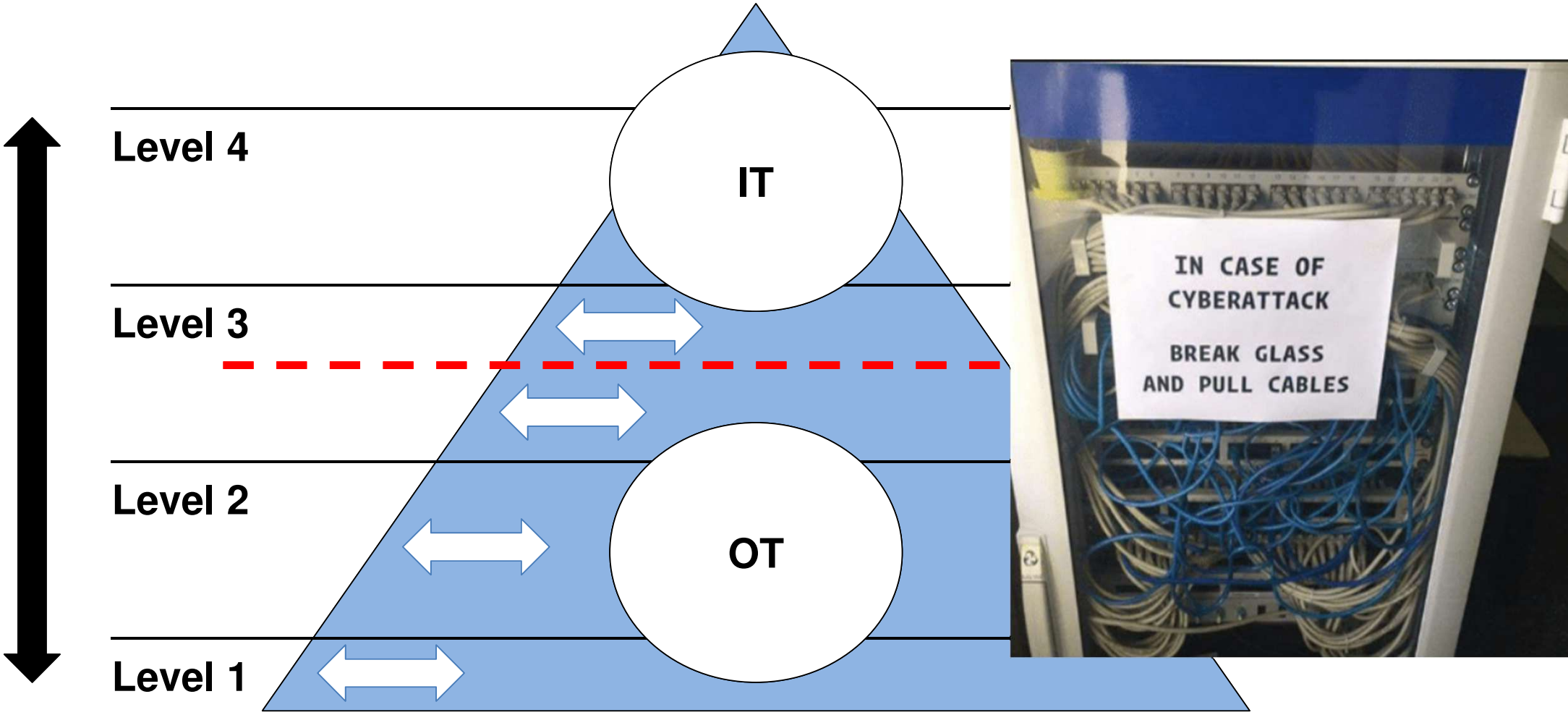
Projektmanagement

anapur AG

THEMEN

- Communication in industrial networks
- Handling of cyber-incidents in industrial networks
- Communication control – a preventive and emergency measure
- Current situation and first steps

COMMUNICATION IN INDUSTRIAL NETWORKS

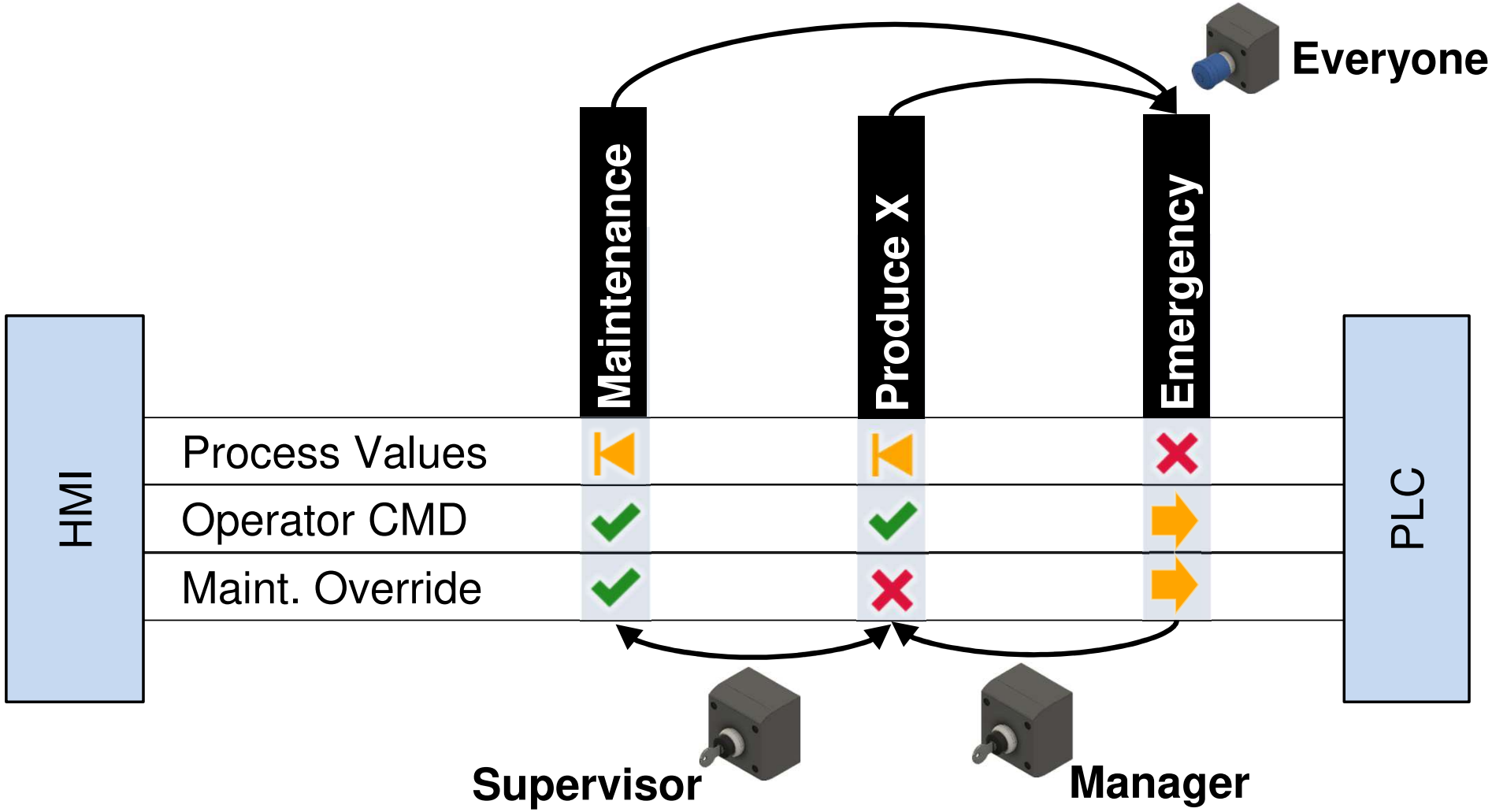


COMMUNICATION CONTROLS

CONTROLS

- Blocked
- Full
- Uni-directional
- Forced

COMMUNICATION CONTROL



CYBER-INCIDENTS IN INDUSTRIAL NETWORKS

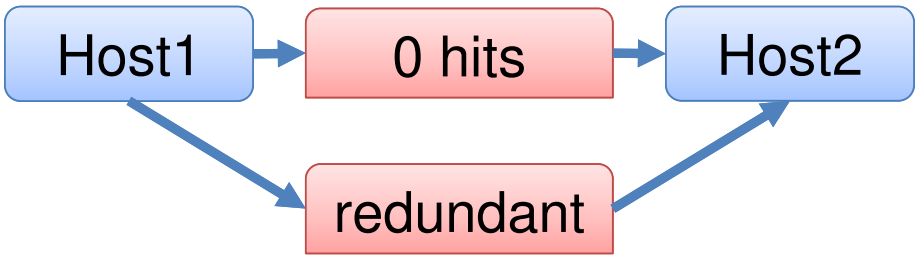
- Wie erkenne ich es überhaupt?
- Wer erkennt es?
- Wie schnell müsste reagiert werden und wie vermeide ich falschen Alarm?
- Regelwerk zur differenzierten Betrachtung
  - Gewichtung der Beobachtung
  - Gewichtung des Beobachtenden
  - Berücksichtigung des „Zustandes“ der Produktionsanlage
  - Zeitlicher Kontext und Korrelation
- Regelwerk zur gestaffelten Einschränkung der Kommunikation

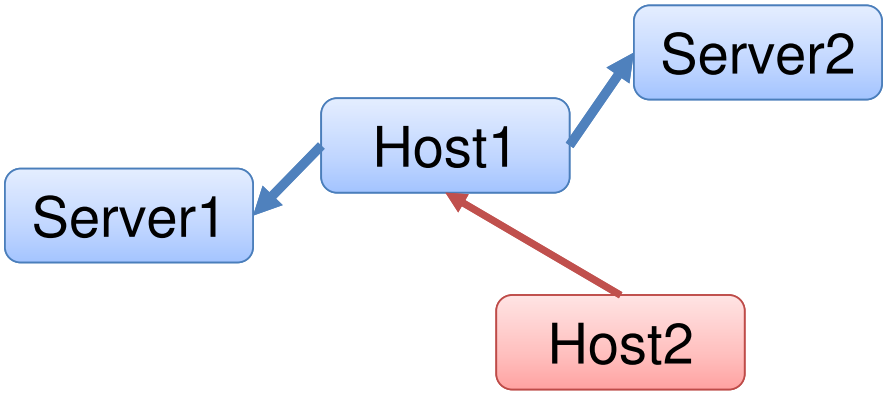
CURRENT SITUATION & FIRST STEPS

- Firewall
- Rules
- Management/Review

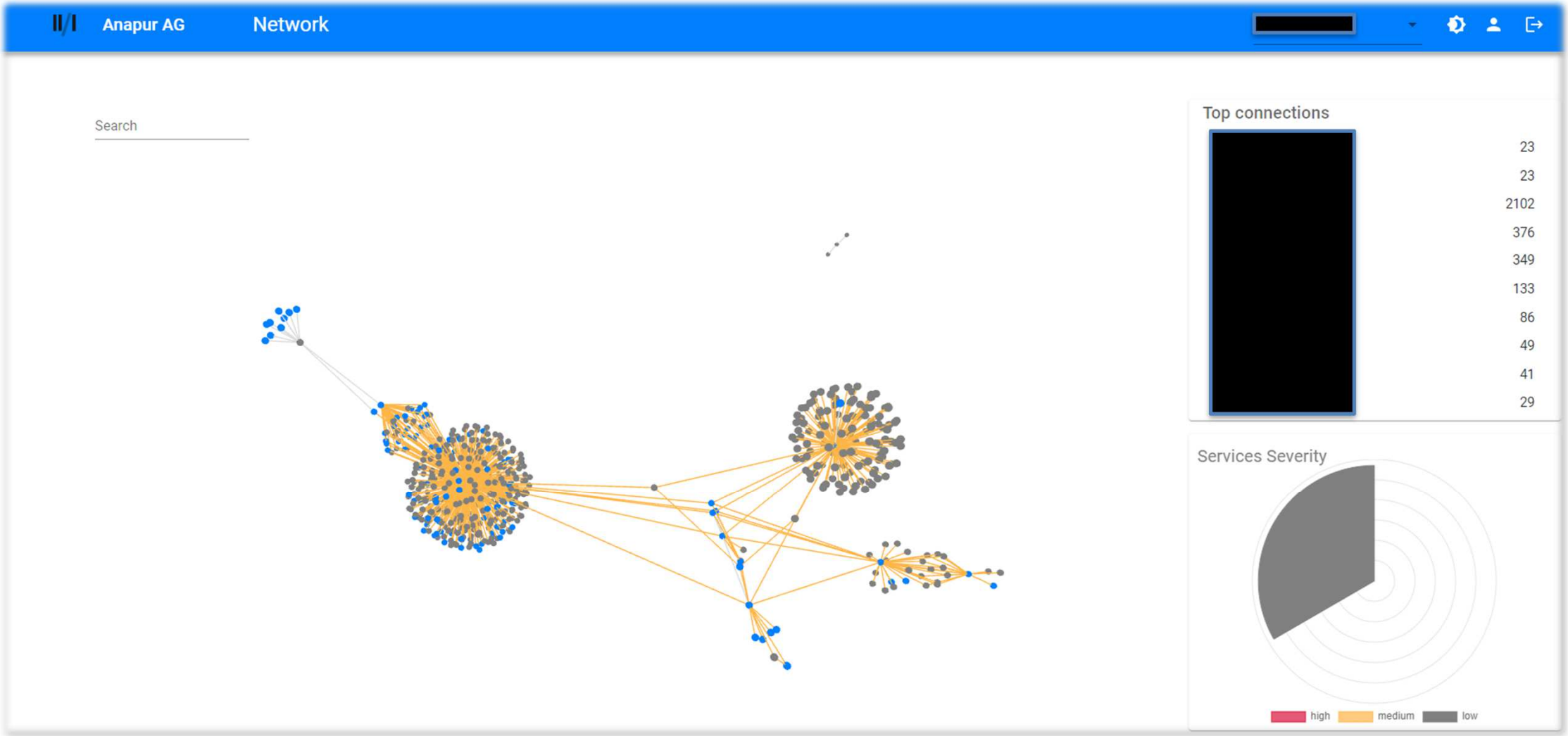
- Good to have
  - Systematic approach to enhance security (and performance)
  - Visualization and deep analysis of firewall configurations
  - Centralized storage and management of firewall rules

REVIEW OF FIREWALL RULES

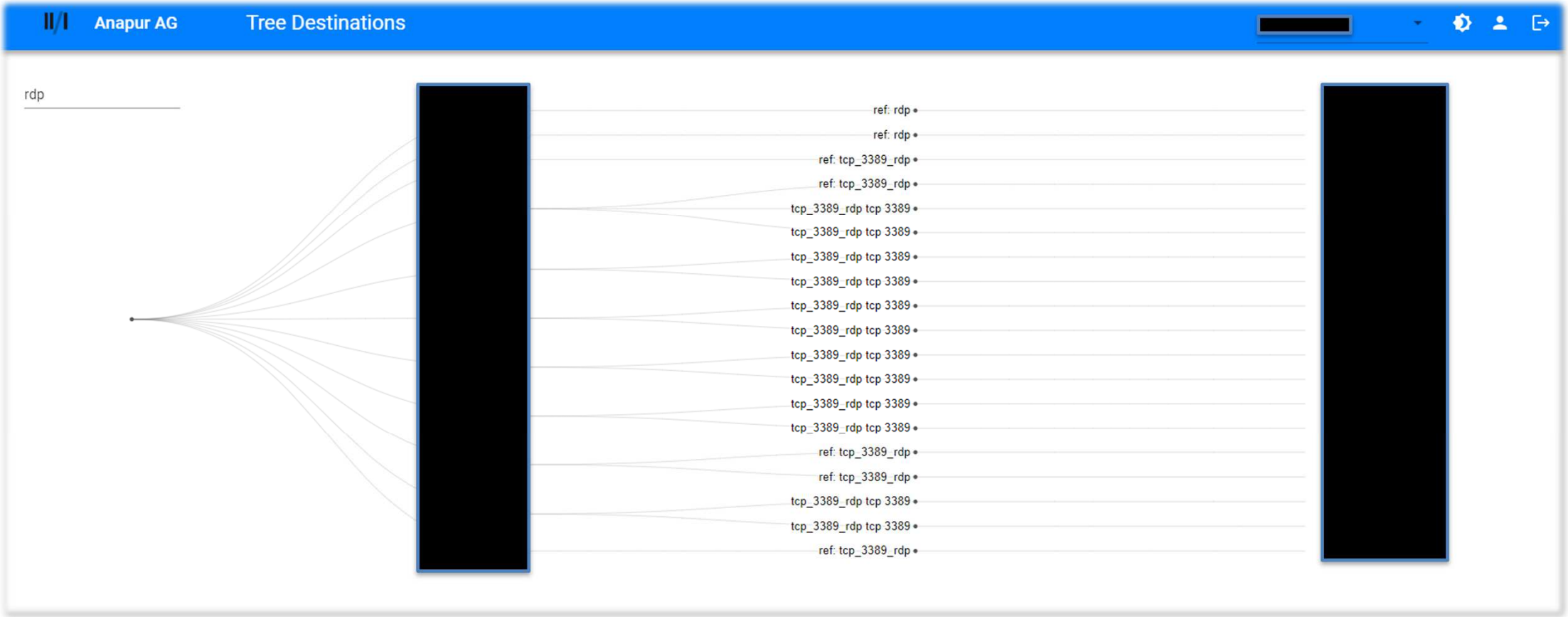




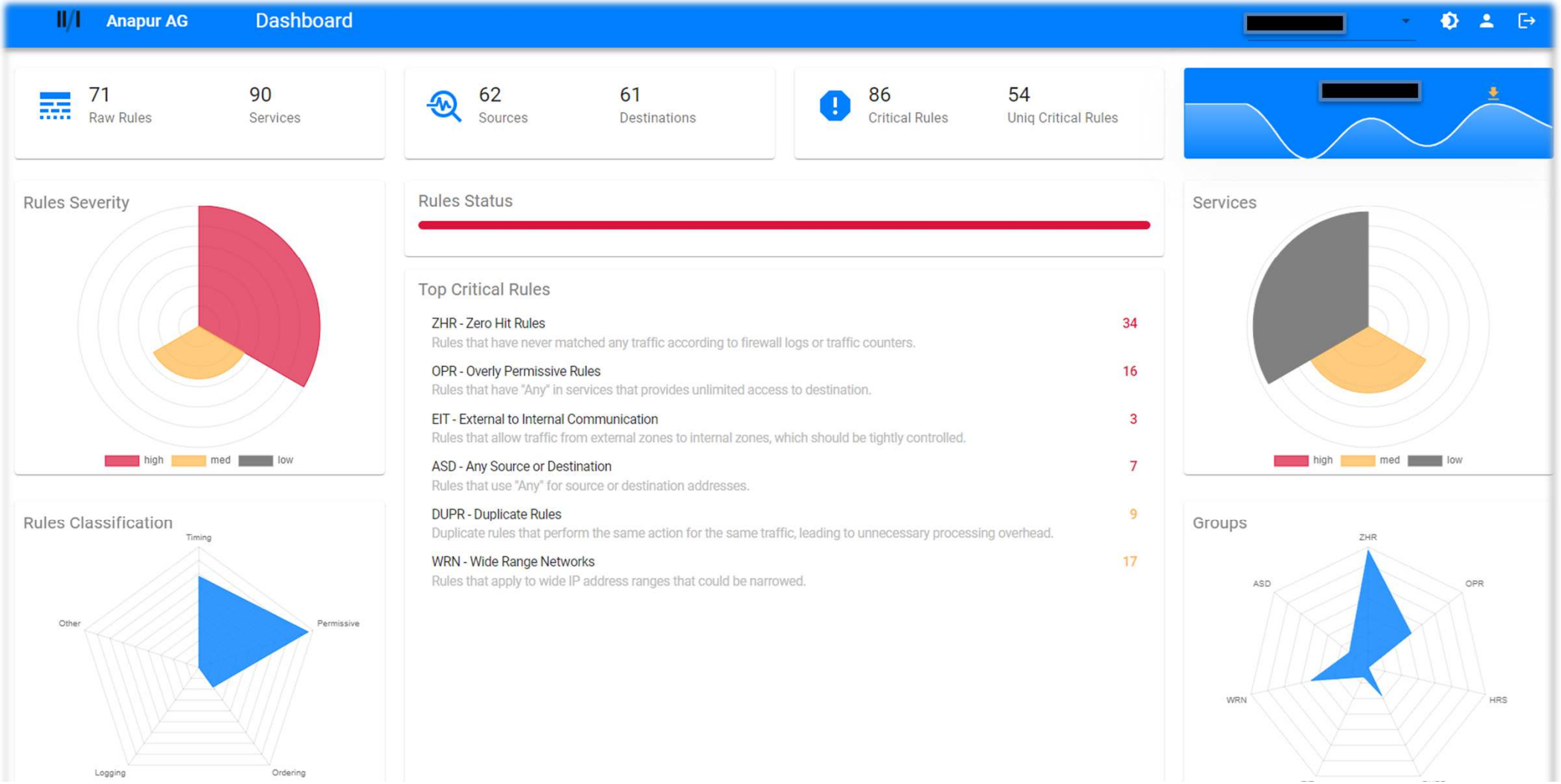
NETWORK VISUALIZATION



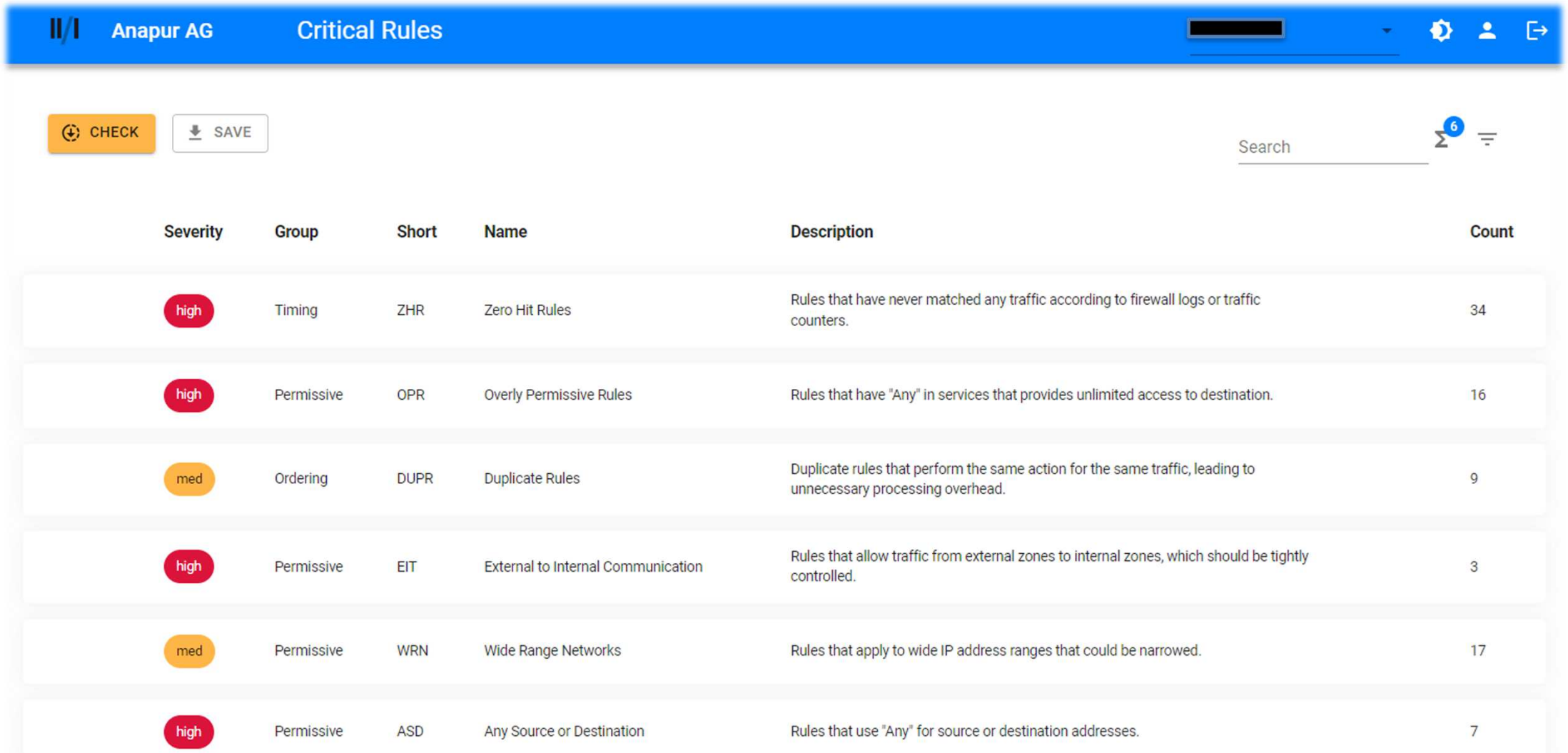
ANALYZING OPEN PORTS



OVERVIEW DASHBOARD



EXAMPLE OF CRITICAL RULES



Severity	Group	Short	Name	Description	Count
high	Timing	ZHR	Zero Hit Rules	Rules that have never matched any traffic according to firewall logs or traffic counters.	34
high	Permissive	OPR	Overly Permissive Rules	Rules that have "Any" in services that provides unlimited access to destination.	16
med	Ordering	DUPR	Duplicate Rules	Duplicate rules that perform the same action for the same traffic, leading to unnecessary processing overhead.	9
high	Permissive	EIT	External to Internal Communication	Rules that allow traffic from external zones to internal zones, which should be tightly controlled.	3
med	Permissive	WRN	Wide Range Networks	Rules that apply to wide IP address ranges that could be narrowed.	17
high	Permissive	ASD	Any Source or Destination	Rules that use "Any" for source or destination addresses.	7

BOTTOM LINE

- Communication control in industrial networks
  - Who is allowed to talk with whom
  - About what subject
  - In which situations (operational state, incidents)
- Prevent avoidable vulnerabilites and know how to react
- Management and review of (static) OT-Firewalls rules
  - Enhanced security
  - Improved efficiency
  - Compliance

anapur AG

WWW.IT-MEETS-INDUSTRY.DE

anapur AG

SITUATION-ADAPTIVE MACHINE COMMUNICATION CONTROL IN INDUSTRIAL NETWORKS

Vielen Dank für Ihr Interesse an Sicherheit!

Harald Gattermeyer
anapur AG Region Wien

+43 (0)664 9277614
h.gattermeyer@anapur.de