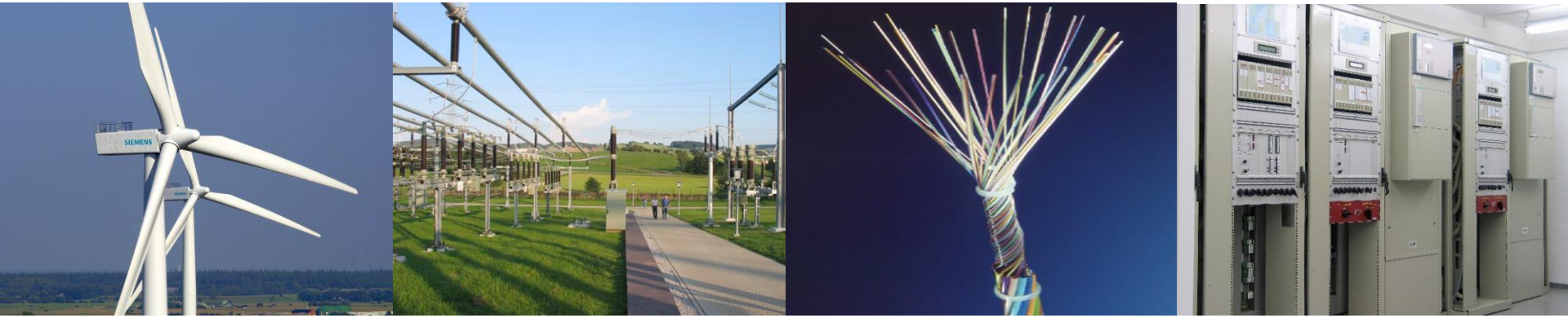


SICIA-Teilprojekt
SIPRO-U

Security **I**ndicators for **PRO**cess control systems specific to the energy **U**tility industry

SIPRO-U - Security Indicators for PROcess control systems specific to the energy Utility industry

- Verbundprojekt: SICIA - Security Indicators for Critical Infrastructure Analysis
  - RWE Teilprojekt SIPRO-U
- Aktuelle gesetzliche Regelungen machen gesetzeskonforme Sicherheitsverfahren und Schutzmaßnahmen verbindlich
- Erfahrungen zeigen, dass die Einführung, der Betrieb und die Anpassung an neue Anforderungen der Sicherheitsprozesse je nach Sicherheitslevel schnell kompliziert, aufwändig und teuer wird
- SIPRO-U soll ein effizientes und in der Praxis gut anwendbares Verfahren zur Bewertung der Leistung eines ISMS nach ISO/IEC 27001 beschreiben und evaluieren

Bewertung der Leistung eines ISMS nach ISO/IEC 27001 (Auszug aus der Norm)

Die Organisation muss die **Informationssicherheitsleistung** und die **Wirksamkeit des Informationssicherheits-managementsystems** bewerten.

Die **Organisation muss bestimmen**:

a) **was überwacht und gemessen werden muss**, einschließlich der **Informationssicherheitsprozesse** und **Maßnahmen**;

b) die **Methoden zur Überwachung, Messung, Analyse und Bewertung**, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

METROSEC

Forschungsprojekt zur Messung, Analyse und Bewertung von Managementsystemen für Informationssicherheit

Das GQMS-Vorgehensmodell für das Messen der Wirksamkeit von Informationssicherheitsmanagement-systemen

CONCEPTUAL PAPER

Eingereicht bei:

Herausgeber der Reihe Working Paper des IMB (Carsten Baumgarth, Gert Bruche, Christoph Dörrenbächer und Friedrich Nagel)

Autor: Prof. Dr. Rainer Rumpel

Es haben mitgewirkt:
Rolf-Dieter Kasper, RWE Deutschland AG
Peter Thanisch, RWE Deutschland AG
Lucas Pentzek, Hochschule für Wirtschaft und Recht Berlin

Bewerten der Effektivität der ISMS-Managementprozesse

- Datensammlung bzgl. Beispielen, Regelungen und Verfahren soll vervollständigt werden
- Die ISMS-Managementprozesse sollen bezüglich Durchgängigkeit und Vollständigkeit (unter Zertifizierungsgesichtspunkten) überprüft, einheitlich modelliert und mit der GQM-Methode messbar gemacht werden

Managementprozesse gemäß ISO/IEC 27001:2013

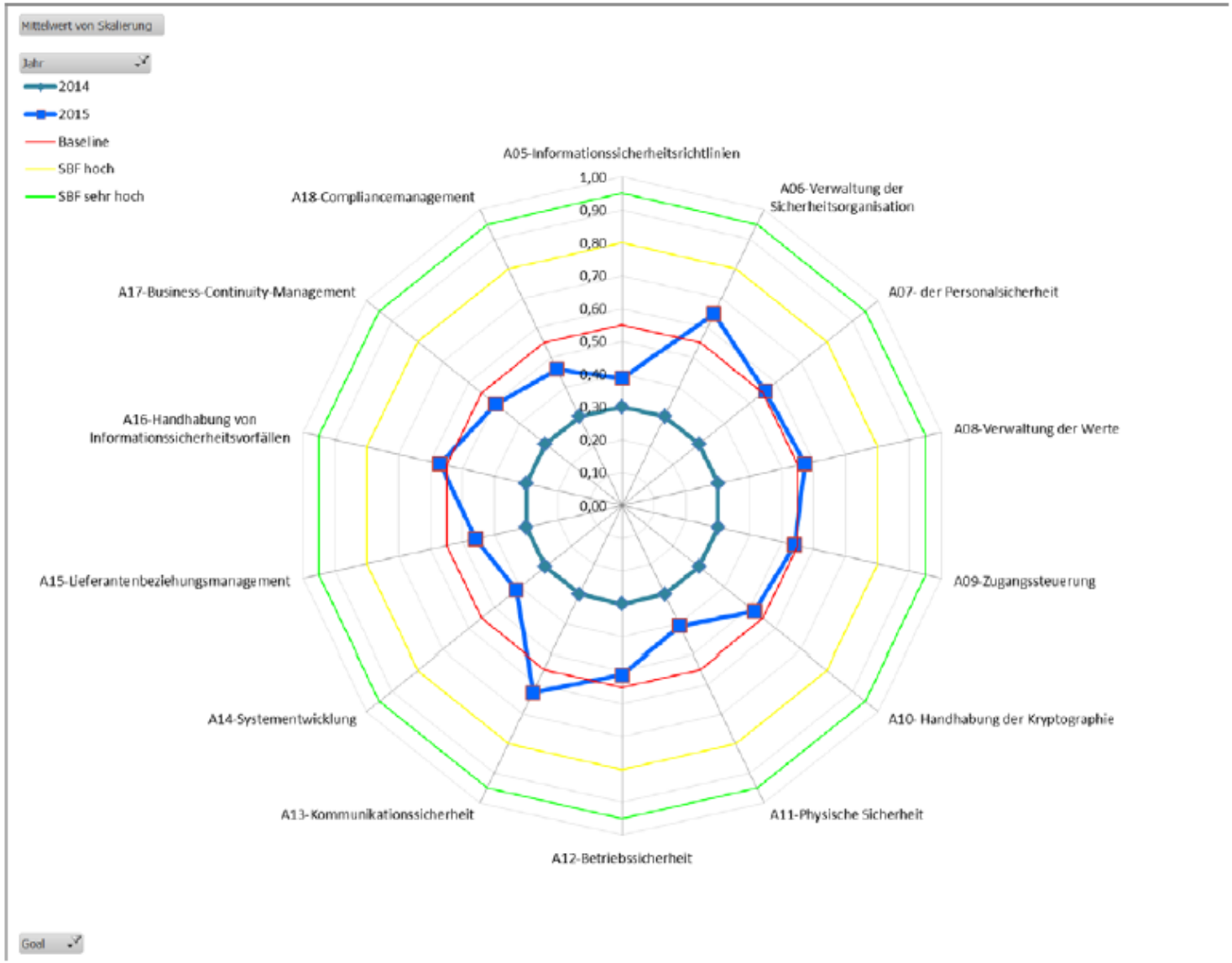
Kürzel	Bezeichnung
M1	Führung
M2	Planung
M3	Unterstützung
M4	Betrieb
M5	Bewertung
M6	Verbesserung

Informationssicherheitsleistung: Bewerten der Effektivität der Informationssicherheitsprozesse

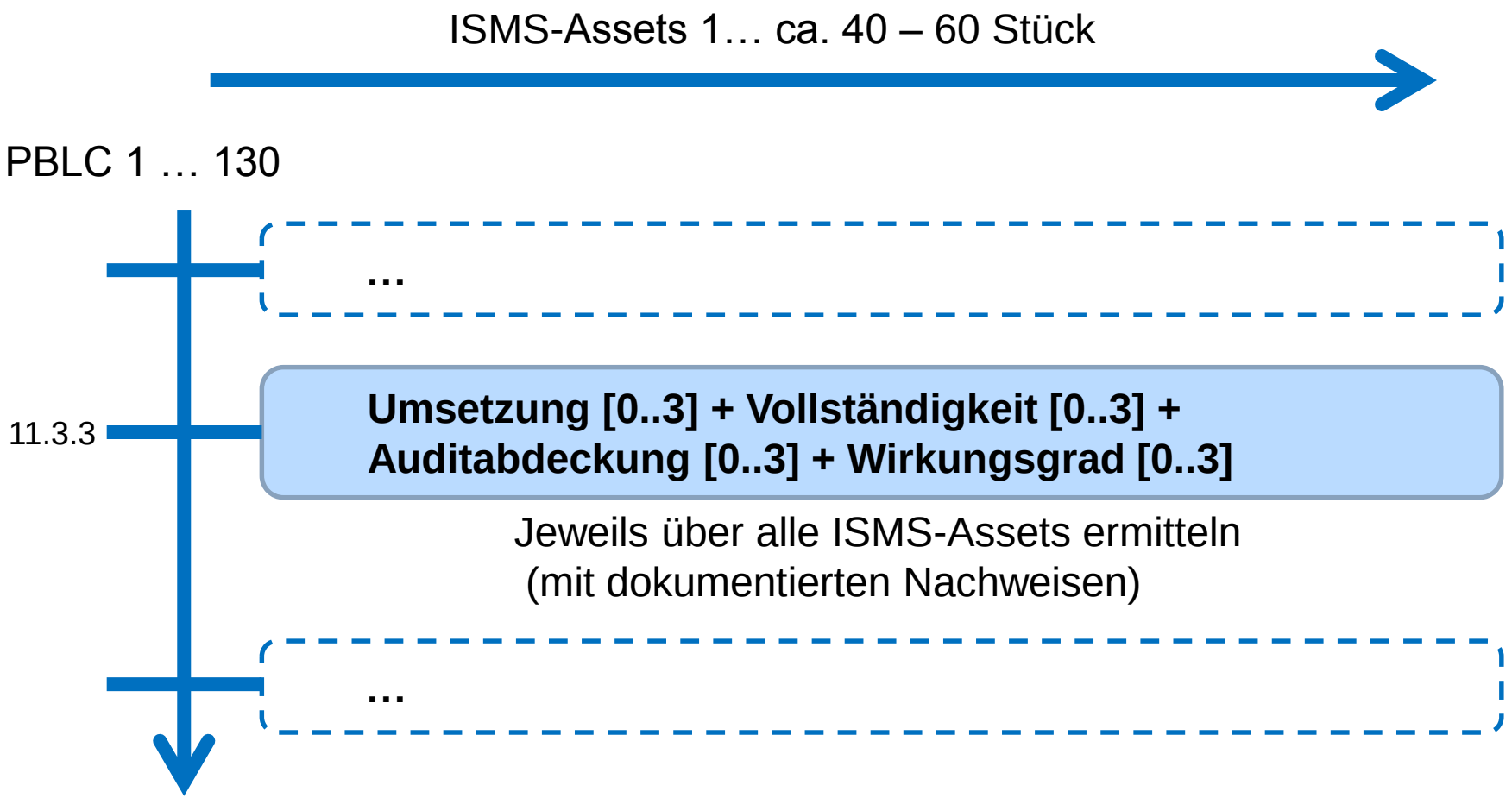
- Für die Informations-sicherheitsprozesse gemäß ISO/IEC 27001:2013 (Anhang A) werden unter Berücksichtigung der ISO/IEC TR 27019:2013 ein Messverfahren nach der GQM-Methode entwickelt

Bezeichnung	Quelle
Informationssicherheitsrichtlinien	A.5
Verwaltung der Sicherheitsorganisation	A.6
Management der Personalsicherheit	A.7
Handhabung der Unternehmenswerte	A.8
Zugangssteuerung	A.9
Handhabung der Kryptographie	A.10
Physische Sicherheit	A.11
Betriebssicherheit	A.12
Kommunikationssicherheit	A.13
Systementwicklung	A.14
Lieferantenbeziehungsmanagement	A.15
Handhabung von Informationssicherheitsvorfällen	A.16
Business-Continuity-Management	A.17
Compliancemanagement	A.18

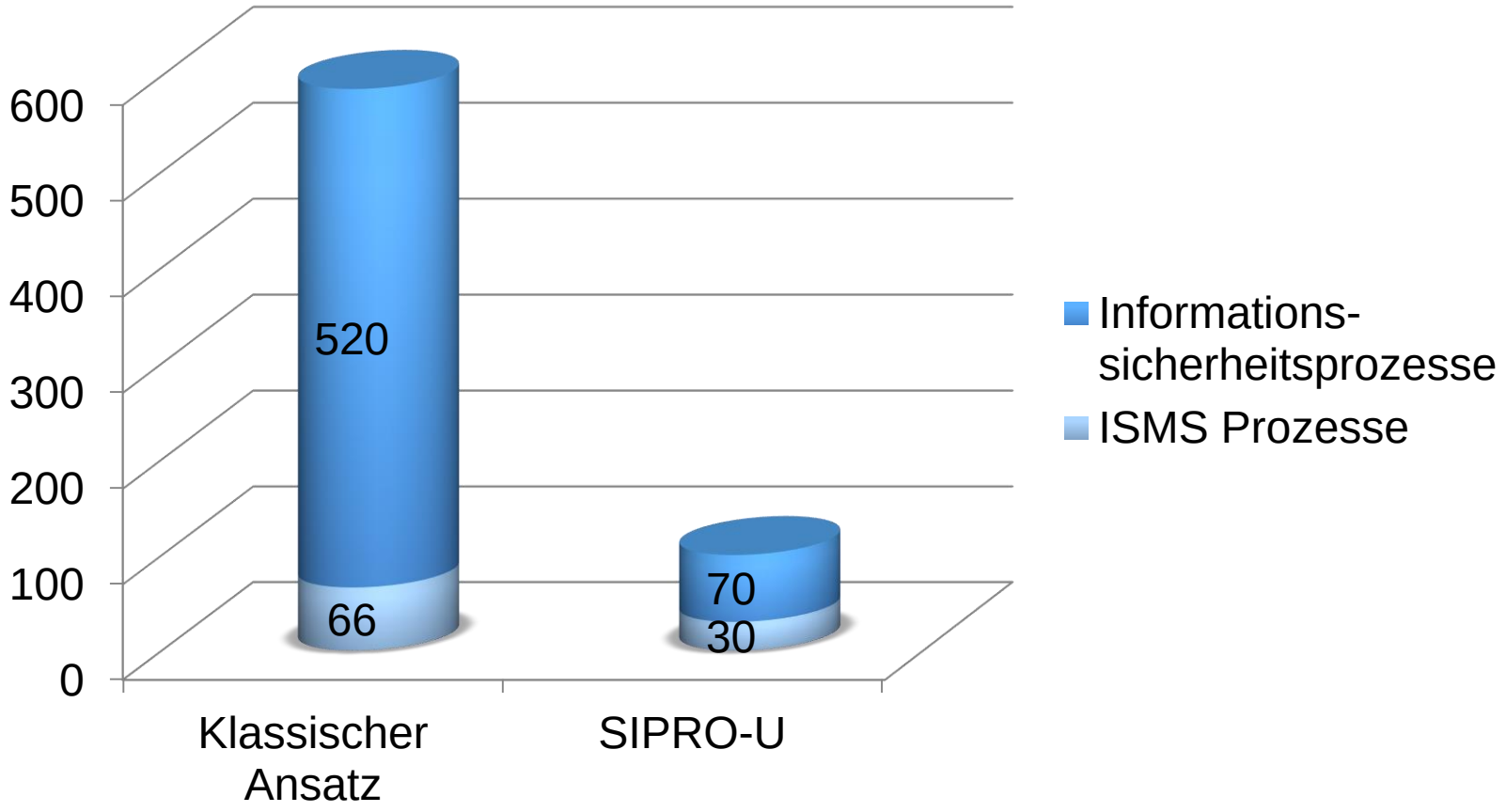
Messung der Effektivität der Informationssicherheits-Prozesse (Dashboard-Darstellung)



Beispiel eines klassischen Ansatzes zur Durchführung des geforderten Messverfahrens



Vergleich der Anzahl der zu ermittelnden Messwerte zwischen dem Beispielverfahren und dem in SIPRO-U angestrebten GQMS-Verfahren für den Testbetrieb



Planung SIPRO-U 2016/2017

AP 3

•1 HJ 2016
• Weiterentwicklung des GQMS Verfahren (Fragen und Metriken) für die ISMS Prozesse
• Entwicklung des GQMS Verfahren (Fragen und Metriken) für die Informationssicherheitsprozesse
• Festlegung der Schnittstellen in Prosec ! ISMS für das Messverfahren

AP 4

• 2 HJ 2016
• Implementierung des GQMS Verfahren Vers 1 in Prosec ! ISMS 3.0
• Entwicklung eines ersten Dashboards
• Anwendungstests im Bereich RWE Metering und Feinabstimmung der Metriken

AP 5

•1 HJ 2017
• Anwendungserfahrungen im Strom- und Gassektor
• Übertragung des Verfahrens auf andere Bereiche wie z.B. Wasser oder Querverbundunternehmen

AP6

•2 HJ 2017
•SIPRO-U Erfahrungsberichte aus anderen Sektoren
•SIPRO-U Abschlussbericht

SICIA

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Ihr Ansprechpartner:

Rolf-Dieter Kasper
RWE International SE
Netztechnik und Security
Kruppstr. 5, 45128 Essen
Phone: +49 (0) 201 12 29386
rolf.kasper@rwe.com