

Bring law and order to the digital Wild West

Presentation for SwiNOG #36, 14.11.2019

and people

We make infrastructures digitally secure

www.electrosuisse.ch/cybersecurity

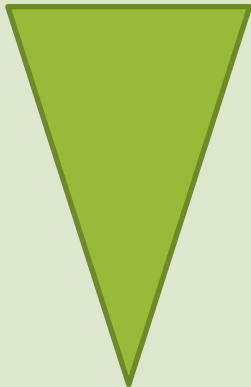


Electrosuisse

- Founded in 1889 as Swiss Electrotechnical Association (SEV/ASE).
- 2002 Re-positioning as Electrosuisse – professional association for electro-, energy- and information technology.
- Headquarter in Fehraltorf, 230 employees.
- Members: 4500 experts and more than 2000 companies.
- Accredited and neutral expert body for standardization, inspection, testing, certification, consulting, and education.
- Committed to electrical safety for 130 years.
- Since 2018 also committed to cybersecurity.

Scope and customers

Scope Electrosuisse

Level	Topic	Lever of impact
People	Expertise	
Processes	Maturity	
Technology	Security Level	

Customer segments

- Energy and water supply
 - Manufacturing facilities
 - Building technology and automation
 - Electromobility infrastructure
- Focus on companies with 50-500 employees. Added value also for smaller companies.

Security by competence

Electrosuisse cybersecurity offering

Consulting and Coaching

Your independent cybersecurity partner

- Status determination, identification of protection requirements and gap analysis
- Strategy and action planning
- Budgeting
- Accompaniment and supervision of implementation of measures
- Supplier management

Cybersecurity Quick Assessment

- Coached self assessment (2h) with recommendations for measures

Education

Training for site managers and IT/OT-responsibles

- Digital risks
- Standards and legal basis
- Key elements/controls
- Procedure

Awareness Training

- Regular sensitization and training of employees on site
- 17 customizable and expandable standard modules

Challenges (in particular for SMEs)

- Merging of IT and OT. In an increasingly interconnected world cybersecurity is becoming central security.
- Despite fewer resources, small companies have to master same duties for basic protection as larger companies.
- New, additional challenges by IIoT and smartmetering.
- High dependence on OT manufacturers.
- Critical infrastructures increasingly in focus of highly professional cyber criminals and state actors.
- Increase of attack surfaces (number of devices and connections).
- Permanent cyber attacks and constant shift of attack vectors.
- Increased frequency and intensity of attacks.
- Increase of complexity and duties.
- Cybersecurity budgets generally too small, not risk-adequate and often wrongly allocated.

Experience of Electrosuisse

- Cybersecurity services and in particular training are not self-running, although the importance of the topic is claimed and there is supposedly a shortage of skilled workers.
- Half-knowledge and unconscious incompetence lead to excessive demands or a false sense of security.
- Fear of exposure and blame for previous neglects.
- Market offers confusing and difficult to compare $\Rightarrow$ disorientation and uncertainty.
- **Lack of binding standards** $\Rightarrow$ need for cybersecurity?
- Lack of budgets $\Rightarrow$ employees too poorly trained or not trained at all.
- **SMEs need easy-to-understand and practicable tutorials, examples/templates** and affordable tools.
- SMEs need support in risk-based budgeting.

Binding safety/security in road traffic and ICT

Road Traffic

technical standards

road traffic law,
traffic rules

safety regulations for
manufacturers

owner's liability
insurance

product liability

traffic licence

type testing

driving test

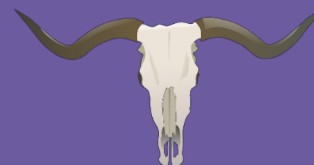
periodic vehicle
inspection

traffic control

ICT (Data Traffic)

IEC 62443,
ISO/IEC 270xx, ...

data protection law



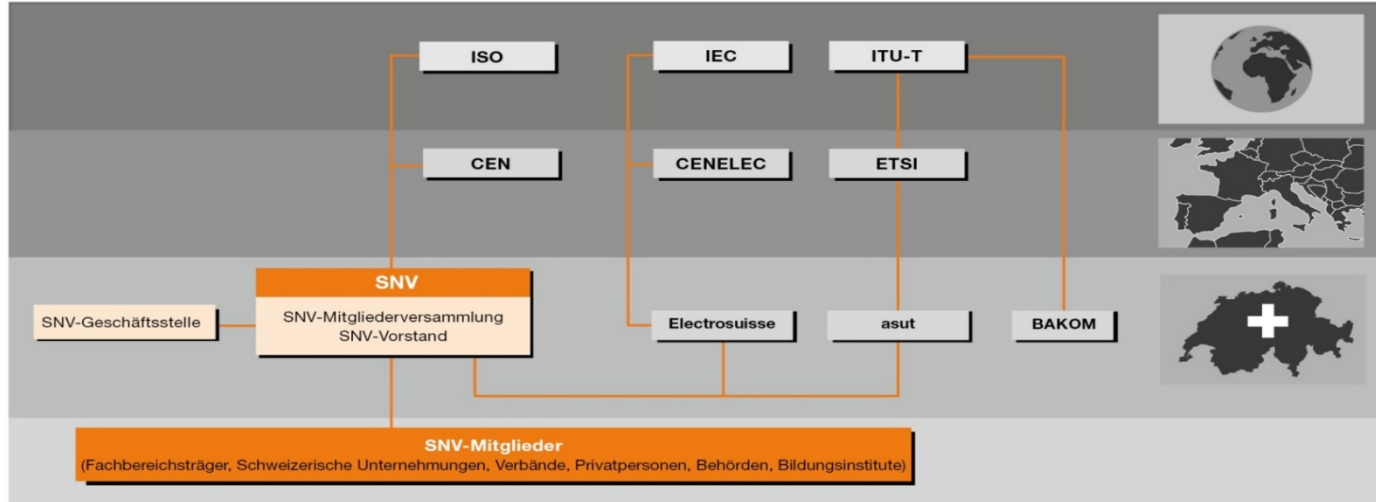
Digital Wild West

→ **Laws & Marshalls!!!**

Problem statement

- Current standards are insufficient in various respects, not easy to implement, not scalable and not binding.
- Confidence in security of digital solutions is declining and damaging.
- Wild growth of initiatives and recommendations for users with poor success.
- Manufacturers and suppliers neglected as sources of hazards → symptom fighting.
- Switzerland needs
 - a) an implementation standard (like Niederspannungs-Installationsnorm NIN),
 - b) a digital security law with regulations for manufacturing, putting into circulation, maintenance and operation of digital solutions over their entire life cycle and
 - c) a directive referring to the standard as «acknowledged rules of technology».

Standardization bodies global structure



Thematische Aufteilung

Interdisziplinärer Normenbereich (INB)*	Maschinen- und Metallindustrie	Bauwesen	Strassen- und Verkehrswesen	Uhrenindustrie	Elektrotechnik	Tele-kommunikation	Fachbereiche
SNV Geschäftsstelle	SWISSMEM	SIA	VSS	FH	Electrosuisse	asut	Träger
INB		s i a				asut	

Cybersecurity vision of Electrosuisse

- Security by standards: Standardization body of Switzerland for digital security like already for electrical safety.
- Neutral expert body for cybersecurity inspection, certification, consulting, and training.
- Comprehensible, scalable and practicable standards and instructions also for SMEs (like Niederspannungs-Installationsnorm NIN).
- Strengthening cyber resilience of business location Switzerland.

Documents according to standard SN 18011

- 
 Schweizer Norm
 Norme Suisse
 Norma Svizzera

classic standard

Normative document prepared by experts on the basis of recognized processes according to international standards.

- 
 Schweizer Regel
 Règle Suisse
 Regola Svizzera

normative rules with limited consensus

Document of normative nature elaborated by professionals, with voluntary or limited public survey carried out. Validity: 5 + 3 years

- 
 Schweizer Guideline
 Guide Suisse
 Guida Svizzera

complementary guidelines to standards

Document with annotations on the preparation and application of standards and regulations. Does not contain normative specifications.

Stakeholders

- BWL, ISB, MELANI and cybersecurity competence center
- Federal agencies with authority to issue directives (BFE, BAG, BAKOM, FINMA, ...)
- SNV, asut, SQS
- ICTswitzerland, SWITCH, swissICT, ISSS, Swiss Cyber Experts, SIGS, SATW, SISA, Swico, SwiNOG, ...
- VSE, SVGW, swissT.net, ...
- economiesuisse, SGV, SVV, SKS
- Universities and universities of applied sciences (ETH/EPFL, FHNW, HSLU, ZHAW, ...)
- ...

Backup

Electrosuisse Beitrag NCS-Massnahmen

Nr.	Massnahme
M8	Evaluierung und Einführung von Minimalstandards (Analyse bis 2021/Q4)
M13	Aufbau von Dienstleistungen für alle Unternehmen
M29	Sensibilisierung der Öffentlichkeit für Cyber-Risiken (Awareness)

Electrosuisse Cybersecurity Publikationen

Datum	Plattform	Titel
2018-11	Jahrbuch Energiezukunft Schweiz 2019	Cybersecurity ist existenziell für die Operational Technology
2019-03	electrosuiss.ch/cybersecurity	Studie «Cybersecurity bei kleinen und mittleren Elektrizitätsversorgungsunternehmen»
2019-03	Electrosuisse Blog	Cybersecurity: Alles eine Frage der Einstellung
2019-03	bulletin.ch 2019-3	Cybersecurity bei kleinen und mittleren Elektrizitätswerken
2019-08	bulletin.ch 2019-7/8	Kompliziert oder komplex?
2019-09	electrosuiss.ch/cybersecurity	Whitepaper Cybersecurity-Budgetierung
2019-10	NZZ Gastkommentar	Cybersecurity: eine grosse Herausforderung für KMU
2019-11	Tagesanzeiger-Beilage «Fokus Sicherheit»	«Cybersecurity-Umsetzungsnorm»

Hauptbefunde EVU Cybersecurity Studie

- Unvollständiges Asset Management.
- Zu wenig Risikobasiertheit bei Massnahmen und Budgetierung.
- Fokus primär auf Schutzmassnahmen.
- Cybersecurity oft Blindflug mangels Visibilität.
- Reaktionsbereitschaft, Notfallvorbereitung und -übung ungenügend.
- Lieferantenrisiken oft unbekannt und vernachlässigt.
- Mensch als grösste Schwachstelle zu wenig behandelt.
- Fehlende Fachkompetenz und Ressourcen.
- Cybersecurity kein geführter Prozess.
- Investitionen in Cybersecurity zu klein.

Schwachpunkte aktueller Standards

- «Unvollständige Ganzheitlichkeit»: diverse weissen Flecken (insbesondere auch rechtliche und finanzielle Aspekte).
- Interne Bedrohungen und digitale Elementarschäden zu wenig berücksichtigt.
- Eine einzige oder unausballancierte, nicht an Anforderungen und Rahmenbedingungen skalierbare Flughöhe.
- Oft zu akademisch, schwammig formuliert oder zu technologielastrig.
- Lassen zu viel Raum für und benötigen fachkundige Interpretation.
- Für Nicht-Spezialisten schwer verständlich und wenig praktikabel.
- Fehlende Verbindlichkeit.

Fehlende (Umsetzungs-) Norm

- Security-Hersteller kreieren eigene marketinggetriebene Begriffswelten.
- Teilweise unterschiedliche Begriffswelten in IT und OT.
- Nicht-Spezialisten brauchen einfach verständliche und praktikable Standards und Anleitungen.
- Fehlende Basis für ganzheitliche, an konkrete Rahmenbedingungen anpassbare Sicherheitsbeurteilung/-zertifizierung (z.B. für Gerätesicherheitsprüfung, Cyber-Versicherung, etc.).

Cyber-Versicherung braucht eine Norm

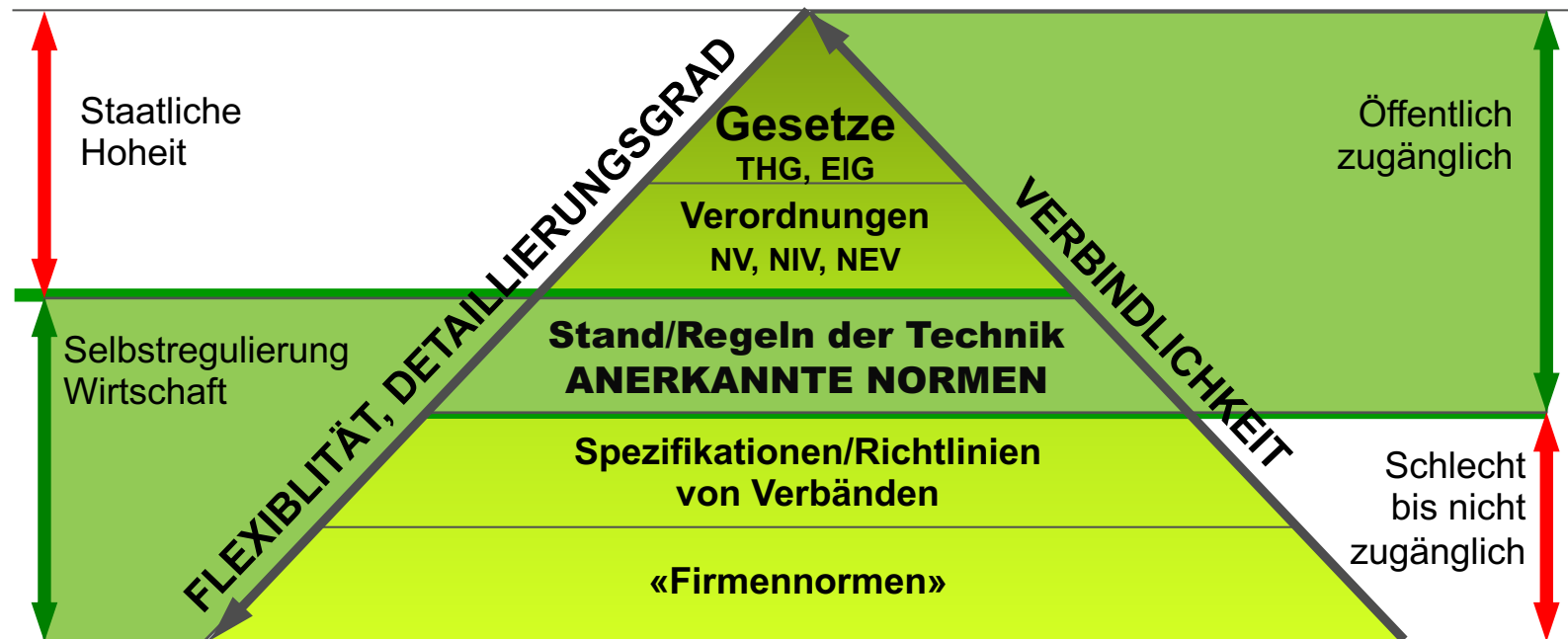
- Versicherung der finanziellen Risiken basierend auf Cybersecurity-Standards:
 - Minimierung der Risiken.
 - Kalkulierbarkeit der Versicherung (Risiko, Deckung, Prämie).
- Versicherungs-Mitgliedschaft bedingt Erfüllung der Minimalstandards (analog Fahrzeugkontrolle) und beinhaltet u.a.
 - regelmässige Mitarbeiterschulung.
 - regelmässige Compliance-Prüfung (Inspektion) durch unabhängige, akkreditierte Prüfstelle.
- Normative Wirkung (analog SUVA für Unfallverhütung).
- Meldepflicht von Cybervorfällen kann teilweise über Versicherung gelöst werden.

Gesetz für digitale Sicherheit

- Verbindliche Sicherheitsvorschriften für Herstellung, Inverkehrbringung und Wartung von digitalen Lösungen.
- Verbindliche Sicherheitsvorschriften für Betrieb von digitalen Lösungen über deren gesamten Lebenszyklus.
- Gesellschaftliche Verhaltensregeln und Strafnormen.
- Verordnung dazu verweist auf Cybersecurity-Norm als «anerkannte Regeln der Technik».

Rechtliche Aspekte – Rangfolge

Swiss WTO membership, TBT agreement



**ANERKANNTEN NORMEN von ISO/IEC/ITU-T, CEN/CLC/ETSI und SNV/CES/asut:
SN 411000:2015 (NIN), SN EN 60335, SN HD 60364-Serie, etc.**

Rechtliche Aspekte – Stand der Technik

- Normen sind anerkannte Regeln, die durch Experten in Vertretung ihrer Interessensgruppe erarbeitet werden.
- Anerkannte Normen, herausgegeben von ISO/IEC/ITU, CEN/Cenelec/ETSI und den nationalen Normenorganisationen (SNV, Electrosuisse, asut, sia, swissmem, VSS, FH), werden mittels festgeschriebenem Prozess beurteilt, ratifiziert und publiziert.
- Normen stellen den anerkannten «Stand der Technik» dar und sind daher bestens zur Konkretisierung von Gesetzen und Verordnungen geeignet.
- Normen sind freiwillig anwendbar. Nichteinhaltung kann nicht bestraft werden (da privatrechtlich erarbeitet), ausser bei Referenzierung in Gesetzen oder Verträgen.
- Bei Beurteilungen geschieht die richterliche Urteilsfindung unter Bezug auf den «Stand der Technik» (z.B. gültige Normen).

Schweizer Normenorganisationen

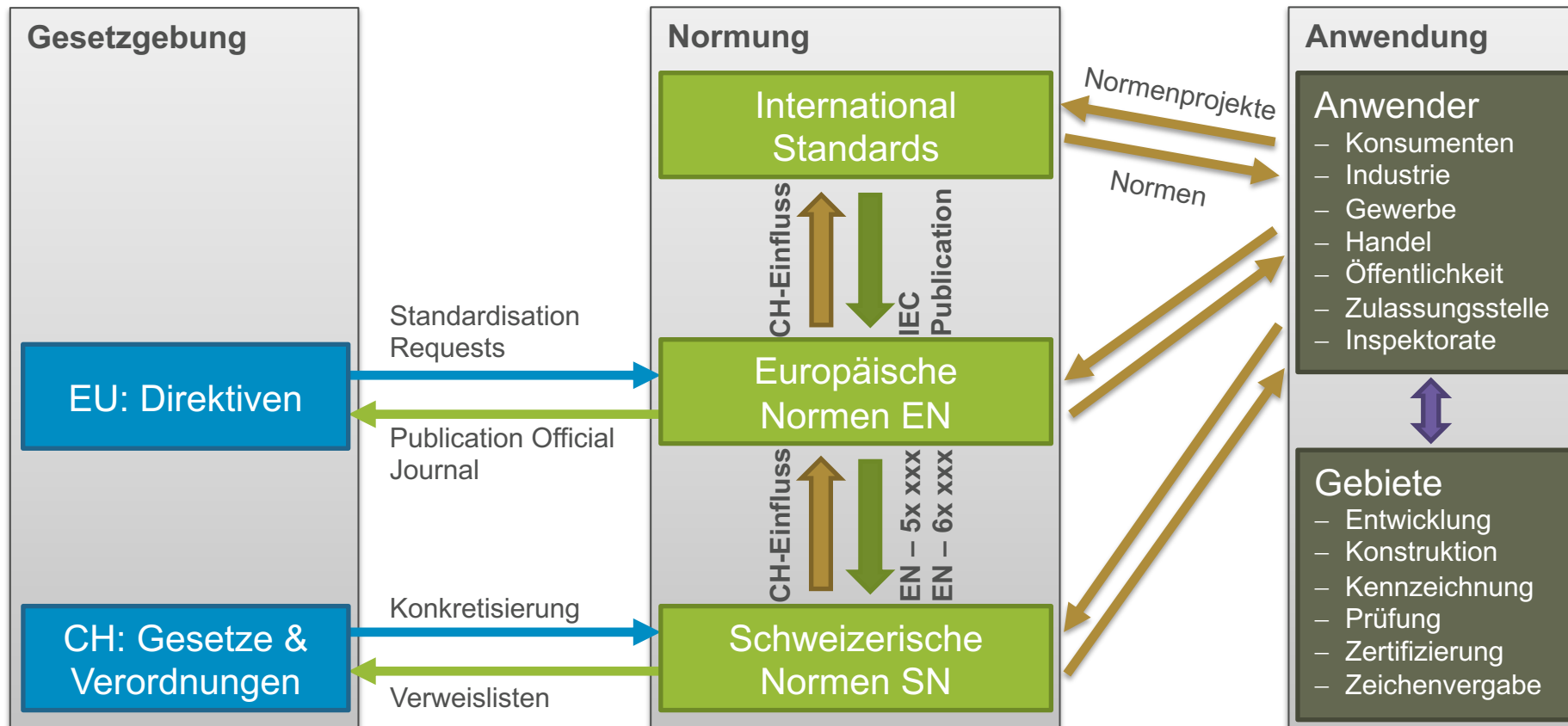
Thematische Aufteilung

Interdisziplinärer Normenbereich (INB)*	Maschinen- und Metallindustrie	Bauwesen	Strassen- und Verkehrswesen	Uhrenindustrie	Elektrotechnik	Tele- kommunikation	Fachbereiche
SNV	SWISSMEM	SIA	VSS	FH	Electrosuisse	asut	Träger
INB	 SWISSMEM	s i a	VSS ↔		 electro suisse	asut	

Vertrauen und Akzeptanz durch:

- Beteiligung aller interessierten Kreise
- Öffentliches Einspruchsverfahren (Public commenting)
- Einheitlichkeit des Normenwerkes
- Bereitstellung der IT-Infrastruktur
- Führung von Sekretariaten (national und international)

Normungsprozess



Cybersecurity-Norm Ziele

- Verbindliche Umsetzungsregeln für Herstellung, Inverkehrbringung und Wartung von sicheren digitalen Lösungen.
- Verbindliche Umsetzungsregeln für sicheren Betrieb von digitalen Lösungen.
- Einheitliche, an Rahmenbedingungen skalierbare Minimalstandards.
- Zweckmässig, verhältnismässig und zumutbar.
- Digitale Risiken für Bevölkerung und Wirtschaft minimieren.
- Cybersecurity-Kosten für Anwender minimieren.
- Vertrauen in Sicherheit von digitalen Lösungen stärken.
- Sichere digitale Transformation ermöglichen.

Cybersecurity-Norm Elemente

- Adressiert sowohl Hersteller und Anbieter als auch Anwender (Unternehmen und Privatpersonen).
- Skalierbarkeit z.B. durch risikobasierte Einteilung in Security-Klassen nach definierten (und einfachen) Kriterien.
- Zu jedem Kapitel:
 - Fachteil mit Erläuterungen.
 - Normteil mit klaren Anforderungs- und Prüfkriterien, Berechnungsformeln und Metriken.
 - Kurzanleitung zu Umsetzungsvarianten und Entscheidungshilfen.
 - Grafische Illustrationen.
- Glossar.
- Musterbeispiele und Vorlagen.
- Referenzen zu anderen Standards/Normen.

20 Schlüssel-Elemente für Anwender



1. Organisation	11. USB und externe Datenträger
2. Ziele, Strategie und Kennzahlen	12. Datenspeicherung und -übertragung
3. Asset Management	13. Backup und Restore
4. Risikoanalyse und Security Testing	14. Patch Management
5. Sicherheitsarchitektur	15. Visibilität und Entdeckung
6. Ausfallsicherheit und Redundanz	16. Überwachung und Alarmierung
7. Systemhärtung und -standardisierung	17. Notfall Management
8. Netzwerkzonierung	18. Richtlinien und Schulung
9. Identitäts- und Zugriffskontrolle	19. Lieferanten-Management
10. Fernzugriff	20. Budgetierung

Cybersecurity artmap®

- Ganzheitliche, grafische Übersicht zu allen relevanten Teilgebieten und Aspekten der Cybersecurity für IT und OT.
- Thema verständlich und auch Laien zugänglich machen.
- Einstieg in die einzelnen Themengebiete erleichtern.
- Format: A3, farbig, beidseitig bedruckt.
- 1. Auflage: 4'500. Laufzeit: ca. 3 Jahre.
- Vertrieb: Fachtagungen, Fachkurse, Veranstaltungen und Messen.
- Gute Erfahrungen mit artmaps zu verschiedenen Themen der Elektrizität/Elektrotechnik.