



RIPE

RIPE-17

Inhaltsverzeichnis

The Langner Group

Washington | Hamburg | München

RIPE Management-Programm für die digitale Industrieautomation (MP-17)

| | | |
|----------|--|-----------|
| 0 | Einführung | 4 |
| 0.1 | Zweck | 4 |
| 0.2 | Prozessbeschreibung | 4 |
| 0.3 | Implementierungsumfang | 5 |
| 1 | Organisatorische Ressourcen | 6 |
| 1.1 | Zentraler Support für digitale Industrieautomation | 6 |
| 1.2 | Mitwirkung anderer Abteilungen | 7 |
| 1.3 | Hinzuziehung externer Ressourcen | 7 |
| 2 | Asset- und Konfigurationsmanagement | 9 |
| 2.1 | Systeminventar und Konfigurationsdatenbank | 9 |
| 2.2 | Netzwerk- und Datenflussdiagramme | 10 |
| 2.3 | Planung, Beschaffung, und Konfiguration | 11 |
| 3 | Benutzer- und Fremdfirmenverwaltung | 13 |
| 3.1 | Benutzer- und Fremdfirmendatenbank | 13 |
| 3.2 | Schulungsprogramm | 13 |
| 3.3 | Polycys und Betriebsanweisungen | 14 |
| 4 | Vorfallsmanagement | 16 |
| 4.1 | Vorfallsreaktionsfähigkeit | 16 |
| 4.2 | Vorfallerkennung und -bewertung | 17 |
| 4.3 | Vorfallsreaktion und -behebung | 17 |
| 5 | Governance | 19 |
| 5.1 | Feststellen der Cyber-Sicherheitsfähigkeit | 19 |
| 5.2 | Schwachstellenanalyse | 20 |
| 5.3 | Ergebnisbeurteilung und Optimierung | 20 |
| 5.4 | Berichtswesen und Freigabe durch die Unternehmensführung | 21 |

RIPE Implementierungsplan (IP-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand und Aufbau dieses Dokuments | 4 |
| 0.2 | Benutzung dieses Dokuments | 4 |
| 1 | Pre-RIPE: Die organisatorischen und technischen Grundlagen | 8 |
| 1.0 | Übersicht | 8 |
| 1.1 | Erstellen eines individuellen Implementierungsplans | 8 |
| 1.2 | Bereitstellung organisatorischer Ressourcen | 9 |
| 1.3 | Aufsetzen einer Konfigurationsdatenbank (CMDB) | 10 |
| 1.4 | Aufbau der Benutzerverwaltung | 11 |
| 1.5 | Aufbau des zentralen Dokumentenmanagements | 12 |
| 1.6 | Bereitstellung von Softwaretools zur Erstellung von Netzwerkdigrammen | 13 |
| 1.7 | Bereitstellung von Softwaretools zur Erstellung von Datenflussdiagrammen | 14 |
| 1.8 | Dokumentation der durchgeführten Tätigkeiten, Arbeitsergebnisse, und Erfahrungen | 15 |
| 2 | RIPE Zyklus Null: Anpassung und Validierung der Instrumente | 17 |
| 2.0 | Übersicht | 17 |
| 2.1 | Erstellen eines individuellen Implementierungsplans | 18 |
| 2.2 | Entwicklung eines konzeptionellen Rahmens für das Systeminventar | 19 |
| 2.3 | Erstellen und Aktualisieren von vorläufigen Netzwerkdigrammen | 20 |
| 2.4 | Erstellen vorläufiger Datenflussdiagramme | 21 |
| 2.5 | Aufbau der Benutzerdatenbank | 22 |
| 2.6 | Anpassen des Schulungsprogramms und Durchführung von Schulungen | 23 |
| 2.7 | Anpassen und Ausrollen der Policys und Standardverfahren | 24 |
| 2.8 | Anpassen und Ausrollen der Referenzarchitektur | 25 |
| 2.9 | Einführung der Beschaffungsrichtlinie | 27 |
| 2.10 | Anpassen der Verfahren zum Management von Cyber-Sicherheitsvorfällen | 28 |
| 2.11 | Sammlung, Analyse und Dokumentation von Ergebnissen | 29 |
| 3 | RIPE Zyklen Eins bis N: Kontinuierliche Verbesserung | 31 |
| 3.0 | Übersicht | 31 |
| 3.1 | Erstellen eines individuellen Implementierungsplans | 31 |
| 3.2 | Einführung verbesserter Instrumente | 32 |
| 3.3 | Anwenden der normativen Instrumente | 33 |
| 3.4 | Verbesserung des Systemmodells | 33 |
| 3.5 | Aufbau und Verbesserung einer Fähigkeit zum Management von Cyber-Sicherheitsvorfällen | 34 |
| 3.6 | Durchführung von Audits | 35 |
| 3.7 | Analyse und Reporting | 36 |

RIPE Systeminventar (SI-17)

| | | |
|----------|--|-----------|
| 0 | Einleitung | 5 |
| 0.1 | Gegenstand und Zielgruppe | 5 |
| 0.2 | Die Rolle des Systeminventars innerhalb von RIPE | 5 |
| 0.3 | Das Datenmodell des RIPE Systeminventars | 6 |
| 0.4 | Aufbau eines Systeminventars | 8 |
| 0.5 | Aktualisierung eines Systeminventars | 9 |
| 1 | Bezeichnernomenklatur | 11 |
| 1.1 | Zweck und Verwendung einer Nomenklatur | 11 |
| 1.2 | Komponentenbezeichner | 11 |
| 1.3 | Netzwerkbezeichner | 11 |
| 1.4 | Kabelbezeichner | 12 |
| 1.5 | Systembezeichner | 12 |
| 2 | Systemkontext | 13 |
| 2.1 | Anlagenkontext | 13 |
| 2.2 | Produktkontext | 13 |
| 2.3 | Räumlicher Kontext | 14 |
| 3 | Geräteklassen | 15 |
| 3.1 | Identifikation | 15 |
| 3.2 | Grundlegende Eigenschaften | 15 |
| 3.3 | Schnittstellen | 16 |
| 3.4 | Textuelle Dokumentation | 16 |
| 4 | Geräte | 17 |
| 4.1 | Geerbte Eigenschaften | 17 |
| 4.2 | Identifikation | 17 |
| 4.3 | Grundlegende Eigenschaften | 17 |
| 4.4 | Konfigurationseigenschaften | 18 |
| 4.5 | Unterstützung automatisierter Konfigurationsermittlung und -verifikation | 18 |
| 4.6 | Textuelle Dokumentation | 19 |
| 4.7 | Verantwortlichkeit | 19 |
| 5 | Softwareklassen | 20 |
| 5.1 | Identifikation | 20 |
| 5.2 | Grundlegende Eigenschaften | 20 |
| 5.3 | Softwareintegrität | 21 |
| 5.4 | Netzwerkschnittstellen | 21 |
| 5.5 | Textuelle Dokumentation | 21 |
| 6 | Softwareinstanzen | 23 |
| 6.1 | Vererbte Eigenschaften | 23 |
| 6.2 | Identifikation | 23 |
| 6.3 | Grundlegende Eigenschaften | 23 |
| 6.4 | Softwareintegrität | 23 |
| 6.5 | Netzwerkschnittstellen | 23 |
| 6.6 | Textuelle Dokumentation | 24 |

| | | |
|----------|---|-----------|
| 6.7 | Verantwortlichkeit..... | 24 |
| 7 | Entwicklung eines Systeminventars | 25 |
| 7.1 | Entwicklung einer Kennzeichnungsomenklatur, sofern sie noch nicht existiert..... | 25 |
| 7.2 | Sammeln von Kontextdaten..... | 25 |
| 7.3 | Ermittlung der Hardware- und Softwareprodukte, die am gegebenen Standort benutzt werden..... | 25 |
| 7.4 | Ermittlung einzelner Geräte und Softwareinstanzen | 26 |
| 7.5 | Vervollständigen der Konfigurationsdaten | 26 |

RIPE Netzwerkdiagramme (NW-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand | 4 |
| 0.2 | Zielgruppe | 4 |
| 1 | Netzwerkdiagramme | 5 |
| 1.1 | Allgemeine Definitionen und Konventionen | 5 |
| 1.2 | Granularität, Hierarchieebenen, und Netzwerkdiagrammtypen | 5 |
| 1.3 | Kennzeichnung des Aufstellungsorts | 7 |
| 1.4 | Diagrammbeschriftung | 8 |
| 1.5 | Anschlussstellen | 8 |
| 2 | Knoten | 10 |
| 2.1 | Symbole für Knoten, Farbcodes, und Beschriftung | 10 |
| 2.2 | Netzwerkswitch | 11 |
| 2.3 | Router | 11 |
| 2.4 | Firewall | 12 |
| 2.5 | Wireless Access Point | 12 |
| 2.6 | Modem | 12 |
| 2.7 | Datendiode | 13 |
| 2.8 | Server | 13 |
| 2.9 | Arbeitsplatzcomputer | 13 |
| 2.10 | Bedienstation | 14 |
| 2.11 | Mobiler Computer (Laptop) | 14 |
| 2.12 | Automatisierungskomponente | 14 |
| 2.13 | Sensor und Aktor | 14 |
| 2.14 | Drucker | 15 |
| 2.15 | Andere Komponenten | 15 |
| 3 | Netzwerke und Subsysteme | 16 |
| 3.1 | Ethernet-basierte Netzwerke | 16 |
| 3.2 | Feldbusse | 16 |
| 3.3 | Subsysteme | 16 |
| 4 | Netzwerkverbindungen | 17 |
| 4.1 | Verbindungstyp: Ethernet vs. Fieldbus | 17 |
| 4.2 | Medientyp: Kupfer vs. Lichtwellenleiter | 17 |
| 4.3 | Punkt-zu-Punkt-Verbindungen | 17 |
| 4.4 | Beschriftung von Schnittstellen und Verbindungen | 17 |

RIPE Datenflussdiagramme (DF-17)

| | | |
|----------|---|----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand und Zielgruppe | 4 |
| 0.2 | Grundlagen von Datenflussdiagrammen | 4 |
| 1 | Komponenten und Subsysteme | 5 |
| 1.1 | Allgemeines..... | 5 |
| 1.2 | Komponenten..... | 5 |
| 1.3 | Subsysteme..... | 5 |
| 2 | Datenflüsse | 7 |
| 2.1 | Allgemeines..... | 7 |
| 2.2 | Schnittstellen..... | 7 |
| 2.3 | Verbundene Schnittstellen vs. offene Schnittstellen | 7 |
| 2.4 | Datenflusskategorien und Farbcodes..... | 8 |
| 2.5 | Beschriftung von Schnittstellen..... | 9 |

RIPE Referenzarchitektur (RA-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand und Zielgruppe | 4 |
| 0.2 | Anwendung der Regeln | 5 |
| 1 | Netzwerkarchitektur | 6 |
| 1.1 | Allgemeines..... | 6 |
| 1.2 | Schnittstelle zum Office-Netz..... | 6 |
| 1.3 | Fernzugriff..... | 7 |
| 1.4 | Email | 7 |
| 1.5 | Web-Zugriff | 7 |
| 1.6 | Wireless LAN..... | 8 |
| 1.7 | Netzwerkzugriff von mobilen Systemen von Fremdfirmen..... | 8 |
| 1.8 | Isolation von "Black Boxes" | 8 |
| 2 | Netzwerk-Infrastrukturdienste | 9 |
| 2.1 | Allgemeines..... | 9 |
| 2.2 | DHCP | 9 |
| 2.3 | DNS | 9 |
| 2.4 | Active Directory, Domain Controller, und LDAP | 9 |
| 2.5 | Zeitserver (NTP und verwandte Protokolle) | 9 |
| 2.6 | Backup-Server | 10 |
| 2.7 | Update von Antivirus-Signaturen..... | 10 |
| 2.8 | Sicherheits-Patches..... | 10 |
| 3 | Netzwerkkomponenten | 11 |
| 3.1 | Firewalls..... | 11 |
| 3.2 | Wireless Access Points..... | 11 |
| 3.3 | Netzwerk-Switche und Router | 11 |
| 4 | Computersysteme | 13 |
| 4.1 | Allgemeines..... | 13 |
| 4.2 | Leitsystemserver..... | 14 |
| 4.3 | Visualisierungen und Bedienstationen..... | 15 |
| 4.4 | Mobile Programmiergeräte..... | 15 |
| 4.5 | Leittechniknahe Anwendungen..... | 15 |
| 5 | Automatisierungskomponenten | 16 |
| 5.1 | Allgemeines..... | 16 |
| 5.2 | Speicherprogrammierbare Steuerungen..... | 16 |

RIPE Systembeschaffung (SP-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Zielgruppe | 4 |
| 0.2 | Die Rolle der Systembeschaffung innerhalb von RIPE | 4 |
| 0.3 | Die RIPE-Philosophie zur Systembeschaffung | 5 |
| 0.4 | Empfohlene Verwendung des Moduls RIPE Systembeschaffung | 6 |
| 1 | Produktdokumentation | 8 |
| 1.1 | Allgemeine Qualität der Produktdokumentation | 8 |
| 1.2 | Hardwaredokumentation | 8 |
| 1.3 | Softwaredokumentation | 8 |
| 1.4 | Netzwerkdokumentation | 9 |
| 1.5 | Systemwiederherstellung und Notfallplan | 9 |
| 2 | Sicherstellung der Konfigurationsintegrität | 10 |
| 2.1 | Systemhärtung | 10 |
| 2.2 | Schutz vor nicht autorisierter Software | 10 |
| 2.3 | Versionskontrolle | 10 |
| 2.4 | Verifikation des Zielsystems vor Neukonfiguration | 11 |
| 2.5 | Verifikation der Konfigurationsintegrität | 11 |
| 2.6 | Disaster Recovery | 11 |
| 3 | Netzwerkstörfestigkeit und -robustheit | 12 |
| 3.1 | Addressraum | 12 |
| 3.2 | Netzwerkstörfestigkeit | 12 |
| 3.3 | Schwachstellen-Scans | 12 |
| 3.4 | Nichtverwendung unsicherer Netzwerkdienste | 12 |
| 3.5 | System- und Netzwerkmonitoring | 12 |
| 3.6 | Uhrzeitsynchronisation | 13 |
| 4 | Zugriffsschutz und Benutzerkonten | 14 |
| 4.1 | Autorisierung | 14 |
| 4.2 | Passwörter | 14 |
| 4.3 | Benutzerkonten | 14 |
| 4.4 | Logging | 14 |
| 4.5 | Netzwerkzugriff | 15 |
| 5 | Herstellerprozesse und -verfahren | 16 |
| 5.1 | Qualitätssicherung | 16 |
| 5.2 | Bekennnis zur Policy Compliance | 16 |
| 5.3 | Fehlerbehebungsprozess | 16 |
| 5.4 | Zentraler Ansprechpartner für Cyber-Sicherheit | 16 |

RIPE Benutzerverwaltung (WM-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 5 |
| 0.1 | Gegenstand und Zielgruppe | 5 |
| 0.2 | Die Rolle der Benutzerverwaltung innerhalb von RIPE | 5 |
| 0.3 | Benutzerrollen | 6 |
| 0.4 | Funktionen der Benutzerverwaltung | 8 |
| 1 | Endbenutzer | 10 |
| 1.1 | Typische Positionen und Anwendungsfälle | 10 |
| 1.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 10 |
| 1.3 | Dokumentenzugriff | 10 |
| 1.4 | Nomadensysteme und Fernzugriff | 11 |
| 2 | Instandhalter | 12 |
| 2.1 | Typische Positionen und Anwendungsfälle | 12 |
| 2.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 12 |
| 2.3 | Dokumentenzugriff | 12 |
| 2.4 | Nomadensysteme und Fernzugriff | 13 |
| 3 | Administrator | 14 |
| 3.1 | Typische Positionen und Anwendungsfälle | 14 |
| 3.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 14 |
| 3.3 | Dokumentenzugriff | 14 |
| 3.4 | Nomadensysteme und Fernzugriff | 15 |
| 4 | Planer/Entwickler | 16 |
| 4.1 | Typische Positionen und Anwendungsfälle | 16 |
| 4.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 16 |
| 4.3 | Dokumentenzugriff | 16 |
| 4.4 | Nomadensysteme und Fernzugriff | 17 |
| 5 | RIPE Unterstützung | 18 |
| 5.1 | Typische Positionen und Anwendungsfälle | 18 |
| 5.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 18 |
| 5.3 | Dokumentenzugriff | 18 |
| 5.4 | Nomadensysteme und Fernzugriff | 19 |
| 6 | Besucher | 20 |
| 6.1 | Typische Positionen und Anwendungsfälle | 20 |
| 6.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 20 |
| 6.3 | Dokumentenzugriff | 20 |
| 6.4 | Nomadensysteme und Fernzugriff | 20 |
| 7 | Supervisor | 22 |
| 7.1 | Typische Positionen und Anwendungsfälle | 22 |
| 7.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 22 |
| 7.3 | Dokumentenzugriff | 22 |
| 7.4 | Nomadensysteme und Fernzugriff | 23 |

| | | |
|----------|---|-----------|
| 8 | Vorfallsmanagement | 24 |
| 8.1 | Typische Positionen und Anwendungsfälle | 24 |
| 8.2 | Rechte und Verantwortlichkeiten für Leit- und Automatisierungstechnik | 24 |
| 8.3 | Dokumentenzugriff | 24 |
| 8.4 | Nomadensysteme und Fernzugriff | 25 |

RIPE Policiys und Standardverfahren (PO-17)

| | | |
|----------|--|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand und Zielgruppe | 4 |
| 0.2 | Benutzerrollen, Policiys, und Standardverfahren..... | 4 |
| 0.3 | Die RIPE Policy-Philosophie..... | 4 |
| 1 | Externe Instandhalter (Fremdfirmen) | 6 |
| 1.1 | Benutzung von Computern | 6 |
| 1.2 | Benutzung von mobilen Systemen die das Werksgelände verlassen (Nomadensysteme)..... | 6 |
| 1.3 | Benutzung von Smartphones, Tablets, MP3-Spielern usw..... | 7 |
| 1.4 | Benutzung von Netzwerken..... | 7 |
| 1.5 | Benutzung mobiler Medien | 8 |
| 1.6 | Dateiaustausch..... | 8 |
| 1.7 | Benutzung von Fernzugriff | 8 |
| 1.8 | Verfahren für Konfigurationsänderungen | 9 |
| 2 | Endbenutzer von Leit- und Automatisierungstechnik | 10 |
| 2.1 | Benutzung von Computern | 10 |
| 2.2 | Benutzung von mobilen Medien und mobilen Computern..... | 10 |
| 2.3 | Benutzung von Internet und Email | 10 |
| 2.4 | Dateiaustausch..... | 10 |
| 3 | Engineering und Administration von Systemen und Netzwerken | 12 |
| 3.1 | Benutzung von Computern | 12 |
| 3.2 | Benutzung mobiler Systeme, die das Werksgelände nicht verlassen..... | 12 |
| 3.3 | Benutzung mobiler Systeme, die das Werksgelände verlassen (Nomadensysteme). 12 | |
| 3.4 | Benutzung von Netzwerken..... | 13 |
| 3.5 | Benutzung mobiler Medien | 13 |
| 3.6 | Dateiaustausch..... | 13 |
| 3.7 | Aufrechterhaltung der Endpunktsicherheit | 14 |
| 3.8 | Aufrechterhaltung der Netzwerksicherheit | 14 |
| 3.9 | Verfahren zur Aktualisierung von Firewallregeln | 15 |
| 3.10 | Allgemeines Verfahren für Konfigurationsänderungen..... | 15 |
| 4 | Planung von Leit- und Automatisierungstechnik | 17 |
| 4.1 | Dateiaustausch..... | 17 |
| 4.2 | Verfahren zur Konfigurationsplanung und Konfigurationsänderung | 17 |
| 4.3 | Verfahren zur Systembeschaffung..... | 18 |
| 5 | Besucher | 20 |
| 5.1 | Benutzung von Computern und Netzwerken..... | 20 |
| 5.2 | Benutzung von Internet und Email | 20 |
| 5.3 | Dateiaustausch..... | 20 |

RIPE Management von Cyber-Sicherheitsvorfällen (IM-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand und Zielgruppe | 4 |
| 0.2 | Die Rolle des Vorfallsmanagements in RIPE | 4 |
| 0.3 | Vorfallsmanagement in der digitalen Industrieautomation | 4 |
| 1 | Entwickeln einer Vorfallreaktionsfähigkeit | 6 |
| 1.1 | Vorfallsreaktionskräfte und wichtige externe Ansprechpartner | 6 |
| 1.2 | Technische Voraussetzungen für das Management von Cyber-Vorfällen | 7 |
| 1.3 | Sonstige Voraussetzungen für das Vorfallsmanagement | 8 |
| 1.4 | Schulungen und Übungen | 9 |
| 2 | Erkennung und Bewertung von Cyber-Vorfällen | 10 |
| 2.1 | Erkennung, Validierung und Bewertung von Cyber-Vorfällen | 10 |
| 2.2 | Priorisierung von Cyber-Vorfällen | 11 |
| 2.3 | Benachrichtigung über Cyber-Vorfälle | 12 |
| 2.4 | Mobilisierung der Vorfallsreaktionskräfte | 13 |
| 3 | Behebung von Cyber-Vorfällen | 14 |
| 3.1 | Prädiktive Analyse möglicher Seiteneffekte der Vorfallsbehebung | 14 |
| 3.2 | Eindämmung des Cyber-Vorfalles | 14 |
| 3.3 | Ursachenbeseitigung und Systemwiederherstellung | 15 |
| 4 | Nach Abschluss der Vorfallsbehebung | 18 |
| 4.1 | Benachrichtigung über den Abschluss des Cyber-Vorfalles | 18 |
| 4.2 | Detaillierte forensische Analyse | 18 |
| 4.3 | Review und Dokumentation des Cyber-Vorfalles | 18 |

RIPE Schulungsprogramm (TC-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 4 |
| 0.1 | Gegenstand | 4 |
| 0.2 | Schulungsformate | 4 |
| 0.3 | Übersicht | 4 |
| 0.4 | Verifikation | 5 |
| 1 | Policy-bezogene Schulungen | 6 |
| 1.1 | Cyber-Sicherheitsverfahren für Endbenutzer von Leit- und Automatisierungstechnik | 6 |
| 1.2 | Cyber-Sicherheitsverfahren für Fremdfirmen, Teil I: Systembenutzung | 6 |
| 1.3 | Cyber-Sicherheitsverfahren für Fremdfirmen, Teil II: Netzwerke und Speichermedien | 7 |
| 1.4 | Cyber-Sicherheitsverfahren für Instandhalter und Administratoren, Teil I: Systembenutzung | 8 |
| 1.5 | Cyber-Sicherheitsverfahren für Instandhalter und Administratoren, Teil II: Netzwerke und Speichermedien | 8 |
| 1.6 | Fernzugriff | 9 |
| 1.7 | Cyber-Sicherheitsregeln für Besucher | 10 |
| 2 | Aufgabenbezogene Schulungen | 11 |
| 2.1 | Anwendung des Moduls RIPE Systembeschaffung | 11 |
| 2.2 | Formulierung von Anforderungen auf Basis der RIPE Beschaffungsrichtlinie | 11 |
| 2.3 | Anwendung des Moduls RIPE Referenzarchitektur auf Netzwerkinfrastruktur | 12 |
| 2.4 | Anwendung des Moduls RIPE Referenzarchitektur auf Systeme | 13 |
| 2.5 | Anwendung des Moduls RIPE Referenzarchitektur auf elektrische Systeme | 14 |
| 2.6 | Aufrechterhaltung der Sicherheit von Endpunktsystemen | 14 |
| 2.7 | Praktische Fehlersuche in Prozessnetzen | 15 |
| 2.8 | Verfahren zur Cyber-Vorfallsbehandlung | 16 |
| 2.9 | Praktische Übung zur Cyber-Vorfallsbehandlung | 16 |
| 2.10 | Planspiel zur Cyber-Vorfallsbehandlung für das Management | 17 |
| 3 | Hintergrundwissen | 19 |
| 3.1 | Automatisierungswissen für IT-Fachleute | 19 |
| 3.2 | Cyber-Angriffe gegen Industrieanlagen: Erkenntnisse aus realen Angriffen | 19 |
| 3.3 | Grundlagen von Prozessnetzen | 20 |
| 3.4 | Designprinzipien für Prozessnetze | 21 |

RIPE Kennzahlen zur Cyber-Sicherheit in der Produktion (CM-17)

| | | |
|----------|---|-----------|
| 0 | Einführung | 5 |
| 0.1 | Zweck | 5 |
| 0.2 | Betrachtungsgegenstand und Verifikationszeitpunkt | 5 |
| 0.3 | Kennzahlarten | 5 |
| 1 | Basisdaten des Standorts | 8 |
| 1.1 | Ressourcen für die Cyber-Sicherheit der Leit- und Automatisierungstechnik | 8 |
| 1.2 | Personal | 8 |
| 1.3 | Installierte Systembasis: Fest installierte Hardwarekomponenten | 9 |
| 1.4 | Installierte Systembasis: Mobile Geräte | 10 |
| 1.5 | Installierte Systembasis: Netzwerke | 10 |
| 2 | Systeminventar (SI) | 11 |
| 2.1 | RIPE.SI.Capability | 11 |
| 2.2 | RIPE.SI.%Completeness | 11 |
| 2.3 | RIPE.SI.%Accuracy | 11 |
| 3 | Netzwerkmodell (NA) | 13 |
| 3.1 | RIPE.NA.Capability | 13 |
| 3.2 | RIPE.NA.%Completeness | 13 |
| 3.3 | RIPE.NA.%Accuracy | 13 |
| 4 | Datenflussmodell (DF) | 15 |
| 4.1 | RIPE.DF.Capability | 15 |
| 4.2 | RIPE.DF.%Completeness | 15 |
| 4.3 | RIPE.DF.%Accuracy | 16 |
| 4.4 | RIPE.DF.%Accuracy.Protocols | 16 |
| 4.5 | RIPE.DF.%Accuracy.MobileDevices | 16 |
| 5 | Benutzerverwaltung (WM) | 18 |
| 5.1 | RIPE.WM.Capability | 18 |
| 5.2 | RIPE.WM.%Completeness | 18 |
| 5.3 | RIPE.WM.%Accuracy | 18 |
| 5.4 | RIPE.WM.%Completeness.ThirdParties | 19 |
| 6 | Schulungsprogramm (TP) | 20 |
| 6.1 | RIPE.TP.Capability | 20 |
| 6.2 | RIPE.TP.%Completeness | 20 |
| 6.3 | RIPE.TP.%Compliance | 20 |
| 6.4 | RIPE.TP.%Compliance.ThirdParties | 21 |
| 7 | Polycys und Standardverfahren (PO) | 22 |
| 7.1 | RIPE.PO.Capability | 22 |
| 7.2 | RIPE.PO.%Completeness | 22 |
| 7.3 | RIPE.PO.%Compliance | 22 |
| 7.4 | RIPE.PO.%Compliance.ThirdParties | 23 |
| 8 | Systembeschaffung (SP) | 24 |
| 8.1 | RIPE.SP.Capability | 24 |

| | | |
|-----------|--|-----------|
| 8.2 | RIPE.SP.%Completeness | 24 |
| 8.3 | RIPE.SP.%Conformity | 24 |
| 9 | Planung und Konfiguration (PC) | 26 |
| 9.1 | RIPE.PC.Capability..... | 26 |
| 9.2 | RIPE.PC.%Completeness..... | 26 |
| 9.3 | RIPE.PC.%Conformity..... | 26 |
| 10 | Konsolidierte Cyber-Sicherheitsfähigkeit (SC) | 28 |
| 10.1 | RIPE.SC.Overall..... | 28 |
| 10.2 | RIPE.SC.Model | 28 |
| 10.3 | RIPE.SC.Policies | 28 |