Sitzungsberichte der Leibniz-Sozietät der Wissenschaften zu Berlin *116(2013), 111–122*

Dietrich Balzer

Die gegenwärtige und zukünftige Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft

1. Einleitung

Der Wirtschaftszweig „Sicherheit“ wird in der Wirtschaftsstatistik noch nicht ausgewiesen. National und international hat sich aber schon eine Sicherheitswirtschaft etabliert.

Wissenschaftliche Untersuchungen und Studien beweisen das. Auf Grund der spezifischen Eigenschaften der Automatisierungs- und Kommunikationstechnik spielt diese Technik in der Sicherheitswirtschaft eine zentrale Rolle, die auf der Einheit von Informationsgewinnung, Informationsverarbeitung und Informationsnutzung basiert.

Innerhalb der Sicherheitswirtschaft wird die Automatisierungs- und Kommunikationstechnik vor allem in folgenden Marktsegmenten eingesetzt:

- Sicherheitstechnik (Biometrie, Videotechnik, Sensorik, Leittechnik, Zutrittskontrolle);
- IT-Sicherheit (Netzsicherheit, Verschlüsselung, Virtual Private Network, Public Key Infrastructure, Smart Card);
- Sicherheitsdienstleistungen (Objekt- und Wachschutz, Risk Management, Trust Center, Sicherheits-Audits, Sicherheits-Engineering, Consulting).

Die Automatisierungs- und Kommunikationstechnik als sicherheitsorientierte Wissenschaftsdisziplin stellt für alle diese Marktsegmente Methoden und Produkte zur Verfügung, die auf die Kompensation nicht ausregelbarer Störgrößen orientieren. Dabei geht es vor allem um Lösungen der Prozessüberwachung sowie der vorbeugenden und elementaren Prozesssicherung.

Im vorliegenden Beitrag werden Probleme der Forschung und Lehre beim Einsatz der Automatisierungs- und Kommunikationstechnik für die Sicherheit von technologischen Prozessen in komprimierter Form dargestellt. Die Leibniz-Sozietät der Wissenschaften zu Berlin kann dabei besonders in Kooperation mit mittelständischen Unternehmen der Region Berlin/Brandenburg bei der Aus- und Weiterbildung sowie bei der Lösung wissenschaftlich-technischer Probleme konkrete Beiträge leisten.

2. Definitionen

Bevor die Rolle der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft dargestellt wird, sollen die Begriffe Sicherheit, Gefahr und Risiko definiert werden:

- Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.
- Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes (qualitativ oder durch sicherheitstechnische Festlegungen bestimmbar).
- Risiko ist eine Wahrscheinlichkeitsaussage bezogen auf einen technischen Vorgang oder Zustand. Dabei werden die Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß bewertet.
- Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.

3. Der Sicherheitsmarkt in Deutschland

Aus den vorliegenden Studien bzw. Analysen sollen zwei charakteristische Beispiele ausgewählt werden.

Durch den Bundesverband für Sicherheitswirtschaft (BDSW) wurde der Sicherheitsmarkt in Deutschland analysiert (s. Abbildung 1).

Dabei wurde im Wesentlichen der klassische Markt der Sicherheitstechnik betrachtet. Probleme der vorbeugenden Sicherung sind nicht analysiert worden. Aus eigener Erfahrung kann eingeschätzt werden, dass der Markt für softwarebasierte Lösungen der vorbeugenden Prozess- und Produktsicherung ca. 5 Mrd. € umfasst, sodass der gesamte Sicherheitsmarkt in Deutschland ungefähr 16 Mrd. € umfasst.

Das zweite Beispiel betrifft eine Analyse der Sicherheitswirtschaft in Berlin und Brandenburg, die von der Landesregierung in Brandenburg und dem Senat von Berlin durchgeführt wurde (vgl. Berlin Partner GmbH 2012). Die Ergebnisse können wie folgt zusammengefasst werden:

- 220 Unternehmen der Sicherheitswirtschaft wurden befragt.
- Der Umsatz aller befragten Unternehmen beträgt 2,43 Mrd. Euro pro Jahr, die Beschäftigtenzahl beträgt 24.500.
- Mehr als 50% der Unternehmen orientieren sich auf den überregionalen Markt.
- Wichtigster Zielkunde ist die Industrie, gefolgt von der öffentlichen Hand und den Betreibern von Infrastrukturen.

- 73% der Unternehmen sind an F&E-Kooperation interessiert.
- 48% haben Bedarf an akademischer Weiterbildung.

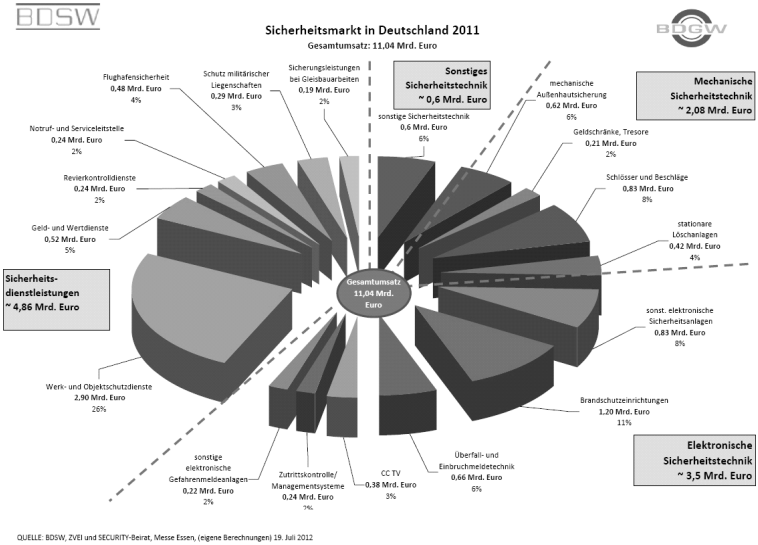

Abbildung 1: Analyse des BDSW
Quelle: BDSW 2012, S. 29

Wichtig sind vor allem die Aussagen, dass ein großer Bedarf an modernen wissenschaftlich-technischen Lösungen besteht und dass eine akademische Aus- und Weiterbildung sowohl als Vertiefungsrichtung in vorhandenen Master- und Bachelor Studiengängen als auch als selbstständige Studiengänge gewünscht wird. Außerdem zeigt die Analyse, dass die Region Berlin/Brandenburg auf dem Gebiet der Sicherheitswirtschaft eine führende Stellung in Deutschland einnimmt.

4. Algorithmen der zentralen Sicherung dezentraler Anlagen

Bevor wir auf die Algorithmen der automatischen Steuerung eingehen, soll auf folgende Vor- und Nachteile der Automatisierungs- und Kommunikationstechnik hingewiesen werden:

- Vorteile: Einheit von Informationsgewinnung (ständige standortunabhängige Prozess- und Produktüberwachung), Informationsverarbeitung (Si-

tuationserkennung, Prognose) und Informationsnutzung(Vor-Ort- und Fernsteuerung).
- Nachteile: zusätzliche Risiken durch Stabilitäts- und Sensibilitätsprobleme sowie durch Security-Probleme.

Es ist also notwendig, einen optimalen Kompromiss zwischen den Vorteilen und den Nachteilen zu erreichen.

Durch eine vergleichende Analyse der Amplitude und der Frequenz der auf das System einwirkenden Störgrößen können die Bereiche der verschiedenen Automatisierungsfunktionen und damit auch der Bereich der Prozesssicherung bestimmt werden. Abbildung 2 zeigt, wie diese Bereiche bestimmt werden können.

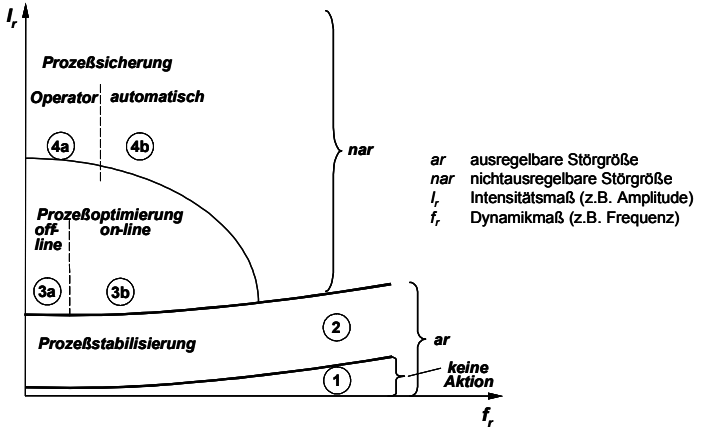

Abbildung 2: Zusammenhang zwischen Störgrößeneigenschaften und Automatisierungsfunktion Eigene Darstellung

Für die Festlegung der Struktur der Steuerungsalgorithmen wird ein so genanntes „Informationsmodell Sicherheit“ bestimmt, das Aussagen zu folgenden Prozesseigenschaften beinhaltet:
- Festlegung der Eigenschaftsprofile der Prozesselemente (Gutbereich, zulässiger Fehlbereich, unzulässiger Fehlbereich);
- dynamische Zustandsvariable (Druck, Temperatur, ...);
- stationäre Prozessparameter (Wärmedurchgangszahl, Katalysatoraktivität, ...);
- Steuergrößen (Motoransteuerung, Sollwertänderung, ...);
- Störgrößen (Umweltbedingungen, Rohstoffeigenschaften, ...).

Am Beispiel einer Ammoniak-Synthese-Anlage ist in Abbildung 3 ein konkretes Informationsmodell dargestellt.

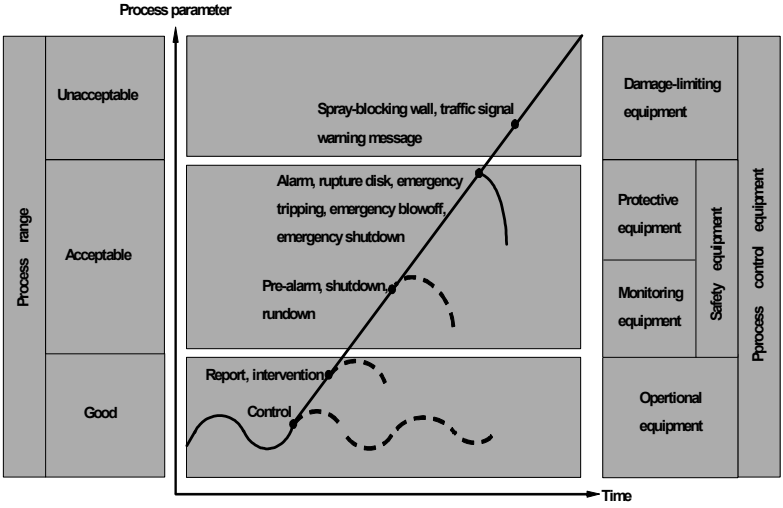

Abbildung 3: Elementary and Preventing Processsecuring of Ammonia plant
Quelle: VAN 2010b, S. 15

Die Erfahrungen auf dem Gebiet der Prozesssicherung zeigen, dass unter Nutzung des oben genannten Informationsmodells die Ljapunovsche Stabilitätstheorie eine gute Grundlage für den Entwurf der Steuerungsalgorithmen darstellt. Im Weiteren soll die Anwendung dieser Theorie erläutert werden.

Der Prozesssicherungsalgorithmus besteht aus folgenden zwei Hierarchieebenen:

- Erkennen gefährlicher Situationen;
- automatische Realisierung einer Abwehrstrategie.

Folgende Abwehrstrategien sind möglich:

- Aktivierung kalter oder heißer Redundanzen;
- Lastabwurf;
- Steuerung der Hauptprozesse auf Teil- oder Nullproduktion;
- sofortiges Abfahren der Anlage bei besonderer Gefahr für Menschen und Ausrüstungen (Grenzrisiko).

Ein gefährlicher Zustand (GZ) bzw. eine gefährliche Situation liegt dann vor, wenn eine oder mehrere Komponenten des Vektors der Zustandsgrößen q

oder des Vektors der Störgrößen x bestimmte obere Grenzwerte (q_i^o, x_k^o) überschreiten bzw. bestimmte untere Grenzwerte (q_j^u, x_e^u) unterschreiten:

$$GZ := q_i \geqq q_i^o V q_j \leqq q_j^u V x_k > x_k^o V x_e \leqq x_e^u . \tag{1}$$

Bei Erfüllung der Gleichung (1) handelt es sich um die Verletzung bestimmter technologischer bzw. apparatetechnischer Begrenzungen (z.B. Verletzung einer Grenztemperatur, eines Grenzdruckes oder einer kritischen Konzentration).

Bei der Synthese des Sicherungsalgorithmus gehen wir von folgendem mathematischen Modell des gesteuerten Systems aus:

$$\frac{dx}{dt} = f(x). \tag{2}$$

Die Ljapunov-Funktion zur Bestimmung von sicheren Einzugsbereichen hat folgendes Aussehen:

$$l(x) = const > 0 . \tag{3}$$

Die Änderungsgeschwindigkeit der Ljapunov-Funktion ist:

$$\frac{dl(x)}{dt} = p(x). \tag{4}$$

Unter Berücksichtigung von (2) haben wir:

$$\frac{dl(x)}{dt} = \frac{\partial l}{\partial x} \cdot \frac{dx}{dt} = \frac{\partial l(x)}{\partial x} \cdot f(x). \tag{5}$$

Die Bestimmung sicherer Einzugsbereiche erfolgt nun unter Verwendung der Gleichungen (2) bis (5). Abbildung 4 zeigt die prinzipielle Vorgehensweise bei der Bestimmung dieser Einzugsbereiche.

Um die Bestimmung des Einzugsbereiches zu vereinfachen, wurde die Ljapunov-Funktion in Form eines Kreises definiert. Dadurch nutzen wir nicht alle Möglichkeiten der Prozesssicherung. Andere kompliziertere Funktionen sind auch möglich und wurden auch erprobt. Dabei sind allerdings genauere mathematische Modelle des gesteuerten Systems notwendig, was zweifellos zu höheren Kosten führt.

Durch die Überführung des technologischen Systems in den sicheren Einzugsbereich wird die Prozesssicherungsaufgabe algorithmisch gelöst.

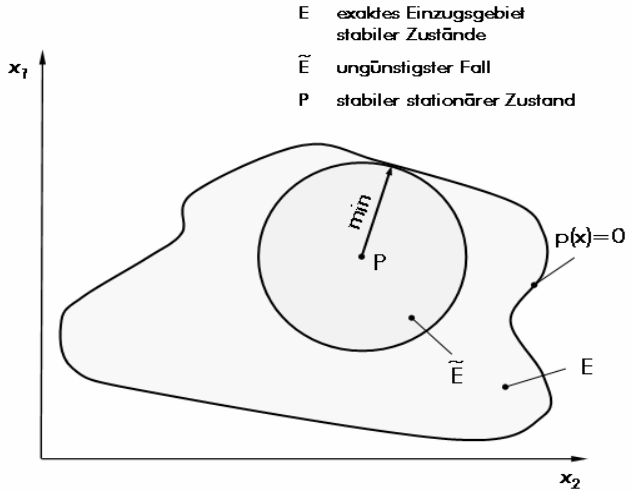

Abbildung 4: Bestimmung sicherer Einzugsbereiche
Eigene Darstellung

Die oben beschriebene Vorgehensweise wird nun auf ein komplexes System übertragen, das aus mehreren Teilsystemen besteht (s. Abbildung 5).

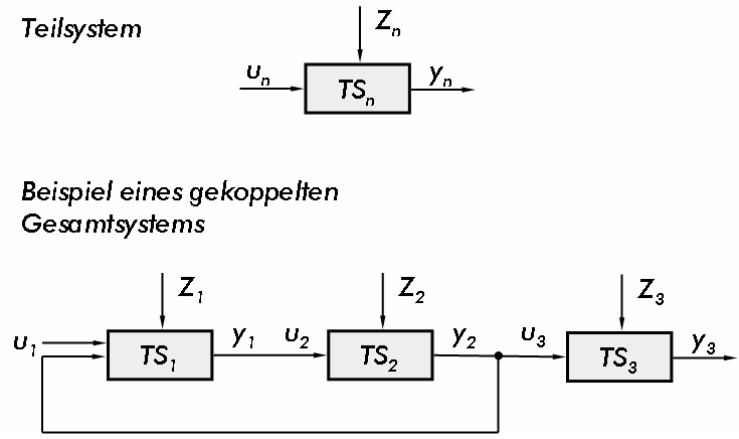

Abbildung 5: Struktur des Sicherungsobjektes
Eigene Darstellung

Die Aufgabe des Prozesssicherungssystems für das in Abbildung 4 dargestellte System besteht in der Überführung der Prozessparameter in ein Gebiet, aus dem sie in einem begrenzten Zeitbereich durch Anwendung der Abwehrstrategie keine gefährlichen Zustände erreichen (Quasistabilität).

Wir gehen vom ungünstigsten Fall aus, nämlich vom Maximum von $\frac{dl(x)}{dt} = p$:

$$p(x) = \sum_{n=1}^{N} p_n(x_n) \to \max . \tag{6}$$

Dabei ist die folgende Nebenbedingung einzuhalten:

$$1(x) = \sum_{n=1}^{N} 1_n(x_n) = const . \tag{7}$$

Darüber hinaus muss die folgende Koppelbedingung berücksichtigt werden:

$$G(x) = \sum_{n=1}^{N} g_n(x_n) = 0 . \tag{8}$$

5. Automatisierte Security-Lösungen

Wie bereits im Abschnitt 4 erwähnt, kommt es beim Einsatz moderner Automatisierungs- und Kommunikationstechnik darauf an, die Security-Probleme zu lösen.

Dabei kommet es darauf an, folgende Anforderungsprofile zu erfüllen:

- *Vertraulichkeit* (Confidentiality): Schutz vor unautorisierten Lesezugriffen, Kopieren, falschen Empfängern;
- *Integrität* (Integrity): Verhinderung unautorisierter Schreibzugriffe bzw. Datenmanipulation;
- *Authentizität* (Authentication): Glaubwürdigkeit eines Benutzers (Mensch, Kommunikationsgerät, Programm);
- *Zugriffskontrolle* (Authorisation): zugelassene Personen bzw. Dienste;
- *Nichtbestreitbarkeit* (Non-Repudiability): Verbindlichkeit, Empfangsbestätigung (erfolgt oder nicht erfolgt);
- *Verfügbarkeit* (Availability): keine Verhinderung berechtigter Zugriffe;
- *Aufzeichenbarkeit* (Auditability): Log-Files (Protokolldateien).

Es sind folgende zusätzliche Security-Lösungen für die zentrale Steuerung dezentraler Anlagen erforderlich:

- Entwurf automatisierungsspezifischer sicherer Netzwerktopologien für heterogene Netzwerke;
- funktionale Dekomposition und Skalierbarkeit von Securityfunktionen unter Beachtung der Echtzeitanforderungen;
- Schaffung von Konfigurations- und Administrationshilfen für heterogene Netzwerke bezüglich Security:
- modellbasierter Zugriffsschutz durch Prüfung der Authentizität und Nichtbestreitbarkeit der übertragenen Prozessinformationen;
- Personifizierung der Authentisierung sowie Willensbekundung mittels Integration von biometrischen Merkmalen (Fingerabdrücke und dynamische Unterschriften).

Um die oben genannten Anforderungen zuverlässig zu erfüllen, ist die Einrichtung von folgenden Schutzzonen (Security Integration Zones – SIZ) notwendig (vgl. VAN 2010b):

- SIZ 1 (hoher Schutz) für die prozessnahen Funktionen: Messen, Regeln, Steuern, elementare Prozesssicherung; on-line-closed loop;
- SIZ 2 (mittlerer Schutz) für die prozessfernen Funktionen: Bedienen, Beobachten, vorbeugende Prozesssicherung, Anlagenkoordinierung zur Kopplung mehrerer Firmenstandorte, Engineering, on-line open loop;
- SIZ 3 (geringer Schutz) für die Funktionen des Unternehmensmanagements: Wartung und Instandhaltung, Training der Operatoren und der Service-Ingenieure.

6. Beispiele realisierter Prozesssicherungssysteme

Die in den vorangegangenen Abschnitten dargestellten theoretischen Ergebnisse der automatischen vorbeugenden modellgestützten Prozesssicherung wurden an mehreren Beispielen praktisch erprobt. Die Abbildung 3 zeigt eine Anwendung für die Ammoniak-Synthese.

In Abbildung 6 ist die Struktur des zentralen Prozesssicherungssystems für dezentrale Biogasanlagen dargestellt.

Diese Anwendung besitzt ein zentrales Operatorzentrum mit den Funktionen: Bedienen, Beobachten, Trainieren, Visualisieren, vorbeugende Prozesssicherung. Das Operatorzentrum besitzt sowohl eine stationäre als auch eine mobile Komponente.

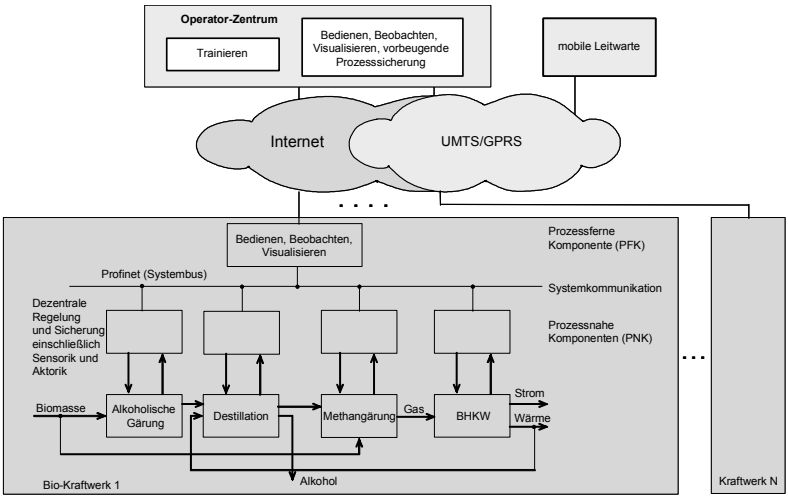

Abbildung 6: Struktur des zentralen Prozesssicherungssystems für Biogasanlagen
Eigene Darstellung

Abbildung 7 zeigt ein Prozesssicherungssystem für ein diskret-kontinuierliches technologisches System einer Papierproduktion (vgl. IPK 2005).

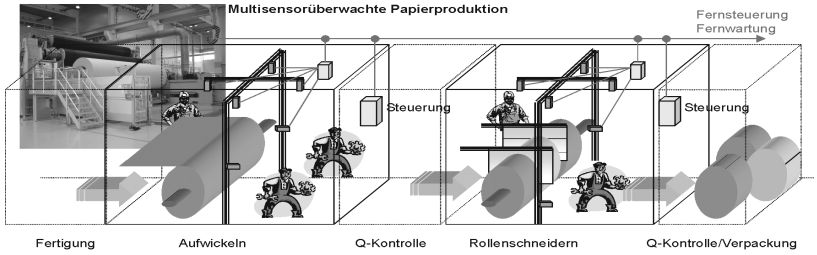

Abbildung 7: Multisensorüberwachte Produktion, Systemübersicht
Quelle: IPK 2005

Die Aufgaben und Eigenschaften dieses Prozesssicherungssystems sind:

- mehrdimensionale visuelle Erfassung;
- automatische Klassifikation;
- Erkennungsrobustheit bei wechselnden Umgebungsbedingungen;
- selektive Bewegungsanalyse;

- schnelle Algorithmen sowie optimierte, zuverlässige Kommunikation;
- Erfassung und Modellierung des Arbeits-/Gefahrenraums.

7. Akademische Lehre und Weiterbildung

In der Region Berlin/Brandenburg existieren bereits auf folgenden Gebieten Aus- und Weiterbildungsangebote:
- Sichere Identität;
- Sichere Infrastruktur;
- IT-Sicherheit/Sicherheit mit IT;
- Sicherheit und Gesellschaft;
- Urban Security.

Folgende Universitäten und Hochschulen bieten auf diesen Gebieten Lehrveranstaltungen an:
- Beuth Hochschule für Technik Berlin;
- Brandenburgische Technische Universität Cottbus (BTU);
- Charité – Universitätsmedizin Berlin;
- Deutsche Universität für Weiterbildung Berlin;
- Europa-Universität Viadrina Frankfurt (Oder);
- Fachhochschule Brandenburg (FH Brandenburg);
- Fachhochschule der Polizei des Landes Brandenburg;
- Freie Universität Berlin (FU Berlin);
- Hochschule Lausitz (FH Lausitz);
- Hochschule für Technik und Wirtschaft Berlin (HTW);
- Hochschule für Wirtschaft und Recht Berlin (HWR);
- Humboldt-Universität zu Berlin (HU Berlin);
- Steinbeis-Hochschule Berlin GmbH;
- Technische Hochschule Wildau (TH Wildau);
- Technische Universität Berlin (TU Berlin);
- Universität Potsdam.

In Ergänzung zu diesen Angeboten bereitet gegenwärtig das Georgius-Agricola-Institut (International School for Safety and Security) Bachelor- und Masterstudiengänge vor, die auf den Einsatz der Automatisierungs- und Kommunikationstechnik in der Sicherheitswirtschaft orientieren. Die Besonderheit dieser Studiengänge ist die Einführung eines Fachvertiefungsprofils „Automation/Sicherheitstechnik“ mit folgenden Fachvertiefungsmodulen:
- Fachvertiefungsmodul 1: „Sicherheitsorientierte Aktor- und Sensorsysteme“

(Informationstechnische Strukturen, Prozessmesstechnik)
(Fertigungsmesstechnik);
- Fachvertiefungsmodul 2: „Prozess- und Gebäudesicherung/Safety“
(Prozessicherungssysteme)
(Requirement-Engineering für die Gebäudesicherung)
(Gebäudesicherungssysteme);
- Fachvertiefungsmodul 3: „Security“
(Security in der Automatisierungs- und Kommunikationstechnik)
(Security-Engineering);
- Fachvertiefungsmodul 4: „Qualitätssicherung/Zuverlässigkeit“
(Qualitätsmanagement)
(Zuverlässigkeit).

Literatur

Berlin Partner GmbH (Hg.) (2012): Die Sicherheitswirtschaft in Berlin und Brandenburg. Trends – Märkte – Potenziale. Auswertung einer Unternehmensumfrage 2011. Berlin. –
URL: http://www.berlin.de/projektzukunft/fileadmin/user_upload/pdf/studien/umfrage_sicherheitswirtschaftbb_2011-12.pdf [27.04.2013]

BDSW – Bundesverband der Sicherheitswirtschaft (Hg.) (2012): Security Essen 2012: Der Sicherheitsmarkt in Deutschland. Zahlen, Daten und Fakten zur Branche. Essen. – URL: http://www.security-messe.de/media/presse_1/security_7/2012_14/3-Marktdaten~1.pdf [27.04.2013]

VAN – Virtual Automation Networks (ed.) (2010a): European R&D-Project “Virtual Automation Networks”. Final Report of Work package 11 “Project Management”. Nuremberg Moorenbrunn

VAN – Virtual Automation Networks (ed.) (2010b): European R&D-Project “Virtual Automation Networks”. Final Report of Work package 5 “Safety in Automation Systems”. Nuremberg Moorenbrunn

IPK – Institut für Produktionsanlagen und Konstruktionstechnik (2005): Abschlussbericht des Fraunhofer IPK im Rahmen des vom Berliner Senat geförderten FuE-Projektes „Sichere Produktion“. Berlin