Gekoppelte Management Systeme in der Informationssicherheit

Wolfgang Boehmer

Technische Universität Darmstadt, Morneweg Str. 30,
CASED building,
64293 Darmstadt, Germany
wboehmer@cdc.informatik.tu-darmstadt.de

Zusammenfassung

Im Bereich der Unternehmensabsicherung (Enterprise Security) haben sich Management Systeme gemäß dem Deming Zyklus (PDCA-Zyklus) etabliert. Zu nennen sind das ISMS (Information Security Management System) der ISO 27001 und das BCMS (Business Continuity Management System) des BS 25999 sowie das ITSMS (IT-Service Management System) gemäß ISO 20000. Diese drei Management Systeme sind weitgehend unabhängig voneinander entwickelt worden. Jedoch werden alle drei oftmals in den Unternehmen gleichzeitig eingesetzt. Formal lassen sich Management Systeme mit der ereignisdiskreten Systemtheorie (DES) ausdrücken und werden in diesem Artikel mittels der Nachbildungsäquivalenz mit dem Deming Zyklus verglichen. Mittels dieser Formalisierung ist es möglich die Kopplung der drei Management Systeme (ISMS, BCMS, ITSMS) in einem Unternehmen zu analysieren. Hierzu wird ein Kopplungsparameter definiert und mittels diskreter Regelkreisgleichungen gezeigt, dass im Idealfall eine starke Kopplung zwischen einem ISMS und einem ITSMS und eine schwache Kopplung zwischen einem ISMS und einem BCMS vorliegen sollte.

1 Einführung

In der Informationstechnologie haben Policies eine weitreichende Bedeutung und sind Gegenstand vielfältiger Forschungen. So werden Policies u.a. im Bereich der Firewall-Konfiguration, der Authentifizierung, Netzwerk Management erfolgreich eingesetzt. Dabei hat eine Policy zunächst einen statischen Charakter, der zulässige von unzulässigen Zuständen eines Systems, eines Prozesses oder Objekte steuert. Im Verlaufe der Zeit wurde erkannt, dass statische Policies alleine nicht den Anforderungen der Unternehmen gerecht werden. Als Konsequenz wurden dynamische Policies entwickelt, die entweder bezüglich einer zeitlichen oder einer inhaltlichen Komponente oder hinsichtlich beider Komponenten flexibel gestaltet werden können. Detaillierte Ausführungen sind z.B. bei Pucella und Weissmann (2004) zu finden [PuWe04]. Die Grundlagen hierzu sind von Meyden (1996) gelegt worden [Meyd96]. Dieser Zugewinn an Flexibilität kam den Anforderungen der Unternehmen entgegen. Ebenso wie die statischen Policies finden heute dynamische Policies ein breites Anwendungsgebiet.

Aus dem Blickwinkel der Gesamtabsicherung eines Unternehmens haften allerdings den statischen und den dynamischen Policies der gleiche Nachteil an; sie liefern keine Rückkopplung ihrer Wirkung. Damit fehlt dem Unternehmensmanagement eine übergeordnete Steuerungsmöglichkeit.

Ferner lässt sich beobachten, dass zur Absicherung eines Unternehmens häufig Management

Systeme gemäß ISO 27001, BS25999, ISO 20000 eingesetzt werden, die dem Deming Zyklus (Plan-Do-Check-Act) folgen. Die weltweit zunehmenden Zertifikate belegen den hohen Nutzwert dieser Management Systeme. Der Standard ISO 27001 stellt Anforderungen an ein Informations Sicherheits Management System (ISMS), der BS 25999 beschreibt ein Business Continuity Management System (BCMS) und die ISO 20000 beschreibt ein IT-Service Management System (ITSMS). Diese Management Systeme werden mittels Deming Zyklus (PDCA-Zyklus) beschrieben. Es existiert jedoch bis dato keine formale Beschreibung dieser Management Systeme. Ohne formale Beschreibungen lassen sich die Methoden der Informatik kaum anwenden, wie z.B. die Nachbildungsäquivalenz, die in diesem Beitrag verwendet wird.

Policies, die eine Rückkopplung besitzen – also Management Systeme – sind bisher wenig in der Informationstechnologie erforscht worden. Im Gegensatz dazu sind in der Ingenieurtechnik Systeme mit einer Rückkopplung – sogenannte Feedback Systeme – für rein technische Systeme zu finden, die als Regelkreise bezeichnet werden und die mit der ereignisdiskreten Systemtheorie beschrieben werden können.

Regelkreise der ereignisdiskreten Systemtheorie besitzen vier Elemente: die Regelstrecke, den Sensor, den Regler und den Aktuator. Die Elemente sind untereinander sequentiell verbunden und bilden den Regelkreis. Regelkreise haben eine weitreichende Bedeutung erlangt, denn es handelt sich nicht nur um ein rein technisches Modell, sondern um ein allgemeines Organisationsprinzip, das auch unter Begriffen wie Selbstregulation in der Biologie, Soziologie/Psychologie und der Systemtheorie vorzufinden ist. Für weitere Ausführungen wird auf die umfangreiche Literatur verwiesen, stellvertretend ist Miller zu nennen [Mill88]. Allgemein kann die Aufgabe von Regelkreisen wie folgt definiert werden:

Def.:	Regelkreise haben die Aufgabe, zeitveränderliche Größen eines Prozesses auf vorgegebene Werte zu bringen und trotz Störungen dort zu halten.

In diesem Beitrag wird untersucht, ob und wie eine Kopplung zwischen den Management Systemen ISMS, BCMS und einem ITSMS möglich ist. Weiterhin wird analysiert, ob es sich um eine schwache oder starke Kopplung handeln muss. Hierzu wird argumentativ auf die Regelkreise der ereignisdiskreten Systemtheorie (DES) zurückgegriffen.

Dieser Beitrag ist in vier Abschnitte unterteilt. Im zweiten Abschnitt wird gezeigt wie ein Regelkreis als Ableitung einer dynamischen Policy mit Rückkopplung erfolgt und wie dieser mit formalen Methoden ausgedrückt wird. Im dritten Abschnitt werden die Management Normen ISO 27001 (ISMS), BS 25999 (BCMS) und ISO 20000 (ITSMS) formal als Regelkreis ausgedrückt. Die Kopplung der Management Systeme wird sodann mit Hilfe des Kopplungsparameter ξ diskutiert. Im Abschnitt drei folgt eine kurze Zusammenfassung der wesentlichen Ergebnisse; mit einem Ausblick auf weiterführende Untersuchungen schließt der Beitrag.

2 Regelkreise für technische Systeme

Nachfolgend werden Regelkreise für technische Systeme diskutiert. In diesem Kontext ist nicht das Zeitverhalten der Regelkreise technischer Systeme von Interesse – welche i.d.R. durch Zustandsdifferentialgleichungen beschrieben werden – sondern das diskrete Verhalten der Regelkreise technischer Systeme, die durch algebraische Gleichungen ausgedrückt werden.

Eine Beziehung zwischen einem zeitkontinuierlichen System und einem diskreten System kann

durch eine Laplace-Transformation hergestellt werden. Die Gleichungen für den Standardregelkreis sind Laplace-Transformierte und somit algebraische Gleichungen. Das Suffix (s) deutet auf die Transformation hin. Weitere Ausführungen hierzu sind in der Literatur z.B. bei Litz (2005) zu finden [Litz05]. Im nächsten Unterabschnitt wird der Übergang von statischen bzw. dynamischen Policies zu einem Regelkreis diskutiert. Weiterhin werden die Eigenschaften von Regelkreisen erläutert.

2.1 Von statischen über dynamische Policies zu Regelkreisen

Statische Policies sind Steuerungsinstrumente, die z.B. das Zustandsverhalten eines Prozesses, Systems oder Objektes bestimmen. Dabei kann ein Zustand zugelassen oder eben gerade nicht zugelassen werden. Betrachtet man die Zustandsmenge eines Prozesses in einem Zustandsraum, so lassen sich durch eine Policy bestimmte Zustände unterdrücken, so dass nur akzeptierte Eingangswerte und damit nur bestimmte Zustände zugelassen werden.

Wird ein Prozess als deterministischer E/A-Automat ($\mathcal{A}$) modelliert, in dem keine Einschränkungen für Eingangswerte, Zustände, Zustandsübergänge und Ausgangswerte existieren, so lässt sich ein Prozess als ein 6 Tupel darstellen. Dieser enthält drei Mengen, zwei Funktionen und den Anfangszustand

$$\mathcal{A} = \{\hat{\mathcal{Z}}, \mathcal{V}, \mathcal{W}, f, g, \hat{z}_0\}. \tag{1}$$

Dabei gilt für $\hat{\mathcal{Z}}$ = Menge der Zustände mit den Zustandsgrößen $\{\hat{z}_0, ..., \hat{z}_n\} \in \hat{\mathcal{Z}}$ und für $\mathcal{V}$ = Menge der Eingangswerte mit $\{v_0, ..., v_n\} \in \mathcal{V}$ und für $\mathcal{W}$ = Menge der Ausgangswerte mit $\{w_0, ..., w_n\} \in \mathcal{W}$ und f = Zustandsübergangsfunktion für die gilt $f : \hat{\mathcal{Z}} \times \mathcal{V} \rightarrow \hat{\mathcal{Z}}$ und g = Ausgabefunktion für die gilt $g : \hat{\mathcal{Z}} \times \mathcal{V} \rightarrow \mathcal{W}$ und für $\hat{z}_0$ = Anfangszustand. Fundamental ist das Konzept des Zustandsraumes für ereignisdiskrete Systeme, die mit einer diskreten Zeitfolge $k \in \mathbb{N}$ der Ausgangswerte $w(k)$ in einem kausalen Zusammenhang zu den Eingangswerten $v(k)$ stehen. Die Gleichung 2 zeigt den Zustandsraum bzw. das Zustandsraummodell von Eingangs- und Ausgangswerten.

$$\begin{aligned} \hat{z}(k+1) &= f(\hat{z}(k), v(k)), \quad \text{mit } k = 0, 1, 2, 3, \ldots \text{ und } \hat{z}(0) = \hat{z}_0; \\ w(k) &= g(\hat{z}(k), v(k)). \end{aligned} \tag{2}$$

Mit dieser Kausalität zwischen Eingangswerten und Ausgangswerten fällt dieser Zustandsraum in die Klasse der deterministischen E/A Automaten. Gerade zur Absicherung von Unternehmen auf ein zuvor definiertes Niveau von Schutzzielen wie z.B. Vertraulichkeit, Verfügbarkeit und Integrität, hat sich herausgestellt, dass eine Rückkopplung der Wirksamkeit in vielen Fällen wünschenswert ist. Die Rückkopplung wird erzeugt, indem der aktuell gemessene Wert $w(k)$ mit dem Eingangswert/Sollwert $v(k)$ verglichen wird. Es findet ggf. eine Korrektur $u(k)$ statt, falls $v(k) \neq w(k)$ ist und dadurch ein Signal $e(k)$ erzeugt wird. Wird diese Art von Policy mit einem E/A-Automat beschrieben, so entsteht die Abb. 1. Es wird ein Automat mit einer Rückkopplung illustriert, der sich verhält wie ein einfacher linearer Laplace-Transformierter (s) Standardregelkreis für ein SISO-System (*Single-Input, Single-Output System*). Das dynamische Verhalten des Gesamtsystem $G_v(s)$ wird durch $v(k)$ und $w(k)$ beschrieben. Dabei zeigt $G_v(s)$ das äußere Verhalten des Automaten. Die Übertragungsfunktion der Korrektureinrichtung $K(s)$ regelt die Störgröße $d(k)$ bzw. die Abweichung $e(k) \in E(s)$ aus der Strecke $u(k) \in U(s)$ bzw. der internen Übertragungsfunktion $G(s)$. Im Fall des einschleifigen Standardregelkreis der Abb. 1 sind lineare Übertragungsglieder verarbeitet worden. Durch diese Rückkopplung ist stets gewährleistet, dass ein Zustand $\hat{z}(k) \in \hat{\mathcal{Z}}$, auf dem die Störung $d(k)$ einwirkt, wieder eingeregelt wird. Damit

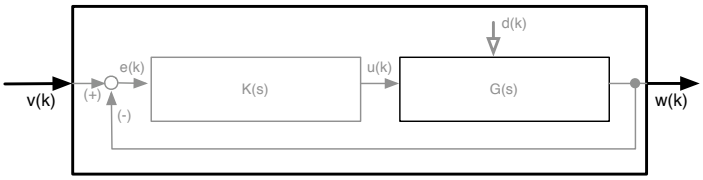

Abb. 1: Standard Regelkreis als E/A Automat

lässt sich das folgende algebraische Gleichungssystem zur Beschreibung des Standardregelkreises für ein SISO-System aufstellen: $\mathcal{W}(s) = G(s)U(s)$ und für $U(s) = K(s)E(s)$ und für $E(s) = \mathcal{V}(s) - \mathcal{W}(s)$. Von Interesse sind die Eigenschaften der diskreten Korrektureinrichtung $K(s)$ und die der diskreten Gesamtführungsübertragungsfunktion $G_v(s)$, wenn zunächst nur für die Ableitung die Störung mit $d(k) = 0$ unberücksichtigt bleibt (Störungsfreiheit).

$$G_v(s) = \frac{\mathcal{W}(s)}{\mathcal{V}(s)} = \frac{G(s)U(s)}{E(s) + W(s)} = \frac{G(s)K(s)E(s)}{E(s) + G(s)K(s)E(s)} \tag{3}$$

Durch Umformung der Gleichung 3 kann die Gesamtführungsfunktion $G_v(s)$ wie folgt ausgedrückt werden:

$$G_v(s) = \frac{G(s)K(s)}{1 + G(s)K(s)} \tag{4}$$

Ebenso kann die Korrektureinrichtung $K(s)$, die auch als Stellglied oder Aktuator bezeichnet wird, durch eine Umformung der Gleichung 4 ausgedrückt werden.

$$K(s) = \frac{U(s)}{E(s)} = \frac{\mathcal{W}(s)}{G(s)\mathcal{V}(s) - \mathcal{W}(s)} \tag{5}$$

Werden nun die in der Abb. 1 dargestellten Größen verallgemeinert, entsteht ein Standard Regelkreis mit seinen vier Elementen (Regelstrecke, Sensor/Messglied, Regler, Aktuator). Die Abb. 2 zeigt diesen Regelkreis. In diesem Regelkreis wird mittels Sensor eine Abweichung hervorgerufen, durch die Störung $d(k)$ registriert und an den Regler weitergegeben. In dem Regler wird eine Korrektur erarbeitet und mittels Signal $u(k)_R$ an den Aktuator übergeben. Dieser wirkt korrigierend mittels dem Signal $u(k)_A$ auf die Regelstrecke ein. Mit dieser Sequenz wird die Regelstrecke kontrolliert und ggf. bei Abweichungen korrigiert. Häufig sind für rein technische Systeme die Regelbewegungen vorgegeben. Ein universeller technischer Regler ist der PID-Regler. Technische Regler stehen jedoch nicht im Fokus des Artikels, da Management Systeme besser durch sozio-technische Regelkreise beschrieben werden können. Entsprechend

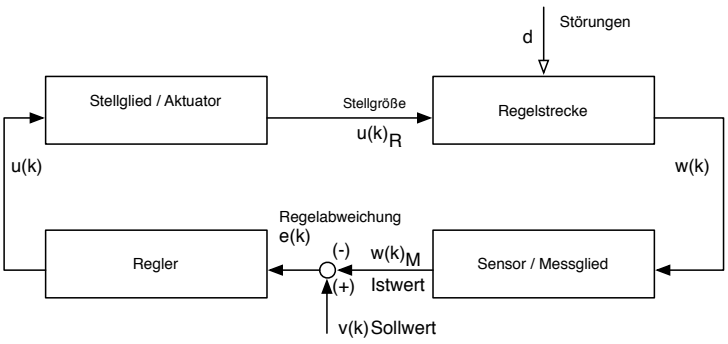

Abb. 2: Standard Regelkreis ergänzt durch Regelstrecke und Messglied

der Gleichung 4 und Gleichung 5 lassen sich für die Elemente der Abb. 2 eine Korrektureinrichtung $K(s)$ und eine Führungsübertragungsfunktion $G(s)$ entwerfen

$$\begin{aligned} K(s) &= \{\text{Regler, Aktuator}\} \\ G(s) &= \{\text{Regelstrecke, Sensor/Messglied}\}. \end{aligned} \tag{6}$$

Ein Regelkreis, der aus vier Elementen besteht und eine Rückkopplung aufweist, wird in Anlehnung an den PDCA-Zyklus (vgl. Abb. 3) als Management System definiert. Die Gleichung 6 ist dann die Management Gleichung bzw. Führungsfunktion und Korrektureinrichtung des Management Systems. Die Führungsfunktion $G(s)$ wirkt auf die Regelstrecke. Die Korrektureinrichtung $K(s)$ wirkt als Stellgröße.

2.2 Verhaltensäquivalenz und Deming Zyklus

Die eingangs erwähnten Management Systeme (ISMS, BCMS, ITSMS) basieren auf den Deming Zyklus, der die vier Elemente Plan-Do-Check-Act beinhaltet. Die Idee des PDCA-Zyklus von Deming basiert auf der Imperfektion von sozio-technischen Systemen und der Notwendigkeit einer Rückkopplung [Demi86]. Wenn die vier Elemente als Zustände interpretiert werden, lässt sich aus dem PDCA-Zyklus ein Standardautomat generieren. In der Abb. 3 ist der Deming Zyklus als Automatengraph skizziert. Es werden die vier Elemente als Zustände $z_{(1,\ldots,4)} \in \mathcal{Z}$ dargestellt und die Zustandsübergänge als Ereignisse $\sigma_{(1,\ldots,4)}$. Mit σ_0 ist das Anfangsereignis in der Abb. 3 skizziert. Ein Endzustand Z_F, wie bei Standardautomaten, existiert jedoch nicht direkt, da es sich um einen kontinuierlichen Verbesserungsprozess handelt. Dieser Verbesserungsprozess wird als Kreislauf (Regelkreis) ohne Endzustand dargestellt. Ein Zustandswechsel δ wird

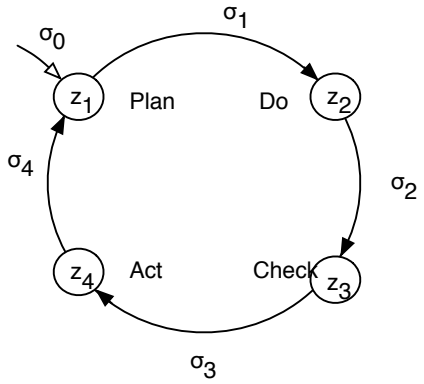

Abb. 3: PDCA-Zyklus nach Deming als Automatengraph

durch $z_n \xrightarrow{\sigma_n} z_{n+1}$ vorgenommen. Somit ist der Nachfolgezustand durch $z_{n+1} = \delta(z_n, \sigma_n)$ bestimmt. Folglich kann der Deming Zyklus als Standardautomat oder als Quintupel $\mathcal{D}$ beschrieben werden:

$$\mathcal{D} = \{\mathcal{Z}, \Sigma, \delta, z_0, Z_F\}, \tag{7}$$

mit $\mathcal{Z} = \{z_1, z_2, z_3, z_4\}$ und $\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ sowie $z_0 = z_1$ und $Z_F = z_1'$. Die Zustandsübergangsfunktion kann wie folgt ausgedrückt werden:

$$\delta : \mathcal{Z} \times \Sigma \longrightarrow \mathcal{Z} \tag{8}$$

Wird beachtet, dass $Z_F = z_1' \neq z_1$ ist, wird im Sinne des Deming Zyklus eine Verbesserung erreicht. Diese Verbesserung strebt jedoch nach (n) Durchläufen des Zykluses einen Gleichgewichtszustand an. Wie Böhmer (2009a) aufgezeigt hat, entspricht dieser Zustand einem Balance-Zustand, der als Gleichgewicht interpretiert werden kann [Boeh09]. Immer dann, wenn sich der nachfolgende Zustand von dem vorherigen Zustand nicht mehr unterscheidet, ist das System in einem Gleichgewichtszustand. Der Deming Zyklus ist dann ausbalanciert. Für diesen und nur für diesen Fall ist dann $Z_F = z_1$. Verantwortlich für das Erreichen des Gleichgewichtszustandes sind die Elemente Check (Prüfen auf Verbesserungen) und Act (Durchführen von Verbesserungen).

Generell kann ein E/A-Automat, wie in Gleichung 1 dargestellt, in einen Standardautomat überführt werden, wenn $v/w = \hat{\sigma}$ mit $\hat{\sigma}$ als diskretes Ereignis der Ereignismenge $\hat{\Sigma}$ gilt und der Endzustand mit $\hat{z}_F \in \hat{\mathcal{Z}}$ definiert wird. Weiterhin gilt $\hat{\Sigma} = \{\mathcal{V}, \mathcal{W}\}$. Dieses diskrete Ereignis, das zu einem Zustandswechsel von $\hat{z}$ nach $\hat{z}'$ führt, wird mit $\hat{\sigma}$ bezeichnet und mit $\hat{z} \xrightarrow{\hat{\sigma}} \hat{z}'$ dargestellt. Die Übergangsfunktion wird mit $\hat{\delta}$ bezeichnet. Damit kann der E/A Automat der Gleichung 1 in Analogie zur Gleichung 7 in ein Standardautomat als Quintupel überführt werden

$$\hat{\mathcal{A}} = \{\hat{\mathcal{Z}}, \hat{\sigma}, \hat{\delta}, \hat{z}_0, \hat{z}_F\}. \tag{9}$$

Wird der Standardautomat $\hat{\mathcal{A}}$ mit vier Zuständen definiert, so gilt für $\hat{\mathcal{Z}} = \{\hat{z}_1, \hat{z}_2, \hat{z}_3, \hat{z}_4\}$ und $\hat{\Sigma} = \{\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3, \hat{\sigma}_4\}$ sowie $\hat{\delta} = \hat{\mathcal{Z}} \times \hat{\Sigma} \longrightarrow \hat{\mathcal{Z}}$ und für $\hat{z}_0 = \hat{z}_1$ und $\hat{Z}_F = \hat{z}_1'$. Basierend auf dem Antwortverhalten zweier Automaten lassen sich die Begriffe wie Ähnlichkeit und Äquivalenz unterscheiden. Dabei ist die Ähnlichkeit durch die Eingaben und Ausgaben des Automaten bestimmt. Diese Ähnlichkeit wird als Schnittstellenäquivalenz bezeichnet. Die Schnittstellenäquivalenz wird in diesem Artikel nicht weiter untersucht sondern nur die Nachbildungsäquivalenz. Gemäß dem Axiom von Milner gelten zwei Zustände als gleich, wenn sie nicht durch (eine Kombination von) Beobachtungen unterschieden werden können [Miln06]. Eine Bi-simulation (Nachbildungsäquivalenz) zwischen zwei Objekten ist somit ein Transitionssystem, welches das beobachtbare *Verhalten* wiedergibt, das beiden Objekten gemeinsam ist. Falls zwischen dem Deming Quintupel $\mathcal{D}$ und einem Standardautomaten wie z.B. $\hat{\mathcal{A}}$ eine Relation zwischen ihren Zuständen existiert, so gilt die Nachbildungsäquivalenz $\mathfrak{S}$, mit

$$\mathfrak{S}_{\hat{\mathcal{A}},\mathcal{D}} \subset \hat{\mathcal{A}} \times \mathcal{D}. \tag{10}$$

Dabei sind $\mathcal{Z}_{\mathcal{D}}$ und $\hat{\mathcal{Z}}_{\hat{\mathcal{A}}}$ die Zustandsmengen der beiden Automaten $\mathcal{D}$ und $\hat{\mathcal{A}}$. Die Gleichung 10 zeigt die Simulationsrelation für die Aussage $\hat{\mathcal{A}}$ simuliert $\mathcal{D}$. Die Simulationsrelation ordnet die Zustände der Automaten $\mathcal{D}$ und $\hat{\mathcal{A}}$ einander zu, und zwar in der Bedeutung, dass der zweite Zustand des Pärchens z.B. $(z_1, \hat{z}_1) \in \mathfrak{S}$ den ersten simuliert und somit $z_1 \sim \hat{z}_1$ gilt. Die Anzahl der Zustände können in beiden Automaten unterschiedlich sein; dies ist kein Widerspruch zur Relation $\mathfrak{S}$. Wenn $\mathcal{D}|z_i$ und $\hat{\mathcal{A}}|z_j$ für alle Eingabesequenzen k äquivalent sind, werden sie k-äquivalent genannt. Beim Deming Zyklus ist $k = 4$ (vgl. Abb. 3). Die k-äquivalenten Zustände sind auch l-äquivalent für alle $l \leq k$. Nicht äquivalente Zustände werden unterscheidbar genannt. Alle Zustände, die durch die Eingabesequenzen der Länge k unterscheidbar sind, werden k-unterscheidbar genannt.

3 Regelkreise und Normen für Managementsysteme

In diesem Abschnitt werden die Regelkreis-Elemente und Management Systeme diskutiert und es wird ihre Äquivalenz zu Standardautomaten mit Rückkopplung gezeigt. Es wird gezeigt, wie

die Nachbildungsäquivalenz (vgl. Gleichung 10) zwischen dem Standardautomaten des PDCA-Zyklus durch Elemente eines Standard Regelkreises bzw. Standardautomaten der Normen ISO 27001, BS 25999 und ISO 20000 ausgedrückt werden kann. Management Systeme, die in den Normen ISO 27001, BS 25999 und ISO 20000 definiert werden, können als sozio-technische Systeme betrachtet werden. Für Managementsysteme, die eng mit der Wertschöpfungskette eines Unternehmen verbunden sind, wie z.B. das Management System gemäß ISO 27001(ISMS) und BS 25999 (BCMS) oder auch das für die ISO 20000, wird die These aufgestellt, dass diese gekoppelt sein müssen.

3.1 Regelkreis der ISO 27001 (ISMS)

Im Wesentlichen folgt ein ISMS einem PDCA-Zyklus. Werden die Regelelemente eines ISMS auf einen Standard Regelkreis (vgl. Abb. 2) übertragen, so entsteht ein Regelkreis wie in Abb. 4 dargestellt. In Abb. 4 sind die vier Elemente eines Management Systems gemäß Deming Zyklus und die vier Elemente eines Regelkreises illustriert. Das in der Abb. 4 dargestell-

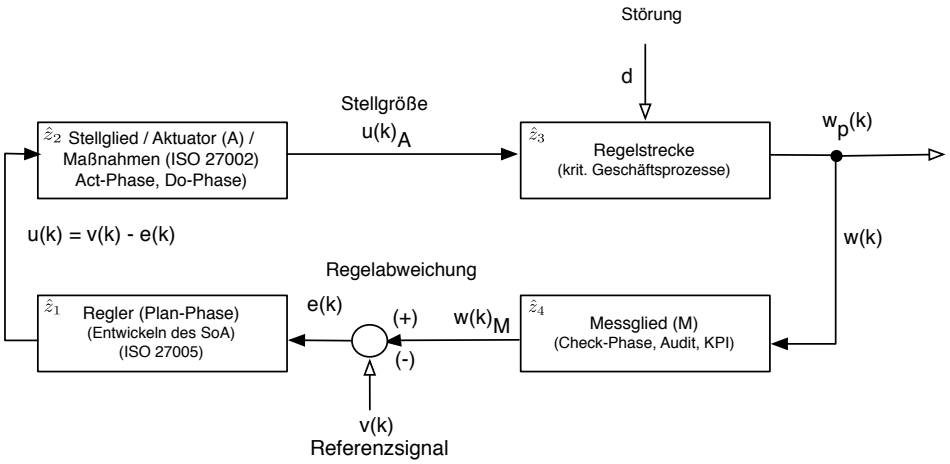

Abb. 4: Regelkreis eines ISMS

te Referenz-Signal (Sollwert) $v(k)$ repräsentiert in dem Regelkreis die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit für ein zuvor definiertes Niveau. Das aktuelle Sicherheitsniveau $w(k)$ wird durch die Störung (d) auf der Regelstrecke erzeugt. Das vom Sensor gemessene aktuelle Sicherheitsniveau wird mit $w(k)_M$ bezeichnet. Der Regler korrigiert mittels des Referenzsignals $v(k)$, um das zuvor definierte Sicherheitsniveau wieder herzustellen. Als Korrekturmaßnahme ist das Signal $u(k) = v(k) - e(k)$ zu verstehen. Es spiegelt die Aktualisierung der Security Policy durch Maßnahmen wieder. Im Aktuator werden die Maßnahmen konkretisiert und in Prozeduren und Arbeitsanweisungen umgesetzt. Das Signal $u(k)_A$ illustriert das korrigierte Signal, das auf die Regelstrecke einwirkt und eine Verbesserung erzeugt.

Es wird nun untersucht, ob zwischen dem Standardautomat des Deming Zyklus $\mathcal{D}$ und dem Standardautomaten des Regelkreises $\hat{\mathcal{A}}_{ISMS}$ für ein ISMS eine Äquivalenz gemäß der Gleichung 10 existiert. Bei der Überführung des Regelkreises in den Standardautomat $\hat{\mathcal{A}}_{ISMS}$ werden die vier Zustände $\hat{z}_1$ = Regler/Controller, $\hat{z}_2$ = Aktuator/Stellglied, $\hat{z}_3$ = Regelstrecke und $\hat{z}_4$ = Sensor/Messglied definiert (vgl. Abb. 4). Werden die vier Zustände des $\hat{\mathcal{A}}_{ISMS}$ mit dem Standardautomat des Deming Zyklus mittels der Gleichung 10 verglichen, ergibt sich für $(z_1, \hat{z}_1) \in \mathfrak{S} = z_1 \sim \hat{z}_1$ und für $(z_2, \hat{z}_2) \in \mathfrak{S} = z_2 \sim \hat{z}_2$ und für $(z_3, \hat{z}_4) \in \mathfrak{S} = z_3 \sim \hat{z}_4$ und

für $(z_4, \hat{z}_2) \in \mathfrak{S} = z_4 \sim \hat{z}_2$. Anschaulich können diese Ausführungen aus der Perspektive des Standardautomat $\mathcal{D}$ wie folgt dargestellt wird:

Zustand 1: Planung → Statement of applicability (SoA) (ISO 27005) → Regler

Zustand 2: Durchführung & Anwendung → Maßnahmen (ISO 27002) → Aktuator

Zustand 3: Prüfung & Kontrolle → Check Phase, → Sensor/Messglied

Zustand 4: Korrektur → Act Phase, Korrektur vornehmen → Aktuator

Ersichtlich ist, dass nicht für alle k des Deming Zykluses eine Nachbildungsäquivalenz existiert, wie z.B. für den Zustand $\hat{z}_3$. Die Regelstrecke wird in dem Deming Zyklus nicht abgebildet. Diese wird nur implizit durch den Scope der jeweiligen Norm definiert. Der Scope für ein ISMS gemäß ISO 27001 ist die Wertschöpfungskette eines Unternehmens. In einem Regelkreis ist die Regelstrecke jedoch Bestandteil des Standardautomaten. Somit liegt lediglich eine l-Äquivalenz vor, denn der Zustand $\hat{z}_{k=3}$ ist unterscheidbar.

3.2 Regelkreis der BS 25999 (BCMS)

Ein Business Continuity Management System (BCMS) ist auf massive Störungen (d) (Krise) reaktiv ausgerichtet und reagiert erst dann, wenn eine Krise bzw. eine Katastrophe eingetreten ist. Im Falle einer Katastrophe wird der Business Continutiy Plan (BCP) und der Desaster Recovery Plan (DRP) aktiv. Damit wird das Überleben der Geschäftsprozesse sichergestellt. Bei den BCPs handelt es sich um Ersatzprozesse, oftmals auch als Notfallprozesse bezeichnet, die im Falle einer Katastrophe aktiv werden und die ein Unternehmen für einen begrenzten Zeitraum vital halten. Denn eine Unterbrechung der kritischen Geschäftsprozesse kann nur für einen identifizierten Zeitraum toleriert werden. Dieser Zeitraum wird durch die MTPD (Maximum tolerable period of disruption) beschrieben. Innerhalb dieses definierten Zeitraums (MTPD) müssen die Notfallprozesse aktiviert worden sein und reibungslos funktionieren. Denn mit diesen Notfallprozessen wird ein Umsatz auf einem akzeptablen Niveau erzielt und somit das Überleben der Firma gesichert. Ein Regelkreis für ein BCMS kann in ganz ähnlicher Weise wie der Regelkreis eines ISMS dargestellt werden (vgl. Abb. 4) wie bei Böhmer (2010a) illustriert wird [Boeh10].

Es wird nun untersucht, ob zwischen dem Standardautomat des Deming Zyklus $\mathcal{D}$ und dem Standardautomaten des Regelkreises $\hat{\mathcal{A}}_{BCMS}$ für ein BCMS eine Äquivalenz gemäß der Gleichung 10 existiert. Bei der Überführung des Regelkreises in den Standardautomat $\hat{\mathcal{A}}_{BCMS}$ werden wiederum die vier Zustände $\hat{z}_1$ = Regler/Controller, $\hat{z}_2$ = Aktuator/Stellglied, $\hat{z}_3$ = Regelstrecke und $\hat{z}_4$ = Sensor/Messglied definiert (vgl. Abb. 4). Die vier Zustände des $\hat{\mathcal{A}}_{BCMS}$ können mit dem Standardautomat des Deming Zyklus mittels der Gleichung 10 verglichen werden. Anschaulich können diese Ausführungen aus der Perspektive des Standardautomat $\mathcal{D}$ wie folgt skizziert werden:

Zustand 1: Planung → BIA und ISO 27005

Zustand 2: Durchführung & Anwendung → Übungen von BCP/DRP

Zustand 3: Prüfung & Kontrolle → Messung der Qualität der Übungen (MTPD), → Sensor

Zustand 4: Korrektur → Act Phase, Korrektur vornehmen → Aktuator

Im Ergebnis lässt sich festhalten, dass, wie beim Regelkreis eines ISMS, lediglich eine *l*-Äquivalenz vorliegt, denn der Zustand $\hat{z}_{k=3}$ ist unterscheidbar.

3.3 Regelkreis der ISO 20000 (ITSMS)

Ziel und Zweck des IT-Service Management ist es, eine Automatisierung und Standardisierung im Bereich der IT-Service zu erzielen. Hierzu werden eine Reihe Prozesse (Incident Management, Problem Management, Change Management, etc.) definiert, die ineinander greifen und mittels Kennzahlen gemessen werden können. Das IT-Service Management System (ITSMS) gemäß ISO 20000-1:2005 und ISO 20000-1:2005 folgt ebenfalls dem PDCA-Zyklus (vgl. Abb. 3) und wurde aus der IT-Infrastructur Library (ITIL) bzw. dem BS 15000 abgeleitet. Eine Einführung bzw. ein Überblick ist bei Engel et al. (2008) zu finden [EnBB08]. Es wird nun untersucht, ob zwischen dem Standardautomat des Deming Zyklus $\mathcal{D}$ und dem Standardautomaten des Regelkreises $\hat{\mathcal{A}}_{ITSMS}$ für ein ITSMS eine Äquivalenz gemäß der Gleichung 10 existiert. Bei der Überführung des Regelkreises in den Standardautomat $\hat{\mathcal{A}}_{ITSMS}$ werden die vier Zustände $\hat{z}_1$ = Regler/Controller, $\hat{z}_2$ = Aktuator/Stellglied, $\hat{z}_3$ = Regelstrecke und $\hat{z}_4$ = Sensor/Messglied definiert (vgl. Abb. 4). Die vier Zustände des $\hat{\mathcal{A}}_{ITSMS}$ können mit dem Standardautomat des Deming Zyklus mittels der Gleichung 10 verglichen werden. Anschaulich können diese Ausführungen aus der Perspektive des Standardautomat $\mathcal{D}$ wie folgt skizziert werden:

Zustand 1: Planung → IT-Objekte, IT-Infrastruktur, Service Management

Zustand 2: Durchführung & Anwendung des Service Management →

Zustand 3: Prüfung & Kontrolle → Messung der Qualität des Services, → Sensor / Monitoring

Zustand 4: Korrektur → Act Phase, Korrektur/Verbesserung vornehmen → Aktuator

Im Ergebnis lässt sich festhalten, dass, wie beim Regelkreis eines ISMS und BCMS, lediglich eine *l*-Äquivalenz vorliegt, denn der Zustand $\hat{z}_{k=3}$ ist unterscheidbar.

3.4 Enterprise Architekturen und der Kopplungsparameter ξ

Unter dem Begriff Kopplung wird allgemein die Verknüpfung von verschiedenen Systemen, Anwendungen oder Softwaremodulen verstanden, sowie ein Maß, das die Stärke dieser Verknüpfung bzw. der daraus resultierenden Abhängigkeit beschreibt. Das Maß der Stärke der Kopplung wird in diesem Artikel durch den Kopplungsparameter ξ ausgedrückt. Ist $\xi \leq 1$ liegt eine geringe Kopplung und somit eine schwache Wechselwirkung vor. Ist $\xi \gg 1$ liegt eine starke Kopplung und somit eine starke Wechselwirkung vor. Die Gleichung 11 beschreibt diesen Zusammenhang

$$\xi = \begin{cases} \leq 1 & \text{geringe Kopplung, schwache Wechselwirkung} \\ \geq 1 & \text{starke Kopplung, starke Wechselwirkung.} \end{cases} \tag{11}$$

Um die Kopplung von Management Systemen diskutieren zu können, ist es erforderlich die Enterprise Architektur detaillierter zu betrachten. Enterprise Architekturen werden als hierarchische Ebenen verstanden. So wird in dem Artikel von Brandt et al. (2008) aufgezeigt, das diese als eine dreistufig gegliederte hierarchische Ebene aufgefasst werden kann [BEBR08]. Dagegen wird in dem Beitrag von Braun und Winter (2007) [BrWi07] und Winter und Schelp

(2008) [WiSc08] eine fünfstufige gegliederte hierarchische Ebene postuliert. Jedoch sind die Sichtweisen der Autoren kompatibel [BEBR08], [BrWi07], [WiSc08].

Abb. 5 skizziert diese drei Ebenen und zeigt, auf welcher Ebene die Management Systeme eingesetzt werden. Die oberste Ebene zeigt die Ebene der Geschäftsprozesse. Hier ist sowohl das ISMS der ISO 27001 als auch das BCMS des BS25999 platziert, jedoch wirkt BCMS auf die Notfallprozesse. Aus dem Blickwinkel der ISO 9001 gehört das ISMS und das BCMS zu den Führungsprozessen. Auf der nächsten unteren Ebene (IT-Service-Ebene) ist das ITSMS der ISO 20000 platziert. Unterhalb dieser Ebene sind die IT-Objekte (Knoten) angesiedelt. Mittels Kombination der Gleichung 11 mit der Gleichung 12 können Kopplungen zwischen

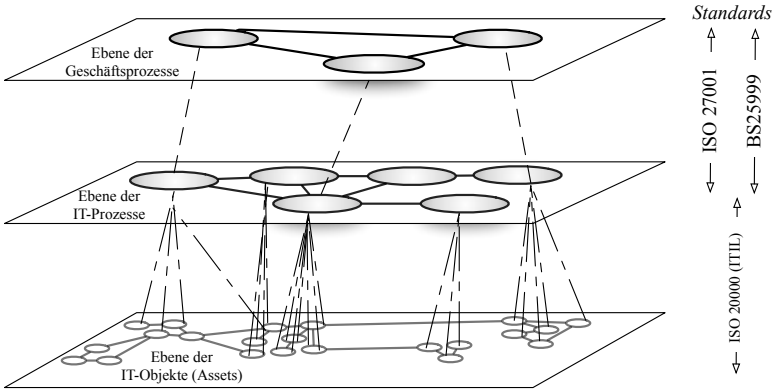

Abb. 5: Enterprise Architektur und Management Systeme

Management Systeme untersuchen werden. Als Kopplungskriterium wird die Regelkreisgleichung, bestehend aus der Korrektureinrichtung und die Führungsfunktion wie in Gleichung 6 definiert. Falls die Führungsfunktion und die Korrekturvorrichtung eines Management Systems von einem anderen Management System abhängt, liegt eine starke Kopplung vor. Hängt nur die Führungsfunktion aber nicht die Korrekturfunktion oder die Korrekturfunktion aber nicht die Führungsfunktion von einem anderem Management System ab, so liegt nur eine schwache Kopplung vor. Besteht keine Abhängigkeit zwischen der Führungsfunktion und der Korrekturfunktion zwischen zwei Management Systemen, liegt keine Kopplung vor. Die Gleichung 12

$$\xi = \begin{cases} 1 & \text{falls } G(s)_i = f(G(s)_{i+1}) \vee K(s)_i = f(K(s)_{i+1}) \\ 1/2 & \text{falls } G(s)_i = f(G(s)_{i+1}) \wedge K(s)_i = f(K(s)_{i+1}) \\ sonst & \end{cases} \tag{12}$$

beschreibt die Kopplung zwischen zwei Management Systemen $G(s)_i$, $K(s)_i$ und $G(s)_{i+1}$, $K(s)_{i+1}$. Nach Böhmer (2009) sind beide Normen ISO/IEC 27001 und BS 25999 über die Risikoanalyse verbunden [Boeh09]. Wenn eine präventive Behandlung von Risiken vorgenommen werden soll, so ist das ISMS der ISO 27001 zu favorisieren. Wenn eine reaktive Behandlung der Risiken aus Kosten/Nutzen Betrachtungen vorgenommen werden soll, weil mit dem Eintritt der Risiken in sehr seltenen Fällen zu rechnen ist, diese jedoch eine erhebliche Auswirkung auf die Wertschöpfungskette haben werden, so ist das BCMS des BS 25999 in dem Unternehmen zu favorisieren. Da ein BCMS in erster Linie auf die Business Continuity Prozesse ausgerichtet ist, ist nur die Korrekturvorrichtung mit den Assets bzw. Ressourcen der kritischen

Geschäftsprozessen gekoppelt. Wird nun das ISMS gemäß ISO 27001 als das $i - te$ Management System und das BCMS gemäß BS25999 als das $i - te + 1$ Management System bezeichnet, so liegt folgender Fall vor

$$\xi = 1/2 \text{ weil } G(s)_i \neq f(G(s)_{i+1}) \text{ aber } K(s)_i = f(K(s)_{i+1}). \tag{13}$$

Als Ergebnis lässt sich festhalten, dass eine geringe Kopplung gegeben ist und somit eine schwache Wechselwirkung zwischen einem ISMS und einem BCMS vorliegen muss. Wird nun die Kopplung zwischen einem ISMS gemäß ISO 27001 ($i - te$ Management System) und das ITSMS gemäß ISO 20000 ($i - te + 1$ Management System) in der Gleichung 14 betrachtet, so lässt sich aus der Kopplung folgendes ableiten. Falls in einem Unternehmen die kritischen Geschäftsprozesse von IT-Objekten abhängen (vgl. unterste Ebene der Abb. 5) so muss eine Ebene des IT-Service Management existieren. D.h. es ist eine funktionale Abhängigkeit zwischen diesen drei Ebenen vorhanden. Denn die kritischen Geschäftsprozesse sind abhängig von den Schutzzielen (Verfügbarkeit, Vertraulichkeit, Integrität), die u.a. von den Prozessen des IT-Service Management berücksichtigt werden müssen. Die Korrekturvorrichtung stellt eine partielle (bezogen auf die IT-Objekte) Abhängigkeit zwischen einem ISMS und einem ITSMS her. Es liegt folgende Kopplung vor:

$$\xi = 1 \text{ weil } G(s)_i = f(G(s)_{i+1}) \vee K(s)_i = f(K(s)_{i+1}). \tag{14}$$

Hieraus wird geschlossen, dass eine starke Kopplung und somit eine starke Wechselwirkung vorliegen muss. Als Konsequenz für die Praxis bedeutet dies, dass die Service Level Agreements (SLA) des ITSMS an die kritischen Geschäftsprozesse gekoppelt sein müssen.

3.5 Gekoppelte Management Systeme versus integrierte Management Systeme

Es wird die Meinung vertreten, dass ein grundsätzlicher Unterschied zwischen einem gekoppelten und einem integrierten Management System existiert. Nur ein gekoppeltes Management System besitzt eine Kopplungsfunktion, die etwas über die Art der Kopplung aussagt (stark, schwach) (vgl. Gleichung 11). Integrierte Management Systeme dagegen vereinen zwei Management Systeme zu einem einzigen Management System. Zu nennen sind z.B. die Integration des Management Systems der ISO 9001 und der ISO 27001. Aus Sicht der ISO 9001 wird die Prozesskette der Wertschöpfung durch die Führungsprozesse gesteuert und durch die unterstützenden Prozesse bedient. Ferner wird die Meinung vertreten, dass die ISO 27001 die operationellen Risiken gemäß Basel II betrachtet und sich somit auf der gleichen Ebene wie die Risikobetrachtung der Markt- und finanziellen Risiken befinden muss. Die ISO 20000 ist dagegen den unterstützenden Prozessen hinzuzuzählen und eine Integration – wie z.B. die ISO 27013 vorschlägt – nur sinnvoll, wenn es sich um ein Rechenzentrum handelt. Wird jedoch die IT-Infrastruktur nebst IT-Services ausgelagert (Outsourcing), ist eine Integration der Management Systeme ISO 20000 und ISO 27001 nicht zielführend, jedoch eine Kopplung sehr wünschenswert.

4 Zusammenfassung und Ausblick

In diesem Beitrag konnte gezeigt werden, dass Regelkreise, die in der ereignisdiskreten Systemtheorie für technische Systeme beschrieben werden, auch auf sozio-technische Systeme übertragen werden können. Diese werden als Management Systeme bezeichnet und verhalten sich äquivalent zu technischen Regelkreisen, wie mit der Bi-Simulationsfunktion gezeigt

werden konnte. Anhand von drei Management Systemen (ISO27001, BS25999, ISO 20000) wurde das Verhalten nach dem PDCA-Zyklus und dem Regelkreis untersucht. Weiterhin wurde ein Kopplungsparameter definiert und mit den Regelkreisgleichungen der ISO27001, BS25999 und ISO 20000 kombiniert. Ergebnis ist, dass zwischen einem ISMS und einem ITSMS eine starke Kopplung herrschen muss und zwischen einem ISMS und einem BCMS eine schwache Kopplung anzustreben ist. Praktischer Nutzen bzw. Handlungsempfehlungen für Unternehmen ist, dafür Sorge zu tragen, dass die SLAs des IT-Service Management mit den kritischen Geschäftsprozessen im Einklang stehen.

Literatur

[BEBR08] C. Brandt, T. Engel, W. Boehmer, C. Roeltgen: Diskussionsvorschlag einer Lösungsskizze zur Behandlung von operationellen IT-Sicherheitsrisiken nach Basel II auf der Grundlage von Anforderungen der Credit Suisse. *In: MKWI-2008, München* (2008).

[Boeh09] W. Boehmer: Survivability and Business Continuity Management System According to BS-25999. In: *SECUWARE '09, Athen/Glyfada (Greece), IEEE Computer Society* (2009), p. 142–147.

[Boeh10] W. Boehmer: Managementsysteme sind Balance-Systeme – Diskussion relevanter Kennzahlen eines ISMS gemäß ISO/IEC 27001:2005. *In: MKWI-2010, Göttingen* (2010).

[BrWi07] C. Braun, R. Winter: Integration of IT service management into enterprise architecture. *In: SAC '07:*, ACM, New York, NY, USA (2007), 1215–1219.

[Demi86] W. E. Deming: Out of the Crisis. ISBN-13: 9780911379013, MIT Press (MA) (1986).

[EnBB08] C. Engle, J. Brewster, G. Blokdijk: ISO/IEC 20000 Certification and Implementation Guide. Emereo Pty Ltd, London, UK, (2008).

[Litz05] L. Litz: Grundlagen der Automatisierungstechnik, Regelungssysteme - Steuerungssysteme - Hybride Systeme. ISBN-3-486-27383-3, Oldenbourg Verlag (2005).

[Meyd96] R. van der Meyden: The Dynamic Logic of Permission. In: *J. Log. Comput.*, 6, 3 (1996), 465–479.

[Mill88] R. M. Miller: Market automation: self-regulation in a distributed environment. In: *SIGOIS Bull.*, 9, 2-3 (1988), 299–308.

[Miln06] R. Milner: Pure bigraphs: structure and dynamics. In: *Inf. Comput.*, 204, 1 (2006), 60–122.

[PuWe04] R. Pucella, V. Weissman: Foundations of Software Science and Computation Structures, Springer Berlin / Heidelberg, *Lecture Notes in Computer Science*, Bd. 2987/2004, Kap. Reasoning about Dynamic Policies (2004), 453–467.

[WiSc08] R. Winter, J. Schelp: Enterprise architecture governance: the need for a business-to-IT approach. *In: SAC* (2008), 548–552.