Heuristische Handlungsmuster

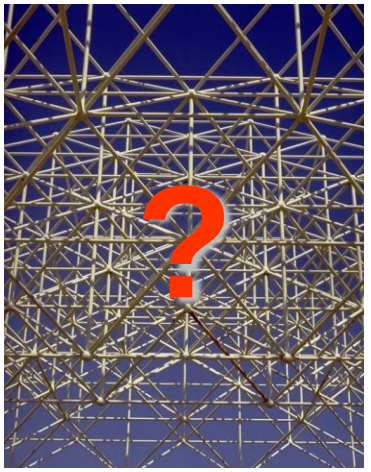
im Security Management

Der klassische Sicherheitsbegriff

„Sicherheit bezeichnet einen Zustand, der weitgehend frei von Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.“

Dilemma 1 : So kann Sicherheit nicht mehr garantiert werden

Sicherheit als ‚relativen Zustand der Gefahrenfreiheit' können wir heute oftmals nicht mehr garantieren, weil:

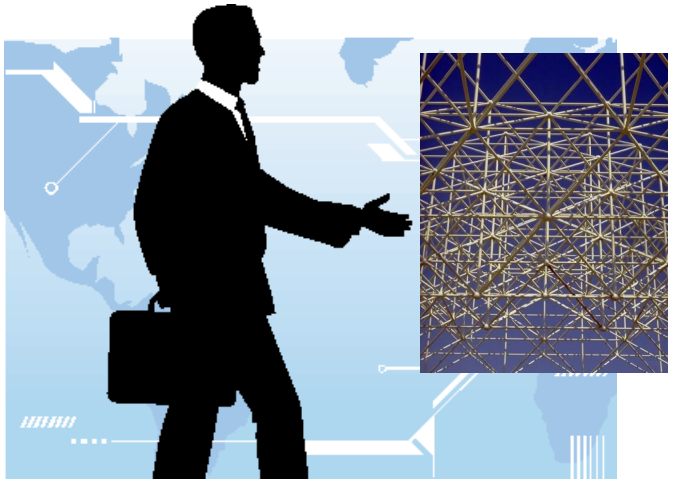


- **die Komplexität des Aktionsraumes in dem wir uns bewegen, in den letzten Jahren extrem angestiegen ist**
- **keine ausreichenden Vorkehrungen zur Beherrschung dieser Komplexität ergriffen wurden.**
- **das Postulat zur Notwendigkeit ständigen Wachstums und unbegrenzter Weiterentwicklung, den Vorrang gegenüber der Beherrschbarkeit von Prozessen in unserer Gesellschaft hat.**

Der moderne, zutreffendere Sicherheitsbegriff

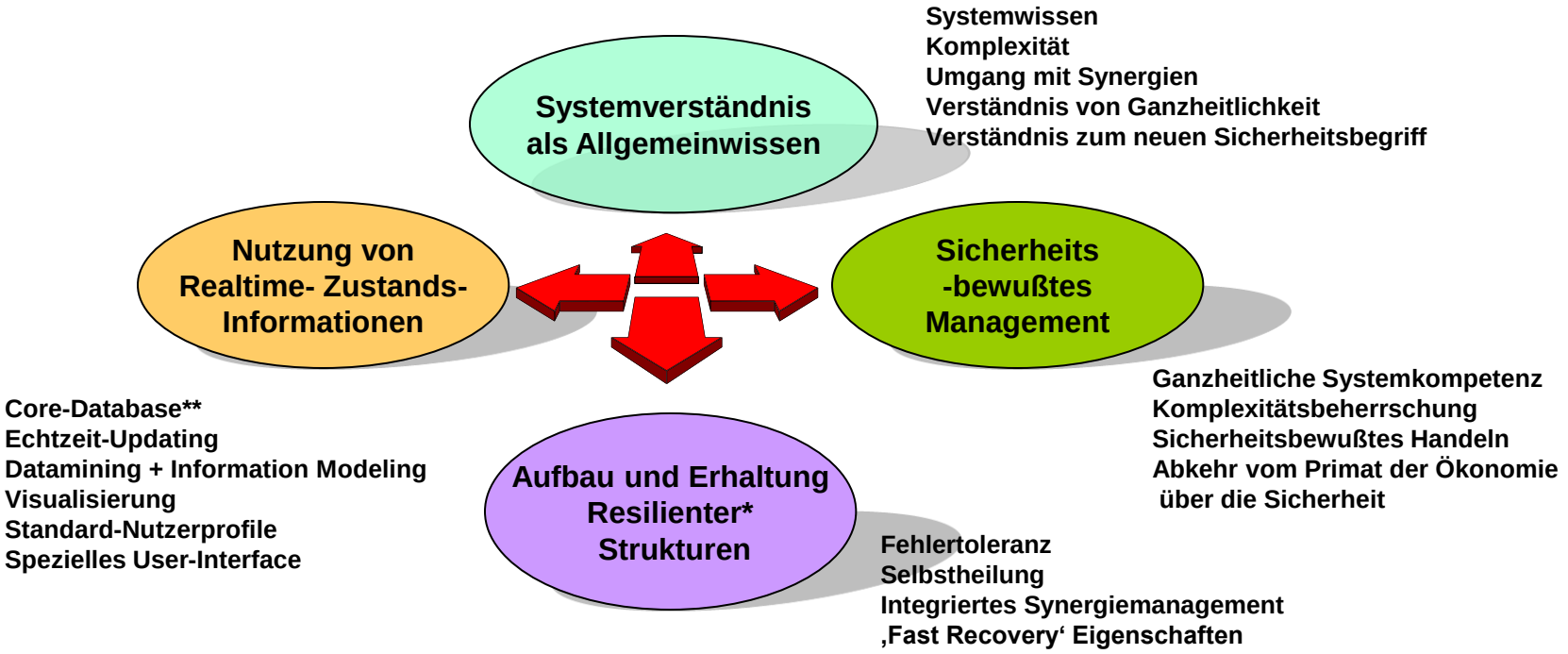
„Sicherheit bezeichnet den Zustand der dauerhaften Verfügbarkeit von Strukturen, Objekten, Systemen und Regeln in der Gesellschaft, die für ein gefahrenfreies Leben ohne Beeinträchtigungen erforderlich sind.“

Dieser Zustand der Sicherheit muß durch ständige Anstrengungen immer wieder neu garantiert werden.



Eine Lösung für das aktuelle Dilemma

Die Anstrengungen, um die dauerhafte Verfügbarkeit von Strukturen, Objekten, Systemen und Regeln in unserer Gesellschaft immer wieder neu zu garantieren, bedeuten unsere ständige Einflußnahme auf folgende Bereiche:



*Resilienz: Fähigkeit von Systemen, bei einem Teilausfall nicht vollständig zu versagen ** Core-Database: Kerndatenbank mit **allen** Informationen zu einem System einschließlich des ganzheitlichen, eigenschaftenbezogenen Wirkgefüges („komplexe Funktionalität")

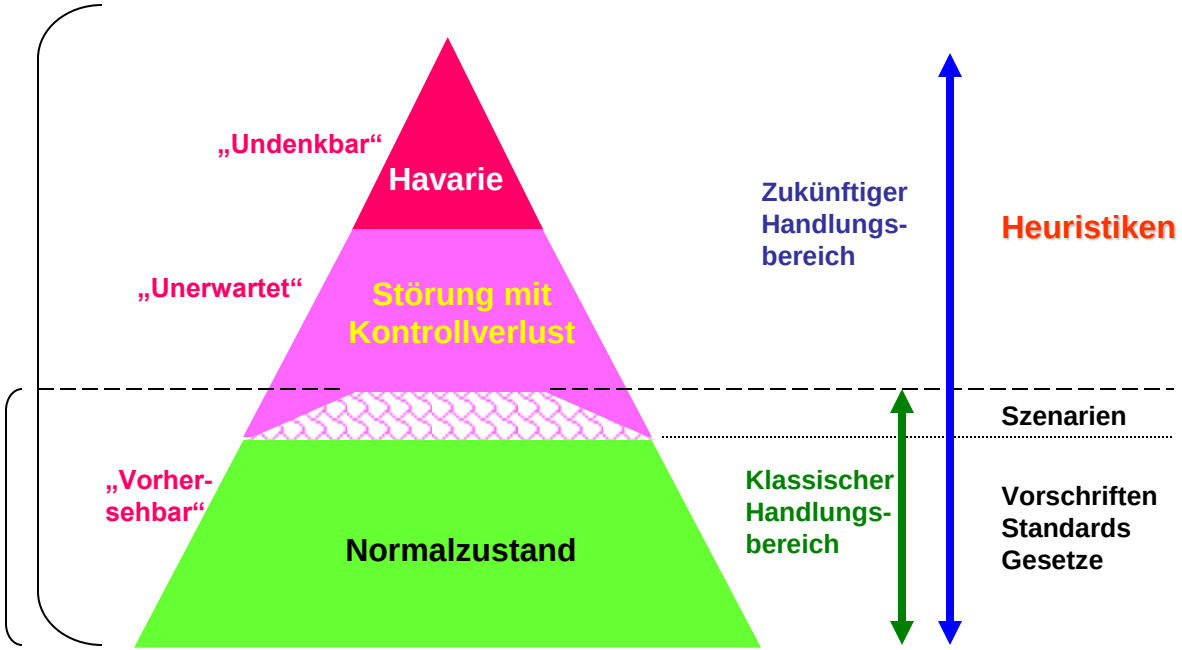
Dilemma 2 : Eine falsche Sicherheitsphilosophie

Ganzheitliche Sicherheits-Philosophie:

- Betrachtung und Behandlung vorhersehbarer Ereignisse + Nutzen von Wissen über Problemlösungsmöglichkeiten außerhalb der ‚Normalität'

Bisherige Sicherheits-Philosophie:

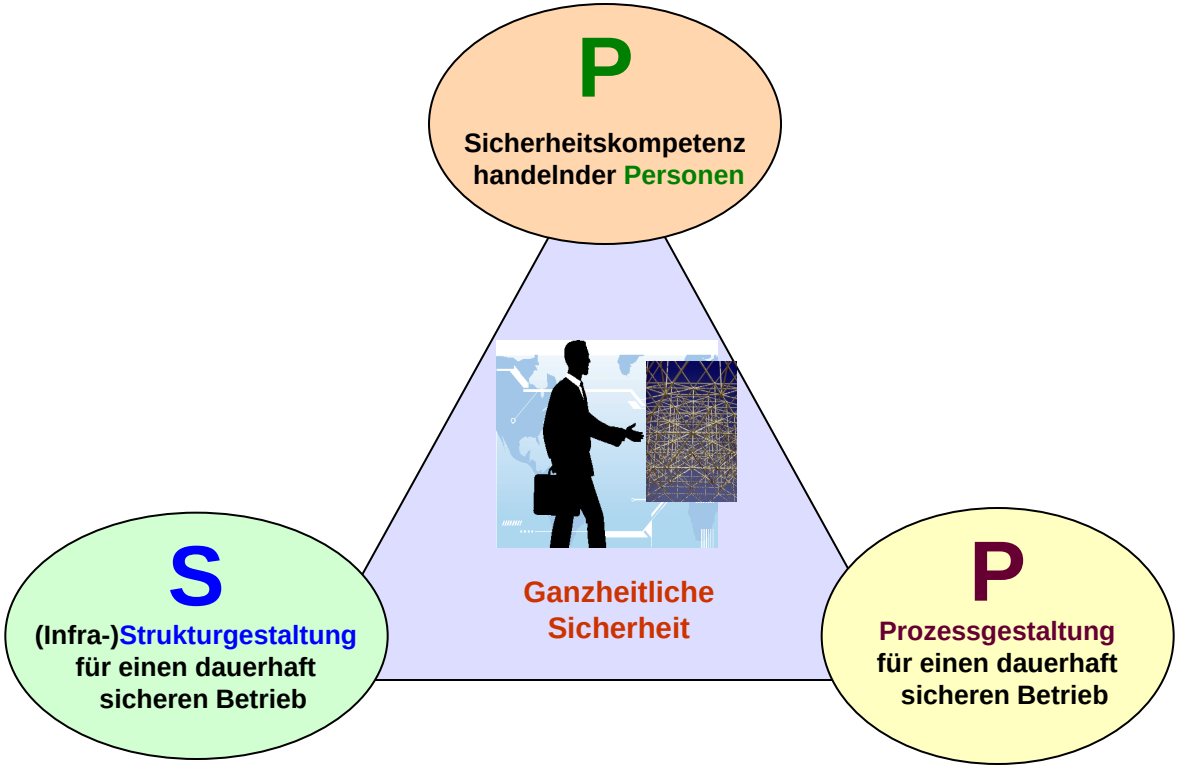
Betrachtung und Behandlung vorhersehbarer Ereignisse und Abweichungen



Im Zeitalter ständig steigender Komplexität in der Gesellschaft, können die bisherigen Handlungs-Grenzen zum Unerwarteten und Undenkbaren nicht mehr akzeptiert werden!

Dilemma 3: Die übersehenen Zusammenhänge

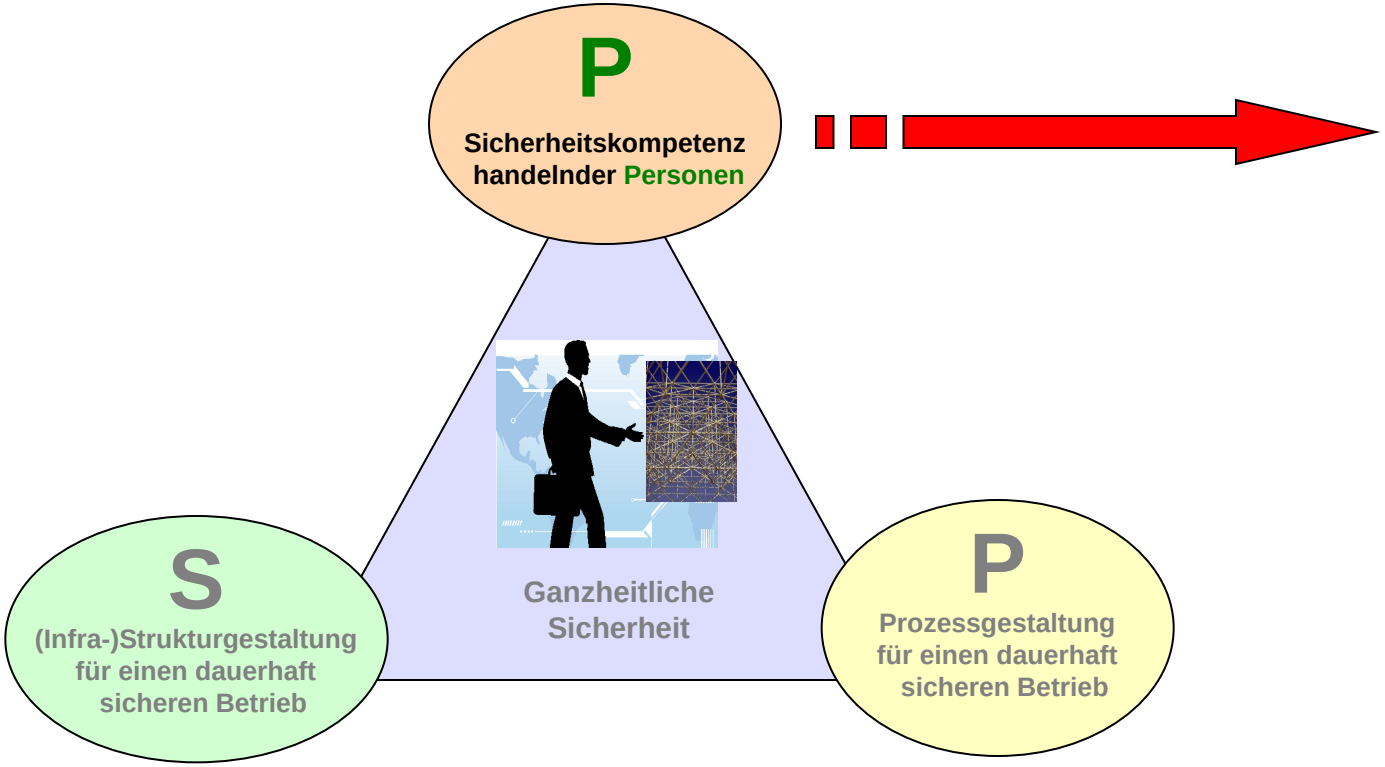
Ohne Beachtung des synergetischen PSP-Wirkgefüges* ist jede Sicherheitsmaßnahme wirkungslos:



*Als **synergetisches Wirkgefüge** bezeichnet man Zusammenhänge, bei denen die Gesamt-Systemfunktion sich signifikant über ihre gegenseitigen Synergien definiert: Fehlt ein Teil, gibt es keine Synergieeffekte **und damit keine Systemfunktion mehr!***

Dilemma 3: Die übersehenen Zusammenhänge

Die größten Defizite gibt es gegenwärtig bei der Sicherheitskompetenz handelnder Personen!

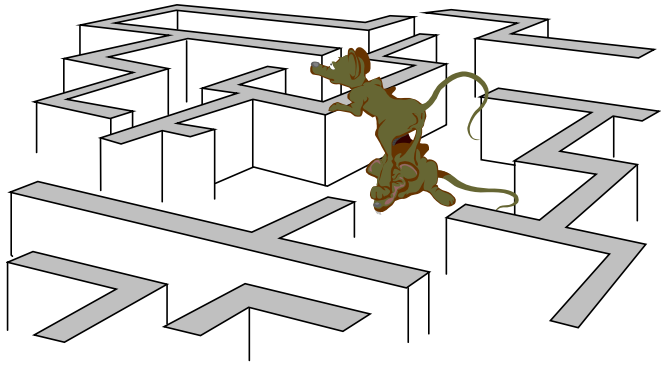


Sicherheitskompetenz handelnder Personen

Entscheidend, aber oftmals nicht ausreichend beachtet:
Der ‚Wirkungsfaktor Mensch‘

Es ist dringend erforderlich, praxisbezogene Handlungsmuster zur Erhöhung der Beherrschbarkeit komplexer Systeme und ihrer Sicherheit zu finden!

Oder einfacher ausgedrückt:
Wie kann man erreichen, daß auch dann, wenn wir in einer immer komplexeren Umgebung leben müssen, in Zukunft der Überblick, und damit unsere Handlungsfähigkeit in allen Situationen erhalten bleibt…



Sicherheitskompetenz handelnder Personen

Der notwendige Lernprozeß in der Gesellschaft:

Um in Zukunft den Überblick, und damit die Handlungsfähigkeit zu behalten, müssen wir schnellstens lernen, umzugehen mit:

- **Systemen** →Was sind eigentlich Systeme? Was muß man wissen um mit ihnen umgehen zu können?.
- **Komplexität** → Was sind komplexe Systeme? Beherrschung von Komplexität
- **Ganzheitlicher Sicherheit** →Der erweiterte Sicherheitsbegriff →Sicherheitsbewußtes Handeln
- **Neuen Handlungsmustern der Beteiligten** → Was sind Kompetenzen ? →Wieso sprechen wir von *System*kompetenz? Was tun wir, wenn der Kontrollverlust so groß ist, daß Regeln und Vorschriften nicht mehr greifen?

Der Begriff Systemkompetenz

Kompetenz bedeutet nach bisheriger Auffassung:

Fundiertes Fachwissen

Handlungsfähigkeit in der Praxis

…und bezieht sich auf die Fähigkeiten aller (auch juristischer!) Personen beim Tätigsein in der Gesellschaft

Der Begriff Systemkompetenz

Systemkompetenz bedeutet daher :

Fundiertes Fachwissen
über Erscheinungsformen und Kennzeichen von Systemen

Handlungsfähigkeit
bei der Steuerung und beim Eingreifen in Systeme

…und bezieht sich gleichfalls auf die Fähigkeiten handelnder Personen oder Einrichtungen (juristischer Personen)

Der Begriff ‚Ganzheitliche Systemkompetenz'

Ganzheitliche Systemkompetenz, wie sie in komplexen Umgebungen benötigt wird, bedeutet unter Beachtung des PSP-Wirkgefüges:

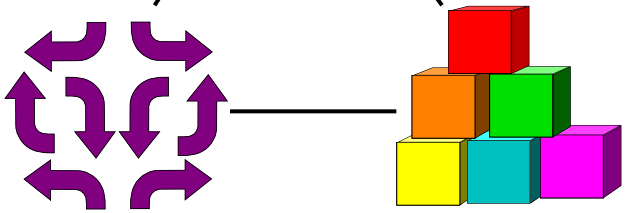
Fundiertes Fachwissen über Erscheinungsformen und Kennzeichen komplexer Systeme

Handlungsfähigkeit bei der Steuerung und beim Eingreifen in komplexe Systeme

Ideeller Teil

Konzeptioneller Teil

Gestaltung und Nutzung nachhaltiger Prozesse in komplexer Systemumgebung



Gestaltung, Betrieb und Erhalt nachhaltiger Strukturen in komplexer Systemumgebung

Fachwissen und Handlungsfähigkeit sind nur wirksam in einer beherrschbaren Systemumgebung, Kompetenz muß deshalb auch konzeptionelle Elemente umfassen

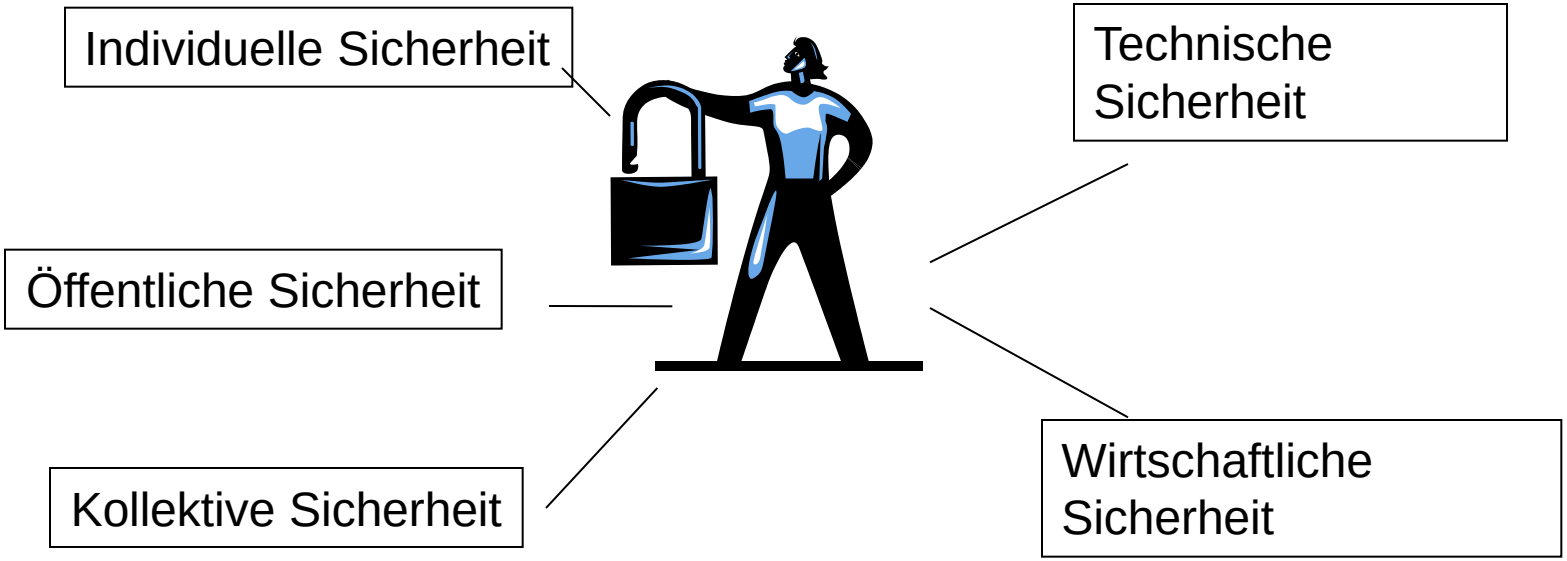
Ganzheitliches Sicherheitsmanagement

Erst Ganzheitliche Systemkompetenz befähigt heute zu Ganzheitlichem Sicherheits-Management:

- **Genaue Kenntnis der funktionellen Zusammenhänge im betrachteten System oder Objekt**
- **Genaue Kenntnis aller, auch der für die aktuelle Funktion nicht genutzten Eigenschaften der Systemkomponenten (‚Hidden Function' Prinzip)**
- **Kenntnisse über das ganzheitliche, eigenschaftenbezogene PSP-Wirkgefüge**
- **Erweitertes Risk-Management mit heuristischen Handlungsmustern bei Havarien, Störfällen, und Sabotage, zur Begrenzung von deren Auswirkungen**
- **Vorsorge gegen vermeidbare Unfälle / Notfälle / Störfälle durch Standard-Nutzungsprofile und ihre intelligente Auswertung**
- **Nutzung von Core-Databases mit Echtzeit-Updating und Information Modeling für die notwendigen Realtime-Zustands-Information**
- **Regelmäßige Sicherheitsmanagement-Validierung**

Sicherheitsbewußtes Handeln

Sicherheitsbewußtes Handeln muß sich auf alle Aspekte der Sicherheit beziehen:



In der heutigen komplexen Umwelt ist die Voraussetzung für sicherheitsbewußtes Handeln die Ganzheitliche Systemkompetenz der agierenden Personen.

Sicherheitsbewußtes Handeln

Sicherheitsbewußtes Handeln benötigt alle Teile der ganzheitlichen Systemkompetenz:

Fachwissen zu sicherheitsrelevanten Elementen und Eigenschaften von Systemen

Handlungskompetenz bei der Sicherung der Systemfunktionen

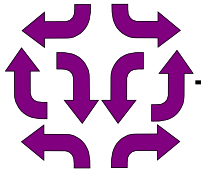
Fundiertes Fachwissen über Erscheinungsformen und Kennzeichen komplexer dynamischer Systeme

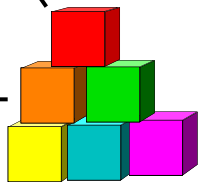
Handlungskompetenz bei der Steuerung und beim Eingreifen in komplexe Systeme

Ideelle Kompetenz

Konzeptionelle Kompetenz

Gestaltung und Nutzung nachhaltiger Prozesse in komplexer Systemumgebung





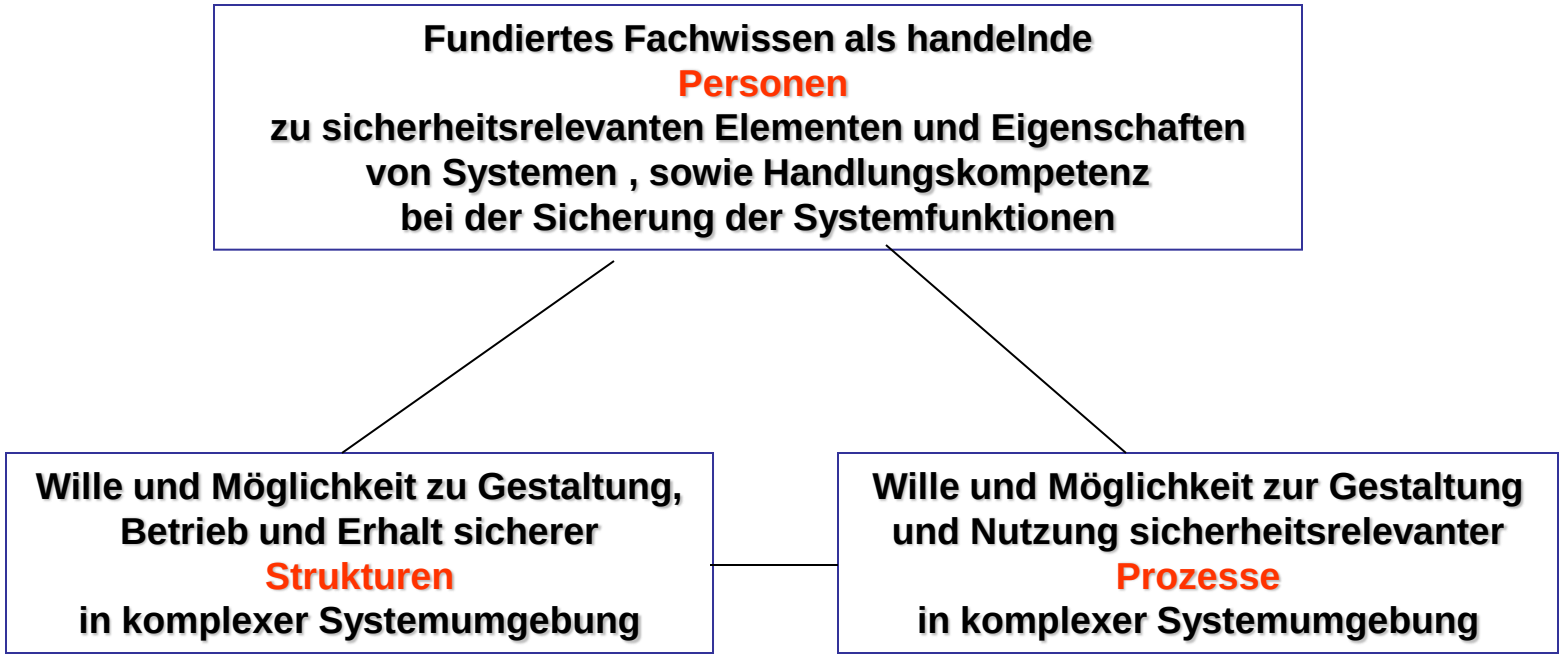
Gestaltung, Betrieb und Erhalt nachhaltiger Strukturen in komplexer Systemumgebung

Gestaltung und Nutzung sicherheitsrelevanter Prozesse in komplexer Systemumgebung

Gestaltung, Betrieb und Erhalt sicherer Strukturen in komplexer Systemumgebung

Sicherheitsbewußtes Handeln

Sicherheitsbewußtes Handeln ist gleichfalls nur unter Beachtung des PSP-Wirkgefüges möglich:



Sicherheitsbewußtes Handeln

Zum Sicherheitsbewußten Handeln gehört:

- **Sicherheitsverantwortliche sollten grundsätzlich zu hohem kognitivem Niveau tendieren. Bei der Besetzung einer solchen Position sollten Ideelle und konzeptionelle Systemkompetenz und die Fähigkeiten zur Komplexitäts-reduzierung abgeprüft werden.**

- **Wo sicherheitsbewußtes Handeln unabdingbar ist (Technik!) muß sicherge-stellt werden, daß die Arbeitsumgebung die zur Ausübung ganzheitlicher Systemkompetenz notwendigen Informationen liefern kann und Regeln aktiv gestaltet werden können.**

- **Führungskräfte benötigen Fähigkeiten zur sicherheitsorientierten Führung von Spezialisten und Teams**

Sicherheitsbewußtes Handeln

Sicherheitsbewußtes Handeln von Führungskräften bedeutet *Einbeziehung ihrer Teams* und entsprechende Anleitung ihrer Mitarbeiter.

Fehler, die dabei gemacht werden, sind vor allem.

1. **Falsche Zielsetzung**
2. **Unvernetzte Situationsanalyse**
3. **Einseitige Schwerpunktbildung**
4. **Unbeachtete Nebenwirkungen**
5. **Tendenz zur Übersteuerung**
6. **Tendenz zu autoritärem Verhalten**

Nach: Prof. Dietrich Dörner . Prof. Frederic Vester: Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Problemlösendes Handeln

Zur Lösung von Problemen gibt es zwei Handlungsstrategien:

Rationales Handeln:

Der Mensch trifft seine Entscheidungen über das Abwägen jedes möglichen Ergebnisses, dessen Wahrscheinlichkeit und relativen Nutzen

Heuristisch determiniertes Handeln:

Der Mensch trifft in einem **unsicheren Handlungsraum** seine Entscheidungen intuitiv und heuristisch determiniert, weil die Wahrscheinlichkeit von Ergebnissen und deren Nutzen nicht genau definiert werden können.

Ein unsicherer Handlungsraum bedeutet:

- Mangelnder Überblick zur Situation,
- Unsicherheit zu Vorgehensweise und Lösungsmöglichkeiten,
- noch unklare, oder sich ständig ändernde Ziele
- Fehlendes Know How und unzureichende andere Ressourcen
- Extremer Zeitdruck bezüglich der Lösung
- Regeln und Vorschriften sind nicht verfügbar oder kontraproduktiv

Heuristisch determiniertes Handeln

- **Heuristiken** sind Strategien, die das Finden von Lösungen zu Problemen ermöglichen sollen, zu denen kein mit Sicherheit zum Erfolg führender Algorithmus bekannt ist

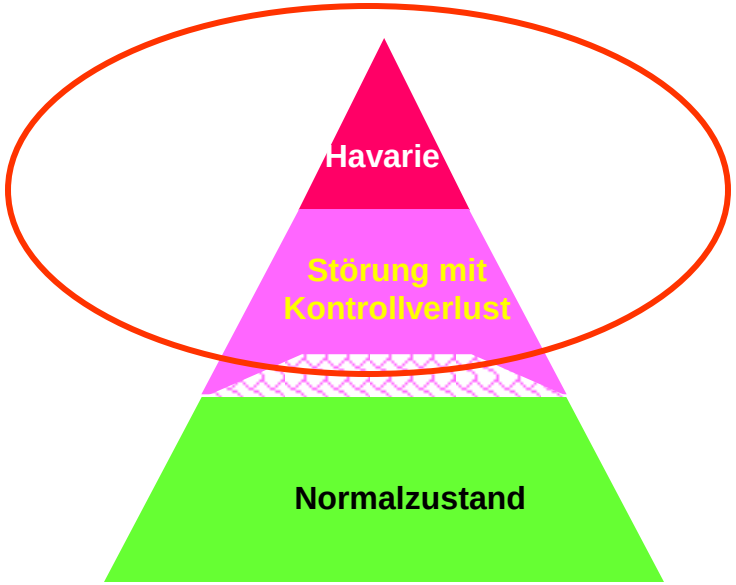
- **Verallgemeinerte Methodische Hinweise** aus erfolgreichen Problemlösungen, im einfachsten Falle „Daumen-“ oder „Faustregeln“, dienen der kognitiven Entlastung

- **Heuristisch determiniertes Handeln** ermöglicht es, schnell und auf der Grundlage bruchstückhaften Wissens, Schlussfolgerungen zu ziehen, die – obwohl nicht logisch zwingend – in vielen Kontexten angemessen und nützlich sind

Heuristiken im Security Management

Der ‚klassische' Handlungsbereich im Security Management umfaßt den Normalzustand und das Verhalten im Bereich von Störungen mit Kontrollverlust.

Gerät die Situation außer Kontrolle, helfen nur Heuristiken als Handlungsbasis!



Heuristiken im Security Management

Beim Auftreten von sicherheitsrelevanten Ereignissen kommen vorgedachte Szenarien, Programme, Vorschriften oder Standards schnell an ihre Wirkungs-Grenzen.
Damit trotzdem noch Handlungsspielraum bleibt, müssen die involvierten Personen heuristische Handlungsmuster beherrschen, welche Kreativität zum aktiven Handeln auch außerhalb der funktionellen Normalität ermöglichen.

Heuristiken im Security Management

Handeln, auch außerhalb der funktionellen Normalität ?

Kompetenz und Effektivität eines Problemlösers hängen erheblich davon ab, wie weit er über Methoden und mentale Strukturen verfügt, die invariant auf umfangreiche Klassen von Aufgabenstellungen seines Berufes anwendbar sind. Sie gewährleisten schnellen Durchblick und ermöglichen die Umsetzung seines Erfahrungs- und Wissensschatzes.
Umfaßt dieser Erfahrungs- und Wissensschatz außerdem Ganzheitliche Systemkompetenz und Verallgemeinerte Methodische Hinweise aus erfolgreichen Problemlösungen, ist ein erfolgreiches Handeln auch außerhalb der funktionellen Normalität möglich.

Heuristiken im Security Management

Verallgemeinerte Methodische Hinweise aus erfolgreichen Problemlösungen haben vielfältige Formen:

- **Einfache „Daumen-“ oder „Faustregeln“, aus langjährigen Erfahrungen mit einer Klasse von Problemen. (Beispiel: Bauernregeln)**

- **Nach heuristischen Verfahren ‚abgehobene‘ Methodiken zu bestimmten Problemlösungsprozessen (Beispiel: Ingenieur-Heuristik)**

- **Allgemeine Denkstrukturen und –Modelle zu Problemlösungsprozessen = „Scaling Laws“**

Heuristiken im Security Management

Wichtig:

Bei der Anwendung heuristischer Strategien ist ein ausreichendes Wissen über ihre Kontextbezogenheit notwendig!

Im falschen Kontext angewandt, können sie zu systematischen Fehleinschätzungen (bias) führen!

Heuristisch Determiniertes Handeln unterscheidet sich grundsätzlich vom „Einfach Drauflos-Werkeln“ mit ungenügendem Wissen und im Vertrauen auf : „Es wird schon gut gehen“!

Heuristiken im Security Management

Beispiel: Faustregeln zum heuristisch determinierten Handeln im Security Management (1)

Berücksichtige folgende Hauptregeln:*

- **Denk nach bevor zu handelst.**
- **Mach Dir Deine Ziele klar.**
- **Beschaffe Dir viele Informationen über eine Sache bevor du handelst.**
- **Lerne aus Deinen Fehlern.**
- **Handele nicht in Ärger und Wut.**
- **Frage um Rat.**

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Einige Fehler beim Sicherheitsbewußtes Handeln (1)*

- Damit alles viel schneller läuft, nehmen wir Hypothesen als Wahrheiten und stellen diese dann nicht mehr in Frage.
- Wir lassen uns gerne durch neue Informationen von dem akutem Problem ablenken.
- Wir lösen Probleme die wir lösen können, statt diejenigen die wir lösen sollen.
- Wir scheuen die Reflektion eigenen Verhaltens und damit die Konfrontation mit der eigenen Unzulänglichkeit.
- Immer wieder regulieren wir den Zustand und nicht den Prozess. Dadurch erreichen wir, dass das Eigenverhalten des Systems und die Steuerungseingriffe sich überlagern: „Die Steuerung „schießt über“.

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Beispiel: Faustregeln zum heuristisch determinierten Handeln im Security Management (2)

- **Das Handeln muss auf die jeweiligen Kontexte eingestellt werden und diese müssen ständig angepasst werden, weil sie sich immer wandeln.**
- **Wir müssen jeweils ein genaues Bild der sich ändernden Bedingungen behalten und wir dürfen nicht glauben, dass das Bild, welches wir einmal für eine Situation gewonnen haben, endgültig ist.**
- **„Es bleibt alles im Fluss“…..**
- **Es gibt Regeln, aber diese haben immer nur lokale Bedeutung.**

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Beispiel: Faustregeln zum heuristisch determinierten Handeln im Security Management (3)*

- **Wir sollten das System, in dem das Problem auftritt, untersuchen, *und nicht nur das Problem selbst.***
- **Entscheidend ist nicht nur, *was mit wem* verbunden ist, sondern *wie es damit* verbunden ist.**
- **Überlebensfähige Systeme sind *funktions-* nicht *produktorientiert*. Produkte ändern sich rasch, Funktionen aber bleiben lange erhalten**
- **Das Bewusstsein der „guten Absicht“ rechtfertigt meist die fragwürdigsten Mittel. Den Leuten mit den *guten Absichten fehlt das schlechte Gewissen, welches ihre Mitmenschen mit den schlechten Absichten haben* ……!**

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Beispiel: Faustregeln zum heuristisch determinierten Handeln im Security Management (4)*

- **Die Gefahr des Groupthink ist die Tendenz einer Gruppe von Fachleuten, sich selbst zu bestätigen, daß sie alles richtig und gut machen. Kritik in der Gruppe wird durch Kollektivdruck unterbunden.**

- **Eine Analyse des Beizubehaltenden ist die einzige Chance, implizite Probleme explizit zu machen und so zu verhindern, dass die Lösung des einen Problems zur Folge hat, dass drei Neue dafür auftreten.**

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Einige Fehler beim Sicherheitsbewußten Handeln (2)*

- Wenn wir ein Komplexziel nicht in Teilziele aufteilen, führt dies zu einem Verhalten, das wir *Reparaturdienstverhalten* nennen: Wir lösen gerade nur die Probleme die momentan anstehen (Erste Hilfe!)
- *Reparaturdienstverhalten* kann dazu führen, dass wir falsche Probleme lösen, da wir die Beziehungen der Probleme untereinander nicht kennen und schon gar nicht den Bezug der Teilprobleme zu dem unklar verbleibenden Gesamtproblem.
- Wir lösen nicht die Probleme die wir lösen sollen, sondern die, die wir lösen können.
- Wir operieren mit dem gesamten System, als wäre es eine Ansammlung unabhängiger Teilsysteme.
- Wir betrachten das System nicht als System, sondern als ein Haufen voneinander unabhängiger Minisysteme.

***Nach: Prof. Dietrich Dörner . Prof. Frederic Vester:** Die Logik des Misslingens - Die Kunst vernetzt zu denken,

Heuristiken im Security Management

Noch in der Forschung befindliche Bereiche, in denen die vorhandenen Methodiken noch weiter vervollkommnet werden müssen, sind:

- **Nach heuristischen Verfahren ‚abgehobene' Methodiken zu bestimmten Problemlösungsprozessen (Beispiel: Ingenieur-Heuristik)**

- **Allgemeine Denkstrukturen und –Modelle zu Problemlösungsprozessen in der fortgeschrittenen Informationsgesellschaft = „Scaling Laws"**

Für diese Arbeiten werden noch Mitstreiter gesucht!!

Fazit

- In unserer ständig komplexer werdenden Welt, muß Sicherheit neu definiert und auf andere Weise garantiert werden, als bisher.
- Dazu ist neues Wissen und neue Handlungskompetenz in allen Bereichen der Gesellschaft erforderlich
- Systemkompetenz und die Fähigkeit zu sicherheitsbewußtem Handeln von Personen gehören dazu
- Es ist nicht mehr möglich, den bisher durch die Begriffe ‚Unvorhersehbarkeit' und ‚Undenkbarkeit' gekennzeichneten Bereich sicherheitsrelevanter Ereignisse, weiterhin vom aktiven Handeln auszugrenzen.
- Heuristisch determiniertes Handeln kann auch in diesen Fällen effiziente Problemlösungen ermöglichen
- Es gibt bereits ausreichend viele Ansätze, um Heuristisch determiniertes Handeln in der Praxis anzuwenden.

Danke für Ihre Aufmerksamkeit !

Dipl.-Ing.
Dieter Skrobotz
Projektentwicklung und -Beratung
Telematik, RFID, Komplexe Systeme

Mobil: +49(0) 171 739 6709
Mailto: dieter@skrobotz.de
Tel.priv:. +49(0)30 6731912