

ICS 13.200; 03.220.40; 47.040; 47.060

## **Security-Modellierungstechnik (SMT) zur gefahrenstufenabhängigen Darstellung und Analyse sicherheitsrelevanter Informationen**

Security Modeling Technique (SMT) for visualizing and analyzing security relevant information based on security levels

Technique de modélisation de sécurité (TMS) pour une visualisation dépendante du degré de danger et une analyse d'informations pertinentes de la sécurité

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:  
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 19 Seiten

Bereich Innovation

# Inhalt

|                                                                                                         | Seite     |
|---------------------------------------------------------------------------------------------------------|-----------|
| <b>Vorwort .....</b>                                                                                    | <b>3</b>  |
| <b>Einleitung.....</b>                                                                                  | <b>4</b>  |
| <b>1 Anwendungsbereich .....</b>                                                                        | <b>5</b>  |
| <b>2 Normative Verweisungen .....</b>                                                                   | <b>5</b>  |
| <b>3 Begriffe .....</b>                                                                                 | <b>5</b>  |
| <b>4 Beschreibung der Security-Modellierungstechnik.....</b>                                            | <b>6</b>  |
| 4.1 Allgemeine Anmerkungen .....                                                                        | 6         |
| 4.2 Modellierung örtlicher Gegebenheiten .....                                                          | 7         |
| 4.2.1 Komponente „Bereich“ .....                                                                        | 7         |
| 4.2.2 Komponente „Schiff“ .....                                                                         | 7         |
| 4.2.3 Komponente „Zugangsbeschränkter Bereich“ .....                                                    | 8         |
| 4.2.4 Komponente „sonstiger Bereich“ .....                                                              | 9         |
| 4.3 Modellierung von Gefahrenstufen .....                                                               | 9         |
| 4.4 Modellierung von Maßnahmen .....                                                                    | 10        |
| 4.4.1 Komponente „Maßnahmen“ .....                                                                      | 10        |
| 4.4.2 Komponente „Ressource“ .....                                                                      | 11        |
| 4.5 Modellierung von Prozessen .....                                                                    | 12        |
| 4.5.1 Komponente „Start“ und „Ende“ .....                                                               | 12        |
| 4.5.2 Komponente „Kontrollfluss“ .....                                                                  | 12        |
| 4.5.3 Beispiel einer Prozess-Modellierung .....                                                         | 13        |
| 4.6 Modellierung von Kommunikation .....                                                                | 13        |
| 4.6.1 Komponente „Kontaktstelle“ .....                                                                  | 13        |
| 4.6.2 Komponente „Kommunikationsfluss“ .....                                                            | 13        |
| 4.6.3 Beispiel einer Kommunikationsmodellierung .....                                                   | 14        |
| 4.7 Modellierung ergänzender Informationen .....                                                        | 14        |
| 4.7.1 Komponente „Hinweis“ .....                                                                        | 14        |
| 4.7.2 Komponente „Verweis“ .....                                                                        | 15        |
| 4.7.3 Komponente „Verbindung“ .....                                                                     | 15        |
| 4.7.4 Komponente „Gruppierung“ .....                                                                    | 15        |
| <b>Anhang A (informativ) Beispiel eines SMT-Modells zur Anwendungsdomäne „Zivile Schifffahrt“ .....</b> | <b>17</b> |
| <b>Literaturhinweise .....</b>                                                                          | <b>19</b> |

## Vorwort

Diese DIN-Spezifikation nach dem PAS-Verfahren beschreibt die Komponenten der Security-Modellierungstechnik (SMT) sowie die Vorgehensweise zur Erstellung von SMT-Modellen. Die SMT unterstützt sicherheitsverantwortliches Personal bei Entscheidungsfindungen während der Umsetzung von Gefahrenstufen und die Erstellung und Prüfung von Security-Maßnahmen durch entsprechende Institutionen.

Verfasser sind:

- Daniel Ley, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)
- Hartmut Adam, Reederei Scandlines mbH
- Karsten Hilbrandt, Verkehrsministerium Mecklenburg-Vorpommern, Hafensicherheitsbehörde (Designated Authority)
- Michael Kalus, Lübecker Hafen-Gesellschaft mbH
- Michael Katzmarzik, Landespolizeiamt Schleswig-Holstein, Dezernat 43: Behörde für Hafenanlagensicherheit (Designated Authority)
- Florian Motz, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)
- Johannes-Stephan Salzig, Landespolizeiamt Schleswig-Holstein, Dezernat 43: Behörde für Hafenanlagensicherheit (Designated Authority)

Die Veröffentlichung der DIN SPEC hat die Abteilung „Entwicklung neuer Arbeitsgebiete“ im DIN (Deutsches Institut für Normung) e. V. betreut. Für den Inhalt dieses Dokumentes sind allein die Verfasser verantwortlich. Für dieses Thema existiert keine Norm.

Die Arbeiten zu dieser Spezifikation wurden gefördert mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) für das Verbundprojekt INFRANORM. Die Arbeiten basieren auf Ergebnissen der BMBF-Verbundprojekte VESPER und VESPER<sup>PLUS</sup>.

DIN Deutsches Institut für Normung e.V.

Entwicklung neuer Arbeitsgebiete (ENA)

10.01.2013

## Einleitung

Seit den Anschlägen des 11. September 2001 werden in unterschiedlichsten Bereichen Methoden und Technologien entwickelt und optimiert, um Security-Standards zu erhöhen und dadurch den Gefahren terroristischer Bedrohungen entgegenzuwirken.

VESPER (Verbesserung der Sicherheit von Personen in der Fährschifffahrt) ist ein Verbundprojekt, welches vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Hightechstrategie der Bundesregierung über die Laufzeit von drei Jahren (2008-2011) gefördert wurde. Eines der Ergebnisse von VESPER ist die Entwicklung der Security-Modellierungstechnik (SMT, Ley & Dalinger, 2010 [1]; Ley & Dalinger, 2011 [2]; Ley et al., 2011 [3]), welche auch weit über die Projektgrenzen hinaus auf breite Zustimmung stieß. Während der Untersuchungen in Häfen und an Bord von Schiffen wurden fünf Datenkategorien identifiziert, welche für eine Situationsanalyse und somit das Situationsbewusstsein des verantwortlichen Security-Personals zur Umsetzung bzw. Änderung von Gefahrenstufen grundlegend sind:

- **Örtliche Gegebenheiten**, wie die Infrastruktur;
- **Gefahrenstufen** zur situationsabhängigen Auswahl von Maßnahmen;
- **Maßnahmen** zur Sicherung von Security relevanten Bereichen;
- **Prozesse** zur strukturierten Abwicklung von Security-Maßnahmen und
- **Kommunikation** zwischen beteiligten Personen und Institutionen.

Zur Ist-Zustand-Erfassung und Soll-Zustand-Ableitung im Rahmen einer Analyse und Umgestaltung, aber auch im betrieblichen Alltag zur Risikoanalyse sowie zur Erstellung und Prüfung von Security-Plänen sind Methoden vorhanden, welche einzelne Datenkategorien berücksichtigen. Eine Methode, welche alle fünf Datenkategorien integriert dargestellt und eine Analyse ermöglicht, konnte im Projekt VESPER nicht identifiziert werden. Hierdurch entstehen Herausforderungen bezüglich Security-Analysen, aber vor allem auch im betrieblichen Alltag, in dem eine zeitnahe und vollständige Umsetzung relevanter Maßnahmen in sicherheitskritischen Situationen notwendig ist.

Ziel der SMT ist es, über eine integrierte Repräsentation aller fünf Datenkategorien verantwortliches Security-Personal bei Entscheidungsfindungen zur Umsetzung bzw. Änderung von Gefahrenstufen, aber auch die Prüfung adäquater und vollständiger Maßnahmen durch entsprechende Institutionen zu unterstützen.

## 1 Anwendungsbereich

Die Anzahl an Modellierungskomponenten wurde bewusst gering gehalten, um eine einfache SMT-Modell-Erstellung für verantwortliches Security-Personal zu gewährleisten. Dies und eine grundsätzliche domänenunabhängige Anwendbarkeit der Methode erlauben einen Einsatz der SMT nicht nur im Bereich der zivilen Schifffahrt, sondern auch darüber hinaus. In Frage kommen dabei hauptsächlich Arbeitsdomänen, in denen Informationen gefahrenstufenabhängig festgelegt und verarbeitet werden müssen.

Die Komponenten der SMT sowie die Vorgehensweise zur Erstellung von SMT-Modellen werden in der vorliegenden DIN-Spezifikation beschrieben. Die nach dieser DIN-Spezifikation erstellten Modelle sollen Anwendung finden für folgende Aufgaben:

- Schnelles Auffinden und Zuordnen gefahrenstufenabhängiger Informationen;
- Unterstützung der Entscheidungsfindung von verantwortlichem Security-Personal bei der Umsetzung von gefahrenstufenabhängigen Security-Maßnahmen;
- Unterstützung des Situationsbewusstseins bezüglich umzusetzender und bereits umgesetzter Maßnahmen;
- Überprüfung der Vollständigkeit vorhandener Security-Maßnahmen.

Die Anwendung erstellter SMT-Modelle kann entweder systembasiert (bspw. im SMT-Editor) oder papierbasiert in Form eines Ausdrucks erfolgen.

## 2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

SOLAS, XI-2 (2004): International Convention for the Safety of Life at Sea. Kapitel XI-2: Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ISPS-Code)

## 3 Begriffe

Für die Anwendung dieses Dokuments gilt der folgende Begriff.

### 3.1

#### **Security**

Abwehr von Gefahren, die aus vorsätzlichem Handeln (einschließlich Handlungen mit krimineller Zielrichtung) zum Nachteil von Personen und/oder ganzen Bevölkerungsgruppen, Einrichtungen und/oder Sachen entstehen

[nach DIN SPEC 91282]

## 4 Beschreibung der Security-Modellierungstechnik

### 4.1 Allgemeine Anmerkungen

Das Konzept der SMT setzt sich aus fünf Modellierungs-Ebenen zusammen, welche integriert in einem Modell dargestellt werden (können):

- 1) Örtliche Gegebenheiten;
- 2) Gefahrenstufen;
- 3) Maßnahmen;
- 4) Prozesse und
- 5) Kommunikation.

Zusätzlich gibt es Modellierungs-Komponenten, die nicht ausschließlich einer dieser Ebenen zugeordnet werden können:

- 6) Ergänzende Informationen.

Um zunächst einen ersten Eindruck zu erhalten, ist in Bild 1 ein exemplarisches SMT-Modell dargestellt. Ein derartiges Modell (hier das eines Fährschiffes mit den Schnittstellen zu landseitigen Hafenbereichen) bietet dem verantwortlichen Security-Personal eine Übersicht über relevante Informationen der fünf Modellierungs-Ebenen.

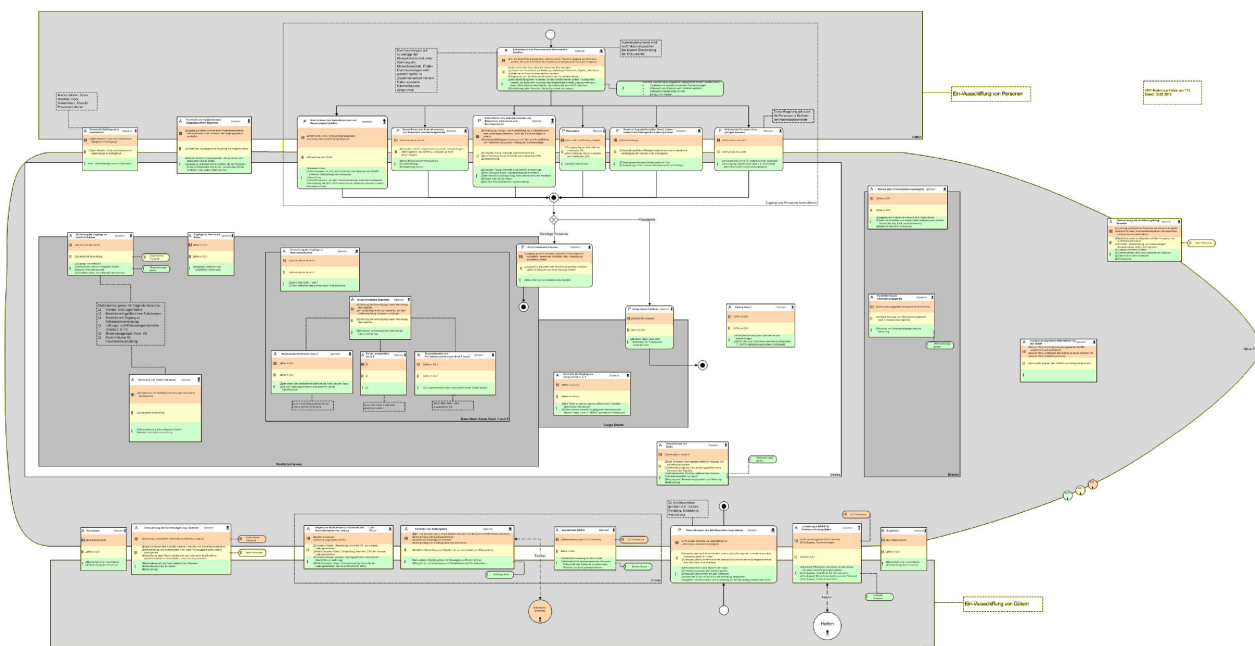


**Bild 1 — Beispiel eines SMT-Modells**

Die einzelnen Komponenten der Modellierungsebenen (1 bis 5, entsprechend obiger Auflistung) sowie die ergänzenden Informationen, aus denen ein derartiges Modell erstellt wird, werden in den nachfolgenden Kapiteln beschrieben. Die Reihenfolge entspricht dabei der empfohlenen Reihenfolge der Modellierung. Es ist grundsätzlich bei der Modellierung darauf zu achten, dass eingetragene Texte immer vollständig zu sehen sind und nicht durch Überlappen von Komponenten verdeckt oder durch zu kleine Komponenten abgeschnitten sind.