Toward Intelligent Decision Support for Security Staff: Evaluation of an Interactive Resource Management System Based on a CMDP Model

Jutta Hild\textsuperscript{a}, Jonathan Ott\textsuperscript{b}, Elisabeth Peinsipp-Byma\textsuperscript{a}
\textsuperscript{a}Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB), Fraunhoferstr. 1, 76131 Karlsruhe, Germany;
\textsuperscript{b}Dept. of Stochastics, KIT, 76131 Karlsruhe, Germany

ABSTRACT

The officer-in-charge deploying the security personnel to protect a large infrastructure meets a complex decision problem if multiple threats have to be handled simultaneously: Limited surveillance resources have to be optimally allocated to the many affected sectors in order to provide the safest threat state for the infrastructure as a whole over time. This contribution presents an interactive resource management system providing decision support for optimally deploying surveillance resources. For this purpose, the user interface displays a risk map of the infrastructure’s current threat situation together with a recommendation of the currently optimal resource allocation. Thereby, the resource allocation recommendation is obtained by solving a CMDP model of an infrastructure’s global threat situation. An evaluation of the CMDP-based decision support shows that displaying both resource allocation recommendation and risk map enables the participants to handle threat scenarios more cost-saving, and additionally causes less workload and higher acceptance among the participants.

Keywords: Resource management system, security management, surveillance task, decision support, mathematical model, continuous-time Markov decision process (CMDP), visualization, evaluation

1. INTRODUCTION

Triggered by suitcase bombs placed in two regional trains in Germany in 2006, the discussion about how security staffs could be supported in detecting and avoiding severe damage to people and property had been reinforced. This incident showed once more that human security guards are not able to detect every threat. On the other hand, there are still no technical systems capable to keep a whole infrastructure fully automated under surveillance. Thus, human security guards are still indispensable. To contribute to an improvement of infrastructure protection we aim to provide some intelligent decision support for security personnel – in fact, for the officer-in-charge of a security staff –, in order to assist the handling of complex threat situations.

Starting point of our work is the state-of-the-art protection of traffic infrastructures as illustrated in Figure 1 using the example of a regional airport. The central role is occupied by the officer-in-charge. To keep the infrastructure in a secure and safe state he strives for optimally deploying the typically limited human resources at the infrastructure’s different sectors. The surveillance and protection task is accomplished in an iterative exploration process (black lettering), preceded by a setup process (blue lettering). During operation, the officer-in-charge gets information (information acquisition) about the infrastructure’s current threat situation both from reports of security guards doing their rounds and from security staff members analyzing video streams on the surveillance screen or in archive. The threat information constitutes the officer’s situation assessment. According to the situation assessment, the decision for an optimal response – more precisely for an optimal resource allocation – is made based on service regulations and emergency instructions.

The service regulations and emergency instructions are established during the setup process, based on extensive risk analysis and legal requirements. Typically, they only provide rules for how to handle the various types of threats, e. g. “in the case of fire, call 112” or “in case of a sensor alarm, first check the sensor, then ...”. Thus, if the number of current threats is less or equal the number of security staff members, resource allocation is not a problem. In this case, the officer-in-charge is able to assign at least one security guard to every threatened sector to handle the threat according to the service regulations.
However, the crucial case of multi-threat scenarios, where the number of threatened sectors is bigger than the number of security guards, is not covered by the service regulations. So, in the latter case the officer-in-charge has to improvise in allocating the security staff members to sectors. Obviously, this practice is potentially prone to errors as it is a complex task to understand and correctly assess the current threat situation of the infrastructure as a whole in a multi-threat scenario: The impact of several alarms has to be regarded not only for the sectors where the alarms took place, but also for depending sectors. Therefore, it is difficult to (quickly) build some sort of “risk map” of the infrastructure just in one’s mind, especially while working under both time and psychological pressure. It is evident that there is need for some kind of reliable information base to support the resource allocation decision.

![Figure 1: State-of-the-art decision support for infrastructure protection](image1)

![Figure 2: CMDP-based decision support](image2)
In consequence, our objective was to create a software tool supporting the officer-in-charge in two ways. First, the tool should enhance the officer’s situation awareness of the infrastructure’s current threat situation. For this purpose, the tool should provide a global view on the current threat situation enabling the officer-in-charge to do the situation assessment both quickly and correctly even in multi-threat scenarios. Secondly, the tool should support the officer’s decision about how to optimally handle the current threat situation even in multi-threat scenarios. For this purpose, it should provide a resource allocation recommendation, which unambiguously represents the optimal deployment of the limited human security resources for any threat situation.

Figure 2 shows the resulting system layout. In addition to the state-of-the-art decision support means shown in Figure 1, our system provides a user interface visualizing a global view on the current threat situation by means of a risk map of the regional airport. The risk map allows capturing the current threat situation at a glance thus enhancing situation awareness. To represent a sector’s current threat level, the risk map uses a range of five colours from red, representing severe threat, to dark green, representing no threat at all. Additionally, to support the resource allocation decision, the resource allocation recommendation is displayed within the selected sectors, using a stick-figure symbol to recommend inspection rounds, or a video camera symbol to recommend video stream analysis, respectively. The integrated representation of the complete decision relevant information in the user interface is described in more detail in section 3.

In addition to the user interface of the decision support tool, Figure shows the underlying method from which both risk map and resource allocation recommendation are derived. To model an infrastructure’s global threat situation, a continuous-time Markov decision process (CMDP) is used. The risk map can be derived directly from the CMDP model. To get the recommendation for any threat situation, the CMDP has to be solved, as the result of the solution directly delivers the corresponding resource allocation recommendations. The underlying CMDP model is described in section 2. Subsection 2.1 describes how an infrastructure’s global threat situation is modelled; subsection 2.2 outlines how the calculation of the resource allocation recommendation is done.

In addition to finding out whether and how an infrastructure’s threat situation could be modelled by a CMDP, we were also interested to examine whether the additionally provided CMDP-based decision support – risk map and resource allocation recommendation – could be really valuable for the officer-in-charge. Therefore, an evaluation was carried out. The experimental design and the results are described in section 4.

2. MATHEMATICAL MODELLING OF AN INFRASTRUCTURE’S GLOBAL THREAT SITUATION

As already mentioned, both risk map and resource allocation recommendation are directly derived from the CMDP model. The following subsection provides a formal specification of the CMDP modeling an infrastructure’s global threat situation, from which the risk map is derived. Subsection 2.2 outlines the solution of the CMDP, resulting in the set of resource allocation recommendations for every defined threat state of the infrastructure. Additional details can be found in several other publications.

2.1 Modeling an infrastructure’s global threat situation using a continuous-time Markov decision process (CMDP)

We are going to model the dynamics of threat of the infrastructure, i.e. the infrastructure’s global threat situation, as a parameterization of a continuous-time Markov decision process (CMDP). A CMDP is described by the finite state space $S$, the finite action space $A$, the restriction set $D \subseteq S \times A$, where $D(s) = \{a \in A : (s,a) \in D\}$ are the actions which are admissible in state $s$, the transition rates $\lambda = (\lambda(s,a))_{(s,a) \in D}$, the transition probabilities $P = (P_{st}^{a})_{(s,a) \in D, t \leq S}$, the cost rates $X = (C(s,a))_{(s,a) \in D}$ and the discount factor $\alpha > 0$. When the current state of the system is $s$, then the officer-in-charge chooses some action $a \in D(s)$. Depending on $a$, the system remains in $s$ for an exponentially distributed random time with rate $\lambda(s,a)$. After that time, the system jumps to the state $s'$ with probability $P_{st}^{a}$, and the officer-in-charge has to choose the subsequent action from the set $D(s')$, and so on. As long as the state is $s$ and action $a$ is carried out, the officer-in-charge has to pay the cost $C(s,a)$ per unit time.
Denoting \((X_t)_{t \geq 0}\) the state process and \((A_t)_{t \geq 0}\) the action process, the total discounted cost over an infinite time horizon is given by \(\int_0^\infty e^{-\alpha t} C(X_t, A_t) dt\). Now, we restrict ourselves to decision rules, i.e., functions \(\mu : S \to A\) such that \(\mu(s) \in D(s)\) for all \(s \in S\). The set of all decision rules is denoted by \(F\). This set includes for any threat state of the infrastructure its corresponding resource allocation recommendation. Each decision rule \(\mu \in F\) induces a probability measure \(P^\mu\) on the underlying measurable space. We denote the expectation taken with respect to \(\mu\) by \(E^\mu\). Given the initial state \(x_0 \in S\), we are searching for a \(\mu^* \in F\), called optimal decision rule (the optimal resource allocation recommendation), such that

\[
E^\mu \left[ \int_0^\infty e^{-\alpha t} C(X_t, A_t) dt \right] \bigg| X_0 = x_0 = \inf_{\mu \in F} E^\mu \left[ \int_0^\infty e^{-\alpha t} C(X_t, A_t) dt \right] \bigg| X_0 = x_0 = v^* (x_0),
\]

i.e., such that the expected total discounted cost is minimized for \(\mu^*\). A decision rule \(\mu^*\) satisfying (1) exists since we assume that the state space and the action space are finite. Moreover, the optimal value function \(v^*\) is the unique fixed point of the so-called Bellman equation

\[
v(s) = \min_{a \in D(s)} \frac{C(s, a) + \lambda(s, a) \sum_{s', \sigma} p_{\sigma s a} v^*(s')}{\lambda(s, a) + \alpha}, \quad s \in S, \tag{2}
\]

where \(v : S \to \mathbb{R}\). From the Bellman equation (2), we might extract an optimal decision rule by choosing \(\mu^*(s) \in D(s)\) such that \(\mu^*(s)\) minimizes the right-hand side of (2) for all \(s \in S\). Methods for deriving an optimal decision rule include, e.g., Howard’s policy improvement algorithm and linear programming. Note that \(\mu^*\) is optimal in the much broader class of so-called history-dependent randomized policies. For the details, we refer to.

Now, we shortly describe the model of the surveillance and protection task. Further explanations, details and numerical examples are available in\(^1,2,3\). The infrastructure itself is given by the set of sectors \(\Sigma\). A sector might be some physical part of the infrastructure such as a building or a room, or it might be some abstract part of the infrastructure such as the electric power supply or the water supply. When threat changes in some sector at some point in time, then threat might change in some of the other sectors of the infrastructure, too, since sectors might be in the neighborhood of the first sector or because they are functionally dependent of the first. Such dependencies are modeled by the adjacency matrix \(N \in [0, 1]^{\Sigma \times \Sigma}\), where \(N(\sigma, \sigma^*) = 1\) if \(\sigma^*\) is dependent on \(\sigma\) and \(N(\sigma, \sigma^*) = 0\) if \(\sigma^*\) does not depend on \(\sigma\). We define \(N(\sigma, \sigma^*) = 0\) for all \(\sigma^* \in \Sigma\). Note that the dependencies might not be symmetric since one sector is functionally dependent of another but not vice versa. Threat of each sector is measured by its current threat level which is supposed to take values from the finite set \(G = \{0, 1, \ldots, g_{\text{max}}\}\). The state space is then defined as \(S = G^\Sigma\) so that each sector is assigned with one threat level. In this manner, each state of the surveillance task can easily be depicted as a risk map.

Events that may have an impact on the threat situation of the infrastructure are modeled by threat events. Let \(E(\sigma)\) denote the set of threat events that may occur in \(\sigma\). Each \(e \in E(\sigma)\) is equipped with the following features:

- When the current threat level of \(\sigma\) is \(g\), then \(e\) will occur after an exponentially distributed random time at rate \(\lambda_e(g)\).
- When \(e\) occurs and the threat level of \(\sigma\) is \(g\) right before the occurrence of \(e\), then the subsequent threat level of \(\sigma\) is given by \(\Psi_e(g)\).
When $e$ occurs, the threat level of some dependent sector $\sigma^*$, i.e., \( N(\sigma, \sigma^*) = 1 \), with threat level $g$ right before the occurrence of $e$ changes to $\psi_e(g)$. When $e$ occurs, the threat levels of the sectors which do not depend on $\sigma$ remain unchanged.

When $e$ occurs, it costs the fixed amount $C_e \geq 0$.

We assume that the sets of threat events are disjoint from each other, i.e., \( E(\sigma) \cap E(\sigma^*) = \emptyset \) for $\sigma \neq \sigma^*$, so that each threat event is uniquely associated with a sector.

Next, we are going to model the actions which the security staff is able to perform. We assume that the officer-in-charge is allowed to assign one elementary action from the finite set $A_0$ to every sector. So, the action space is $A = A_0^\Sigma$. Each elementary action $a_0 \in A_0$ is endowed with the following features:

- It takes an exponentially distributed random time with rate $\lambda_{a_0}(\sigma)$ to accomplish $a_0$ in $\sigma$.
- When $a_0$ is accomplished in $\sigma$ and $g$ is the threat level of $\sigma$ right before the completion of $a_0$, the threat level of $\sigma$ will be $g'$ with probability $\Phi_{a_0}(g, g', g^*)$.
- Depending on $g$ and the result $g'$ of $a_0$ which is completed in $\sigma$, the threat level of a sector $\sigma^*$ which is dependent on $\sigma$ will change from $g'$ right before the completion of $a_0$ in $\sigma$ to $\varphi_{a_0}(g, g', g^*)$. Sectors which are not dependent from $\sigma$ will not be affected by the completion of $a_0$ in $\sigma$.
- As long as $a_0$ is being executed in $\sigma$, the officer-in-charge incurs the cost $c_{a_0} \geq 0$ per unit time.

We assume that there is a special elementary action $0 \in A_0$ whose interpretation is “do nothing.” That is to say, executing 0 in some sector $\sigma$ will leave the sector to the mercy of the threat events or to the completion of elementary actions in sectors from which the first is dependent. In detail, we define $\lambda_0(\sigma) = 0$, $c_0 = 0$, $\Phi_{0}(g, g', g^*) = 1$ and $\varphi_0(g, g', g^*) = g^*$ for all $\sigma \in \Sigma$, $g, g' \in G$, so that formally, 0 will never be accomplished, will never change the state, and does not cost anything.

For the following, we make the assumption that all random times stemming from the occurrences of threat events and the completions of elementary actions are independent.

From the above definitions, the CMDP is built in the following manner. We assume that the number of the security staff is given by some number $r \leq |M|$, where $|M|$ denotes the number of elements of the set $M$. Moreover, we assume that each elementary action apart from 0 requires exactly one member of the security staff, and the elementary action 0 does not require any human resources. Therefore, the restriction set of the surveillance task is given by

$$D(s) = \left\{ a \in A : \sum_{\sigma \in \Sigma} \left[ 1 - \delta_{ba(\sigma)} \right] \leq r, s \in S \right\},$$

where $\delta$ is the Kronecker delta. By independence of the occurrence of threat events and the completion of elementary actions, the transition rates are given by

$$\lambda(s,a) = \sum_{\sigma \in \Sigma} \lambda_{a0}(\sigma) + \sum_{e \in E(\sigma)} \lambda_e(\sigma), (s,a) \in D.$$
The Bellman equation to determine an optimal decision rule for the surveillance may then be written as

$$v(s) = \min_{a \in D(s)} \frac{1}{\lambda(s, a)} \left[ C(s, a) + \sum_{\sigma \in \Sigma} \lambda(a(\sigma)) \sum_{g \in G} \Phi_{a(\sigma)}(g, s) v(\zeta_s^g(s)) + \sum_{\sigma \in \Sigma} \lambda(s(\sigma)) v(\zeta_s^e(s)) \right], \quad s \in S,$$

where the subsequent state of $S$ after elementary action $a(\sigma)$ is accomplished in $\sigma$ and the result of $a(\sigma)$ is $g'$ in $\sigma$ is denoted by $\zeta_s^g(s)$, and the subsequent state of $S$ when the threat event $e$ occurred is denoted by $\zeta_s^e(s)$.

In order to provide decision support, one could consider other optimization criteria apart from minimizing the expected total discounted cost. One approach might be to minimize a certain risk measure of the total discounted cost. A meaningful risk measure might be the so-called average value-at-risk at level $\tau \in (0, 1)$, for the definition see, e.g.\(^5\). The respective optimization criterion would be to minimize the average of the $\tau \cdot 100\%$ most expensive possible outcomes of the discounted total costs of all scenarios, which means that only the most expensive scenarios are considered. This approach would lead to the prevention of the most devastating scenarios. This problem has been solved in\(^2\), and it turns out that this approach is not suitable in order to provide reasonable decision support for practitioners for two reasons:

1. Solving the respective problem is much more numerically complex than solving the expected total discounted cost criterion.
2. An optimal policy according to the average value-at-risk criterion might not be time-consistent, i.e., when the system is in the same state at different points in time, then the optimal action might not be the same. This property might be confusing for the person in charge.

Therefore, the expected total discounted cost is used as the optimization criterion for the surveillance and protection task.

### 2.2 Obtain the resource allocation recommendation: calculation of the optimal decision rule

As presented in the previous section, an optimal decision rule – the resource allocation recommendation – can be computed by solving the Bellman equation (2) and by choosing minimizing actions of the right-hand side of (2) as the respective optimal action. Due to the curse of dimensionality, this approach has its limits. Note that the state space increases exponentially with the number of sectors and the number of actions increases at least polynomially. Therefore, the linear program to solve the Bellman equation cannot be solved for surveillance tasks with five threat levels for rather small infrastructures consisting of six sectors. Thus, approximation techniques such as simulation methods\(^6\), aggregation methods\(^7\), and linear programming methods\(^8\), or heuristics are needed in order to obtain suboptimal solutions for the surveillance task. In this section, we briefly present a heuristics which might be used to approximately solve the surveillance task presented in the preceding section. Detailed descriptions of the following algorithms can be found in\(^1^2\), and the mathematical background can be found in\(^8^2\).

The idea of the heuristics is to split up the infrastructure into all of its subinfrastructures of some given size $m \geq r$ so that the entire available security staff of size $r$ can be assigned to these subinfrastructures. The number $m$ must not be chosen too large as the corresponding surveillance tasks might not be computable for subinfrastructures of size $m$ within reasonable time. The data for the surveillance tasks of the subinfrastructures are given by the restriction of the data of the underlying infrastructure given in the previous section. With help of a suitably defined real-valued function on the (restricted) state space for the surveillance tasks of the subinfrastructures, the algorithm chooses some subinfrastructure which approximately benefits the most from assigning the security staff to it according to the current overall state of the underlying infrastructure. This real-valued function is called the index. Indices find use in so-called resource allocation problems where a limited number of resources have to be assigned to given projects in order to minimize the cost of the projects altogether. Examples include the so-called multi-armed bandit\(^9\), where an index exists which induces an optimal decision rule by working on the project with maximal index, or the so-called restless bandit\(^1^0\), where there is an index which induces some very good heuristics by working on those projects having the largest indices. In our case, each

$$C(s, a) = \sum_{a(\sigma)} C_{a(\sigma)} + \sum_{e \in E(\sigma)} \lambda_e(s(\sigma)) C_e, \quad (s, a) \in D.$$
subinfrastructure might be regarded as a single project and the entire security staff is the only resource. The algorithm picks the subinfrastructure whose index depending on the current state is currently the largest. Then the elementary actions which are optimal for this subinfrastructure are assigned to the respective sectors of the underlying infrastructure of interest. All further sectors are assigned with the passive elementary action \( 0 \). Several errors are made since dependencies between subinfrastructures are not considered and since the index itself is only an approximation of the benefit.

Numerical examples have shown that this heuristics provides promising results\(^{2,3}\). Furthermore, the decision rules induced by this heuristics are not counterintuitive in the sense that the security staff is assigned to implausible sectors. Therefore, the above heuristics can be used as a solution method for the surveillance task in order to provide reasonable decision support for resource allocation.

This approach works well as long as there is some \( m \geq r \) such that all surveillance tasks of the subinfrastructures are computable. But the index might be used in order to determine suboptimal actions in case \( m < r \). Then, one might choose the number \( m \) arbitrarily so that all surveillance tasks of the subinfrastructures of size \( m \) are computable. For some given state of the underlying infrastructure, one might compute the indices for the subinfrastructures and choose the subinfrastructure with maximal index. The elementary actions which are optimal for this subinfrastructure are assigned to the underlying infrastructure. Now, at least \( r - m \) persons of the security staff are left to be assigned to the infrastructure. Therefore, one might next choose the subinfrastructure with second largest index and assign the elementary actions which are optimal to the underlying infrastructure where the elementary actions from the first step are kept if the same sector is considered in the subinfrastructure with second largest index. If the subinfrastructure with second largest index has more free sectors than staff is available which can be assigned to the infrastructure, ties have to be broken in a considerable manner, e.g., by considering the sectors in decreasing order of their monetary values. In this manner, one might go through all subinfrastructures in decreasing order of their current indices until the entire security staff is assigned to the underlying infrastructure or until all subinfrastructures have been considered.

### 3. VISUAL REPRESENTATION OF THE CMDP-BASED DECISION SUPPORT

To make the information about an infrastructure’s current threat state described in its CMDP model usable for decision support, it has to be appropriately represented to the officer-in-charge. This section describes the user interface of the decision support tool.

Figure 3 shows the user interface using the example of the underlying infrastructure of the evaluation, the Fraunhofer IOSB (see section 4). It displays the complete exploration process as it is shown in Figure 2. The information acquisition is depicted in the window top left. It shows the history of events, both threat events (preceded by a red highlighted “E” for “Event”) and response actions which have already been finished (preceded by a green highlighted “A” for “Action”). When an action has been finished the corresponding event “E” is tallied by a green tick (see the warning in the first line). The response actions are executed using the window on the right. The number of response actions which can take place simultaneously at any point in time is in this example limited to two. They selection of an action for a certain sector is done by clicking on the corresponding button, whereby the camera symbol means activation of video analysis and the stick-figure symbol means activation of doing round. The currently selected response actions are highlighted in green (in the example doing rounds in sector “First Floor” and in sector “Garage”).

The decision support to enhance both the commander’s situation assessment and decision is displayed in the window bottom left. The decision relevant information represented provides in total five different information types:

1. **Sketch of infrastructure as abstracted layout of its sectors (light grey lines)**. This information is static. It represents the set of sectors \( \Sigma \) (see subsection 2.1, p. 4) arranged as a picture of the infrastructure’s topology.

2. **Value of every sector in TEURO**, displayed in the very sector. This information is also static. It represents the fixed amount \( C_\sigma \geq 0 \) of the event \( e = \text{destruction} \) which has to be paid in case of the destruction (i.e. rebuilding needed) of a sector.

3. **Dependencies between sectors**. This information is also static, as it represents the adjacency matrix \( N \in \{0,1\}^{\Sigma \times \Sigma} \), where \( N(\sigma, \sigma^+)=1 \) if \( \sigma^+ \) is dependent on \( \sigma \) and \( N(\sigma, \sigma^+)=0 \) if \( \sigma^+ \) does not depend on \( \sigma \).
In the example of Figure 3, \( N \in \{0, 1\}^{S \times \Sigma} \), is symmetrical: In the sketch, two sectors sharing a boundary line depend on each other symmetrically.

4. **Risk map of the infrastructure.** It represents the infrastructure’s current threat situation, which is defined to be an element of the state space defined as \( S = G^G \). \( G = \{0, 1, \ldots, g_{\text{max}}\} \) is the set of threat levels. The current threat level of a sector is represented by its color (see legend right above). As already mentioned in the introduction, the colors used to represent different threat levels symbolize sort of intuitive “traffic light code” ranging from red for severe threat situation over orange, yellow, and light green to dark green for no threat at all. This information is dynamic as the risk map changes according to the occurring events (displayed in the information acquisition window top centre-left).

5. **Recommendation for resource allocation.** While information 1 to 4 are directly derived from the CMDP model parameters, information 5 represents the result of the solution of the CMDP model, the optimal decision rule. It is pre-calculated in the setup phase (see Figure 2) and then put into the database of the decision support system to be available during operation. Therefore, it is, in fact, static information. Of course, as it represents the currently optimal resource allocation it changes according to the current threat state. So, for the officer-in-charge it appears as dynamically changing information. The recommendation is represented by icons placed within the respective sector. In the example of Figure 3, the current recommendation suggests the response action “doing round” for the sectors “First Floor” and “Garage”. In this example, the officer-in-charge has taken over the recommendation. Recommendation of “video analysis” is depicted using the same camera symbol as in the response selection window on the right.

All five information types are considered to contribute to optimally decide on the resource allocation. However, the conspicuousness of their representation differs according to their relevance for the decision. In the simplest case, the officer-in-charge should be able to rely upon the recommendation and simply follow it. The conspicuousness of the display of the icons is ensured by their size. If the officer does not want to follow the recommendation, the risk map provides a basis for the resource allocation decision. The conspicuousness of the display of the risk map is ensured by the intuitive color coding as well as by the size of the sectors. Information 2 (value of every sector) is displayed in a relatively unobtrusive way, as it is already contained in the calculation of the risk map and the resource allocation recommendation.

4. **EVALUATION**

To examine the potential benefits of the CMDP-based decision support, below abbreviated by “CMDP-DS”, a pilot study was conducted with 20 participants, 16 students and 4 experts (security guards). Core of the pilot study was a test task simulating the work task of “surveillance and protection of a closed infrastructure/property” in a small computer simulation. As we aimed to have experts (security guards) among the participants, we chose the example of our own research institute, the Fraunhofer IOSB, as the infrastructure to be protected in the test task. The Fraunhofer IOSB deals with security relevant business fields and, in consequence, is protected by a fence and security guards. Thus, it can serve as an appropriate substitute for a critical infrastructure.

4.1 **Test task and evaluation criteria**

In the trial, the participant plays the role of the security officer-in-charge of the property. Using the user interface shown in Figure 3, the participant is told to protect the Fraunhofer IOSB over a certain period of time by appropriate resource allocation of the available two human security resources to the Fraunhofer IOSB’s sectors. The goal the participant shall strive for is do the protection of the Fraunhofer IOSB with the lowest costs possible. The costs are the most important evaluation criterion as they reflect the participant’s performance in the test task. This criterion had been chosen because it corresponds to the optimization criterion of the CMDP optimization process (see subsection 2.1).

The costs of a completed test task are calculated as follows. A completed test task consists of a sequence of threat situations (threat states) of the infrastructure. To calculate the total costs of a completed test task, the cost rate of all passed threat states are summarized. Time is also regarded: Before summarizing, every threat state’s cost rate is multiplied by the length of the time period the infrastructure stayed in this threat state. In more detail, using the notation of section 2, the cost rate \( C(s) \) of a threat state \( s \in S \) can be estimated from the costs of every sector using the formula
\[ C(s) = \sum_{\sigma \in \mathcal{\Sigma}} \lambda_{\text{destruction}(s(\sigma))} \cdot C_{\text{destruction}} \]

(The estimation is possible, because we defined other threat events to cause no or negligibly small costs, the discount factor \( \alpha > 0 \), and the time horizon to be small.) The current costs of every sector are calculated by the product of the occurrence rate \( \lambda_{\text{destruction}} \) for the sector to be destroyed and the value \( C_{\text{destruction}} \) of the sector. Summarizing the costs of all sectors gives the cost rate of a single threat state.

Figure 3: Experimental setup of the evaluation, including CMDP-based decision support “CMDP-DS”.

Figure 4: “State-of-the-Art-like” decision support “STOA-DS”
The total costs of a completed test task can be calculated using the following formula (n number of state changes in the completed task, \( T_k \) point in time of k-th state change, \( T_{k+1} \) point in time of k+1st state change):

\[
c_{\text{total}} = \sum_{k=0}^{n} [C(X_{T_k}) \times (T_{k+1} - T_k)]
\]

In addition to cost calculation for measuring the participants’ performance, two other aspects were investigated in the evaluation. The participant’s perceived workload in performing a test task is rated using the NASA-TLX11. To get some feedback about the acceptance of the CMDP-based decision support, a self-defined questionnaire is used.

### 4.2 Experimental design

To evaluate the potential benefits of CMDP-DS, it is compared to a self-defined “state-of-the-art-like” decision support system, below called “STOA-DS” (STate-Of-the-Art Decision Support, Figure 4). Here, “state-of-the-art” means “not CMDP-based”. In consequence, it provides only the static information types 1 to 3, i.e. sketch, values, and dependencies. This was thought to be a realistic selection in the way that these information types represent part of the general knowledge a today’s officer-in-charge has about the infrastructure he is protecting.

As these information types provide static information only, the dynamics of the changing threat situation is not represented. Thus, the officer-in-charge or the participant has to derive the current threat situation as a “virtual risk map” by combining both the information displayed in the information acquisition window (top centered-left) and the static picture of the STOA-DS. In the same way, the decision for the resource allocation has to be derived. It is likely that the cognitive load using STOA-DS is greater than using CMDP-DS. Therefore, the expectation was that using CMDP-DS, the participants would receive lower costs, would perceive lower workload, and hence, would rate the CMDP-DS with higher acceptance.

For comparing of CMDP-DS and STOA-DS, every participant had to carry out the test task twice, once using CMDP-DS, once using STOA-DS. To avoid that the results are influenced by the order in which the two decision support models are used, one half of the participants started with CMDP-DS, the other half with STOA-DS. To avoid that the participants would remember and repeat their decisions from the first test task in the second one, they got different threat scenarios for the two test tasks. In consequence, the experimental design resulted in four test groups, covering all possible combinations of DS, order, and scenario (see Table 1). To ensure realistic scenarios, they were elaborated in cooperation with the administration manager of the Fraunhofer IOSB who is also responsible for security aspects.

<table>
<thead>
<tr>
<th>Test Group</th>
<th>First Test Task</th>
<th>Second Test Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DS</td>
<td>Scenario</td>
</tr>
<tr>
<td>A1</td>
<td>STOA</td>
<td>I</td>
</tr>
<tr>
<td>A2</td>
<td>STOA</td>
<td>II</td>
</tr>
<tr>
<td>B1</td>
<td>CMDP</td>
<td>I</td>
</tr>
<tr>
<td>B2</td>
<td>CMDP</td>
<td>II</td>
</tr>
</tbody>
</table>

Altogether, the steps of the experiment were as follows:

1. Introduction (Main objective, experimental steps, introduction to experimental setup)
2. Performance of test task with DS No.1 + Training NASA-TLX
   a. Introduction to DS No. 1
   b. Exercise task using DS No.1
   c. Introduction to NASA-TLX, followed by NASA-TLX exercise
4.3 Results

In our evaluation, the CMDP-DS achieved better ratings as the STOA-DS in all three aspects. Particularly, the CMDP-DS allows accomplishing the test task with lower costs. In addition, the experts’ acceptance ratings show the potential of a software-tool for security officers-in-charge providing both a global view of the current threat situation and resource allocation recommendations. In the following, the results of the three aspects – cost (performance), workload and acceptance – are discussed in more detail.

Results of cost determination

The box plots in Figure 5 show the results of the cost determination, separately for the two test scenarios. The separation is necessary, as the baseline values – the minimal expected total discounted cost (the optimization criterion defined in subsection 2.1 by formula (1)) – plotted in the diagram by light grey crosses, differ a lot for the two scenarios. The baseline values were calculated by simulating the performance of a test task while strictly following the resource allocation recommendation.

For both test scenarios there is a slight tendency that the CMDP-DS allows the performance of the test task with lower costs than STOA-DS. Test scenario I shows for CMDP-DS lower values for median, maximum, lower quartile, and minimum than for STOA-DS; the upper quartile is nearly identical. This means that at least some participants could benefit from the additional information provided by the CMDP-DS. Test scenario II shows for CMDP-DS lower values for median, maximum, upper quartile, and lower quartile. Here, the minimum is nearly the same.

Comparison of the calculated baseline values (light grey) and the participants’ values shows remarkable differences for the two test scenarios. For test scenario I, the baseline value is always best compared to both using CMDP-DS and STOA-DS. However, for STOA-DS even the best achieved cost value is considerably higher than the baseline value; for CMDP-DS the difference is only small. This is an objective proof that the CMDP-DS provides valuable support.

For test scenario II the baseline value also delivers very good cost values. However, for test scenario II there were participants – one using STOA-DS, even two using CMDP-DS – who achieved better cost values (see minima for STOA-DS (385 €) and CMDP-DS (324 €) in the box plot diagram). Such an effect had been expected beforehand, for the optimization criterion of the CMDP algorithm is the minimal expected total discounted cost and not the absolute minimum (see section 2.1, formula (1)). Furthermore, the index policy introduced in section 2.2 delivers not the optimal policy but an approximately optimal value for the minimal expected total discounted cost. However, the participants’ cost values for test scenario I show that there are scenarios which without using advanced decision support like CMDP-DS can probably be handled only with costs much higher than the minimum expected total costs. For such scenarios the CMDP-DS provide valuable support.

Results of workload determination

For determination of the cognitive workload a reduced NASA-TLX questionnaire, rating mental demand, performance, effort, and frustration, was used. Physical demand as well as temporal demand seemed not to be relevant for
characterizing the test task. Physical demand is low as performing the test task requires simply the use/utilization of a user interface. Temporal demand is low as well, for the participants were asked to strive for optimizing the costs of a test task, not its time of duration. Thus, we considered the demands of the test task being sufficiently described by determining mental demand.

As most of the participants were using the NASA-TLX for the first time, the assessment was performed without doing the characteristic pairwise comparisons of all subscales\(^1\). Therefore the value of the workload is the unweighted arithmetic mean calculated from the four selected subscales. The result is shown in Figure 6. It shows that out of 20 participants, for eleven there was higher workload using STOA-DS, while for seven there was higher workload using CMDP-DS. In total, the workload is slightly lower for CMDP-DS. Considering the four subscales separately shows slightly lower ratings for all of them for CMDP-DS, too.

Correspondences between cost results and workload results have not been found.

---

**Figure 5:** Results of cost determination

---

**Figure 6:** Workload results for each participant, experts no. 17 to 20; right: arithmetic mean.
Results of acceptance determination

Acceptance was determined both in a quantitative and in a qualitative way. Quantitative rating was used to determine acceptance of the single decision support components (information 1 to 5 described in section 3) sketch of infrastructure (including sectors’ dependencies), values of sectors, risk map, and resource allocation recommendation. The rating was done separately for the CMDP-DS and the STOA-DS right after each test task by a questionnaire using a rating scale ranging from 1 („decision support component was very helpful“) to 9 („decision support component was not helpful at all“). Best rates got the sketch of the infrastructure and the risk map (see Figure 7). Notably, the experts rated these two decision support components very high (not shown in the Figure).

The qualitative assessment of using either the CMDP-DS or the STOA-DS resulted in a clear statement: 19 out of 20 participants, including all four experts would prefer the CMDP-DS for decision support. The answer to the more differentiated question, which decision support components the participants would choose to build a self-defined decision support, is shown in Figure 8. All 20 participants would choose the sketch of the infrastructure and the risk map. Display of the values of the sectors would be chosen by 15 participants, display of the resource allocation recommendation by only ten participants. Comparing the rating of the students and the experts shows an interesting difference. While the students are reluctant in trusting the resource allocation recommendation – they rather prefer the values of the sectors to be displayed – the majority of the experts prefers the recommendation to be displayed. Interestingly, the three experts who would choose the recommendation are the three experts which work as security guards in the Fraunhofer IOSB. One of them told us: “I would really like to have a recommendation which provides me suboptimal minimum average (i.e. expected) cost instead of having to improvise.” Accordingly, the self-defined decision support shown in Figure 9 differs between experts and students.

![Figure 7: Results of the acceptance questionnaire rating the single decision support components by answering the question “How valuable was the decision support component in performing the test task?”](image-url)
The number of surveillance means to protect an infrastructure, both human security guards and sensor equipment, is typically limited. Hence, the officer-in-charge faces a complex decision problem where to allocate the resources, if the number of threatened sectors in the infrastructure is greater than the number of available surveillance means. The introduced resource management system is a step toward providing intelligent decision support for optimal resource allocation. It is based on a global threat model of the infrastructure which models the dynamics of threat of the infrastructure using a continuous-time Markov decision process (CMDP). The core of the CMDP model is the threat state of the infrastructure, which can be easily derived from the model to be visualized as a risk map by the user interface of the resource management system. The risk map provides the officer-in-charge a global view of the infrastructures.
current threat situation. In addition, the solution of the CMDP model provides for every threat state the corresponding optimal resource allocation. Due to the curse of dimensionality, which is inherent in many optimization problems, the provided resource allocation recommendation is only appropriately optimal. In an evaluation has been showed, that even this suboptimal recommendation provides valuable support, for the participants were able to perform a simulated resource allocation scenario with lower costs. In the evaluation, the CDMP-based decision support achieved great acceptance. Particularly, the visualization of the risk map had been appreciated very much by the participants.

However, bringing the basic research results into practical applications is still a long way off. Due to the curse of dimensionality, only infrastructures of small or medium size can be modeled. Thus, to facilitate the modeling of real-sized infrastructures will require various model modifications.

ACKNOWLEDGEMENTS

The underlying projects to this article are funded by the German Federal Ministry of Education and Research under promotional references 03BAPAC1 and 03GEPAC2. The authors are responsible for the content of this article. We thank the b.i.g. Company, who kindly supports us with their knowledge in security management and provided the experts of our evaluation.

REFERENCES
