

Experts-Group Event-Safety 2017

Event Security

A Culture of Responsibility

Technology
Arts Sciences
TH Köln



Experts-Group
Event-Safety

Experts-Group Event-Safety 2017

Technology Arts Sciences TH Köln



Arbeitsgruppe
Veranstaltungssicherheit



Landeshauptstadt



Fachbereich Feuerweh

Arbeitskreis der Sicherheitsingenieure

von ARD.ZDF.medienakademie, ARTE, Bavaria, BR, DeutschlandRadio, DW, HR, IRT, MDR, NDR, RBB, ORF, RB, RBT, RTL, SF, SR, SRG, SSR, Studio Hamburg, SWR, WDR, ZDF

Introduction

Inhalt

	Introduction.....	3
A	Experts-Group-Event Safety	11
A.1	The Security Concept	11
A.2	Public Security and Order.....	13
A.3	Security Terminology	14
A.4	The Event System.....	17
A.5	Needs, Goals, and Behaviours of Visitors.....	20
A.6	The Term „Panic“	23
A.7	The First-Aid Service	25
A.8	The Security Service	27
A.9	Can an Event be Secure?	28
A.10	Prevention as a Basis for Secure Events.....	29
B	Structure of the Security Concept	40
B.1	Description of the Event	42
B.2	Security Objectives	50
B.3	Prevention	53
B.4	Risk Management.....	54
4.1	General	54
4.2	Risk Identification	54
4.3	Risk Analysis.....	54
4.4	Risk Evaluation.....	55
B.5	Unanimity.....	57
5.1	Integration of Public Administration by the Organiser	57
5.2	Definition of the Process.....	57
5.3	Unanimity among the Parties Involved.....	58
C	Methods and Procedures	60
C.1	Risk Management.....	60
1.	Finding, identifying and assessing risks	60
2	List of dangers Checklist.....	63
3	PFAC Procedure.....	66
4	Index Method.....	67
5	Bow-Tie Analysis.....	67
6	Swiss Cheese Model/LOPA (Layer protection analysis)	69
C.2	Assessment of the First-Aid Station	70
C3	Security service	71
C4	Evacuation calculations pedestrian flow	78
D	Literature and References.....	91

Experts-Group-Event Safety

People have been gathering together since the beginning of mankind. The current events we face today have behind them a long history with a variety of cultural origins. But in the end, people come together for special reasons - be they attending a concert, a political speech, a play at the theatre, or an exhibition: One of the core expectations in this form of human behaviour is to stay safe and not get (seriously) harmed at any type of event. This expectation should be the simple goal of any organiser and producer of public or private gatherings all over the world, regardless of the political system or the societal structure of that particular country or continent.

The German Task Force for Event Security (Arbeitsgruppe Veranstaltungssicherheit AGVS) was founded by event managers and stage managers Christian A. Buschoff and Harald Scherer in May 2010, together with the Cologne University of Applied Science, with the aforementioned ideas and intrinsic motivations in mind. Shortly after the first meeting a serious accident at the Loveparade, a techno music open-air festival in Germany's Ruhr region, resulted in the deaths of 21 people.

As many fatal accidents as there were in the 19th century because of theatre fires and the enormous loss of lives they resulted in, the Loveparade disaster brought about a paradigm shift: The work of the task force is now monitored by the event industry and the media due to the public awareness of the topic. Safety is everybody's concern and is on the agenda of every organisation, because it is closely connected with both the idea of human and cultural rights, as well as the freedom of the individual. This is decreed by the UN's Universal Declaration of Human Rights (1948).

In essence the task force focuses its concept for event safety on prevention and risk management. It is a guideline, a manifest, which consolidates the content of a variety of safety analyses and combines proper methodology with experiential knowledge from all parties involved in the planning and holding of events.

There are no intentional specific links to national or local laws or rules and regulations: Nowadays almost every country has its own laws, be they written or unwritten. And even in the absence of such laws, the nearest neighbouring country may have their own approach to the topic. And, last but not least, there are technical standards that should be followed to achieve a proper result.

After more than **seven** years in the field the experts-group's ideas are being used in many events all throughout Europe and have been discussed at international meetings worldwide, from Cincinnati to Moscow to Beijing and to Istanbul. This is the first English translation, which aims to give this manifest a broader audience and to open it up to international review.

During the discussion about content the considerations departed from the search for one method toward a preventative approach of observation. The strict disconnect between the individual areas remains in place, thereby providing a clear and recognisable framework for all parties involved.

The **free publishing** of the instructions allows for the unification of the planning of events, in turn making it more transparent for all involved.

We would be very happy to receive your feedback on this document and if you would discuss it among your peers so that we can incorporate your experience in the future. Cologne, March 2016

Prof. Dr. Alexander Fekete | Christian A. Buschhoff | Harald Scherer

Contact:

Technische Hochschule Köln
Institut für Rettungsingenieurwesen und Gefahrenabwehr IRG
Fakultät 09 – Anlagen, Energie und Maschinensysteme
Betzdorfer Straße 2 | 50679 Köln

Christian A. Buschhoff
christian.buschhoff@th-koeln.de

We thank the EVVC, DTHG and R.A.D for financing the translation .

Introduction

The responsibility for the security of an event and its visitors lies first and foremost with the operator of a venue and the organiser. The laws in the various states regulate this task.

The considerations necessary for this security shall be presented in a security concept in accordance with these regulations.

The Task Force for Event Security accepts this task and provides the work results to the public with this document. To do so, the question of event security was extensively discussed with various interest groups and associations. The results are divided into four chapters:

A	Considerations of Event Security
B	The Security Concept
C	Methods and Procedures
D	Literature and References



Stance

A

Considerations



A Experts-Group-Event Safety

A.1 The Security Concept

The elaboration of a security concept demands an extensive and coordinated alignment between the actors of an event. Before beginning to elaborate, it must be determined whether the manner - i.e. the execution of the event - or the number of visitors require a security concept. If the manner of the event or low number of visitors present NO risk for the visitors, or if a security concept is already in place at the venue for this type of event, a new security concept is not obligatory if such is not required by the responsible authority. This preliminary determination, e.g. as part of a feasibility study, is thus initially subjected to a cohesive overview of the event and its creative process as well as the resulting interfaces. The organiser should name a responsible person (e.g. the process supervisor) who coordinates and moderates these interfaces. Currently this person's qualifications are not often defined, and should be oriented to suit the regulations of the respective states.

The basis for this observation is the right to life and physical safety in accordance with Art. 3 of the Universal Declaration of Human Rights from December 1948. Because a significant amount of creativity and artistic liberty always plays a role in planning and holding an event, these two approaches must be incorporated into the observation and may not just have an effect on the technical procedures of an event. Article 22 of the Convention on Human Rights thus specifies: „Everyone, as a member of society, has a right to social security and is entitled to realisation ... [of] social and cultural rights.“ The following rule of thumb can be applied to the assessment:

In the artist's **workspace**, i.e. concerning the manner of artistic creation, justifiable intervention by the state is almost inconceivable. Such justifiable intervention is more possible in the so-called **scope of efficacy** of the artist, however, because this is where the artist forms a connection with the environment through conveyance to third parties, in which collisions with the basic rights of others' cannot be ruled out.

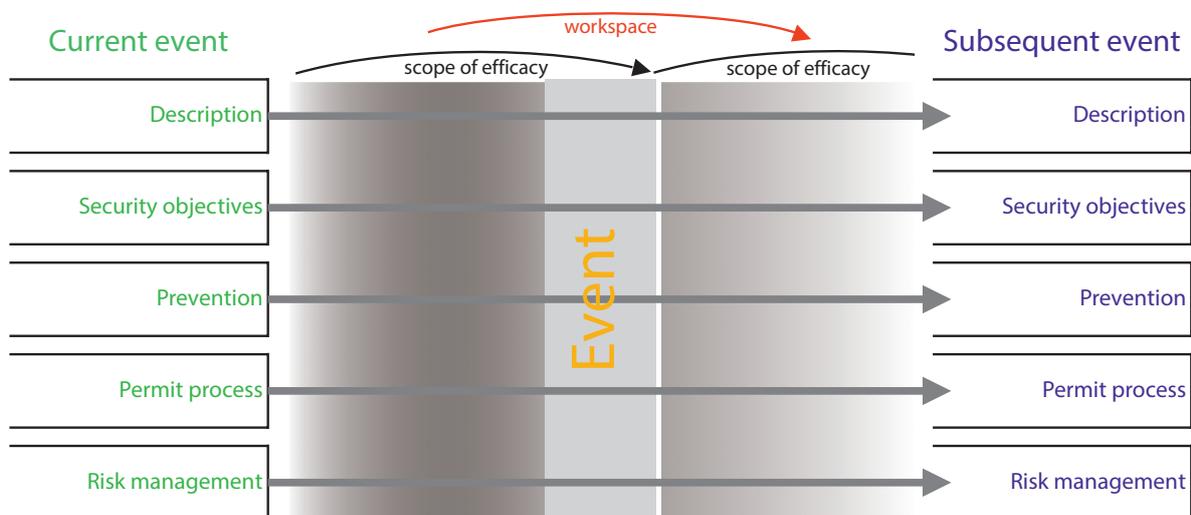


Fig. 1 Workspace and scope of efficacy of an event

The security concept should help ensure that there is no risk to public safety and order during the event. The safety of the employees and people involved must be considered, although this entails a separate observation via the requirements and methods of labour law. The security of the visitors is stipulated by the principle that visiting an event should occur in such a way that the right to life and physical safety is the core focus of all observations, and is not violated. Measures are defined to this end that ensure that visitors are not put at risk by outside factors.

Within the visitors' area, every visitor must always be able to move **freely, without danger, without outside factors, and of their own volition.**

The development of the security concept is a moderating process within the event planning, and should be controlled by one person (the process supervisor). This person lays the foundations of mutual information, alignment, and preliminary work. The objective of their work should be a cohesive understanding among all parties involved of the security-relevant aspects.

The obligation to develop a security concept lies with the operator and is determined by the manner of the event as well as the laws of the respective state. The organiser must actively cooperate with the operator of a venue, the event leader, and the head of the security service.

Should cooperation with the security authorities and organisations (SAO) be required, this cooperation must be actively led by

the operator / organiser. This cooperation process is led by the organiser, who is also responsible for implementing the measures. This results in complex interfaces that must be clearly defined and structurally conducted in such a simple manner that it is clear which person is responsible for the respective measures..

A.2 Public Security and Order

Along with ensuring the basic right to life and physical safety as per Art. 3 of the Convention on Human Rights, the public safety and order at an event must be ensured by the organiser.

The term „public safety“ includes all unwritten laws of which their observance is considered an indispensable requirement of proper human coexistence within a specific area based on the respectively prevailing social and ethical outlooks.

If the expected behaviour of the visitors/actors results in danger or risk, or if the behaviour of the visitors/actors disrupts the public security and order in the organiser's scope of efficacy, the operator/organiser must prohibit, amend, or stop these events in their scope of efficacy (area of influence). To do this the organiser must maintain public security and order, and ensure that their measures do not further disrupt order and thus become the target of police activity.

These sources of risk are based on the behaviour of the visitors/actors and must be separated from the direct environment. The visitor to the event is thus not only considered at risk, but also as a jeopardising aspect that may disrupt public security and order.

The term **danger** is defined as the abstract possibility of harm due to an objectively present source of risk.

A **threat** is the temporal-spatial concurrence of danger and individual (environment, material items) that can result in „harm“ due to its unimpeded advancement. Another definition views a threat as the possibility of harm or impairment of health without specific limits to the extent or likelihood thereof, whereby this term is clearly separate from that of risk.

Risk, on the other hand, is the effect of uncertainties on objectives. Risks are often described in conjunction with the effects of an event and the likelihood of said event occurring.

The organiser must recognise the dangers of an event, analyse the potentially resulting threats, and assess the risk thereof in order to

choose and implement safety measures, and prevent or decrease the dangers' effects.

But what exactly is a „safe event“? How can one define a fundamental observation that entails broad social layers and various event formats? Is the focus of the observation on the size of the events? Are all smaller events thereby safer? The following considerations should provide a basis for the observation that facilitates finding a clear view for these various types of event, despite the broad spectrum of formats..

A.3 Security Terminology

The following observations should place emphasis on how secure an event is and how the safety of the visitors can be guaranteed. Yet before the foundations for a secure event are described in further detail, the security terminology should be observed.

This is bound to a social structure in which the term is constantly changing and cannot be clearly demarcated. Society has an increased expectation of security and the state must/can/ should fulfil this expectation. Security, including objectively and subjectively perceived security, can be influenced by many circumstances. The organiser must address these in cooperation with the security authorities and organisations (SAO). It helps to divide these into four dimensions according to Daase.

Digression:

After World War II military dangers were the main focus in the 1950s and 1960s, and dominated the discourse on security with the beginning of the Cold War. First social/economic problems were integrated into this in the 1970s before ecological threats to security began being discussed as of the mid-1980s due to increasing environmental destruction.

Since the end of the Cold War there has been greater discussion of the protection of human rights and humanitarian security as a task of comprehensive security policy.

This development has resulted, against a backdrop of a constantly changing level of security, in the basic requirement for the demands of a security concept..

1. **Material dimension**

The material dimension of security terminology defines the areas in which dangers are perceived, and the type of security the security policies of states are supposed to provide. This makes it clear that on one side the term is closely associated with actual examples and events from history, and on the other side the expansion of the term has resulted in a change in security policy.

One consequence of this is that the socially demanded degree of security is always aligned with political events, and cannot be observed as a whole. **The basic right to life and physical safety is the top priority at events in the material dimension.** However, an event also has a bearing on economic and ecological fields that may trigger significant changes in society (e.g. international sporting events).

2. **Referential dimension**

The referential dimension of security terminology in the context of event security defines three areas that must be considered in the evaluation:

Individual visitors:

In observing the referential dimension the individual visitor can be subdivided and observed at a more micro level. Not all visitors have the same physical constitution, visitors may get lost or confused, or the enjoyment of intoxicants leads to some visitors not being able to control their actions.

Groups:

It is not uncommon for visitors to come to events in groups and the formation of the group - solely made up of the respective culture and language - should also be observed. However, clearly definable visitors such as children, people with special safety needs, or visitors with limited mobility are also included in the groups.

Neighbours and residents:

The neighbours and residents in the immediate neighbourhood of a venue/in an event's area of influence may have their daily routines significantly restricted by the event. These restrictions or disruptions must also be observed. The group of participants and workers will be extensively observed by the requirements of state labour law. This especially concerns the work performed by the first-aid and security services, as these have direct contact to the visitors.

3. **Spatial dimension**

The spatial dimension encompasses the spatial areas in which the event is held and upon which the organiser has influence. The demarcation is fluid, as small local events may trigger a nationwide and international effect. All three areas - **local, nationwide, and international** - can be even more finely divided and define whether the event is locally based or whether it affects a city district, an entire city, or an administrative district. Events like a European Year of Culture, a large sporting event, or a commemorative holiday/year may have national effects on security and are not uncommonly influenced by international events.

4. **Danger dimension**

The last aspect of the expansion of security terminology concerns the danger dimension, which stipulates how to define the uncertainty that security policy aims to overcome. Because if one is to take seriously Arnold Wolfer's adage that **security is nothing but the lack of insecurity**, then one recognises that security can be conceptualised in many different ways: as defence against threats, as a way to decrease vulnerability, and as a way to reduce risks. With each step the danger becomes less concrete and the requirement for security becomes ever more complex.

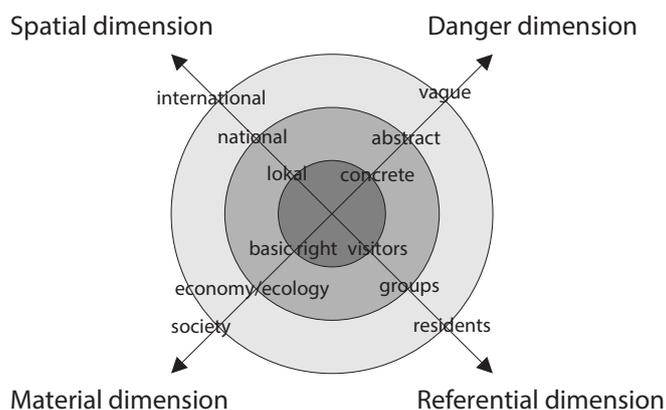


Fig. 2 Dimensions of the expansion of Daase's security terminology

A.4 The Event System

Bezogen auf die Sicherheit einer Veranstaltung werden alle vier With regard to the security of an event all four dimensions (material - referential - spatial - danger) are observed. The development of the security concept primarily answers the question of visitor security and thus moves within various areas of the four dimensions. The overall image of the event can, however, entail a completely independent and opposing observation due to the evaluation of the SAO.

An event is an open, dynamic, and complex system consisting of a large number of elements. These may be very heterogeneously (differently) or very homogeneously (equally) compiled. The individual microscopic states of the elements determine the macroscopic state of the entire system.

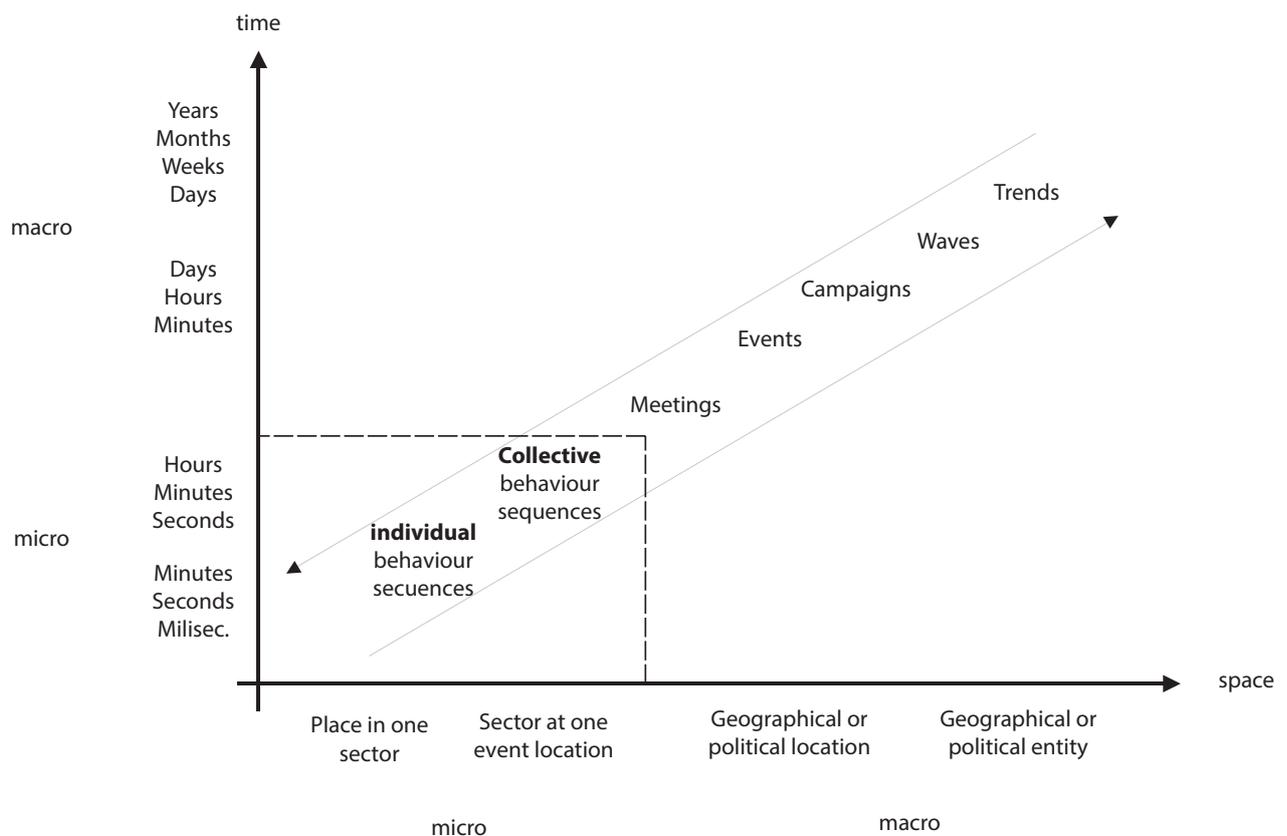


Fig. 3 Micro- and macroscopic conditions of the event

The environment, also called the peripheral system, influences the event and may be a source of danger, e.g. vehicle traffic at a street festival, weather at an outdoor event, public transportation strike, etc. An event can also be a source of danger to the environment in turn: e.g. noise emissions are too high at an open-air concert, rioting guests, piles of rubbish outside the event area, etc.

Viewed from the outside the event system can appear chaotic, and from the inside it is generally organised as there are no (perceived) disruptions within the system itself, and this system is not disrupting its environment.

An observation of the possible threats and disruptions must be performed so that no disruptions affect the system and that none arise from it in turn. However, this requires constant supervision and any necessary adjustment to current events.

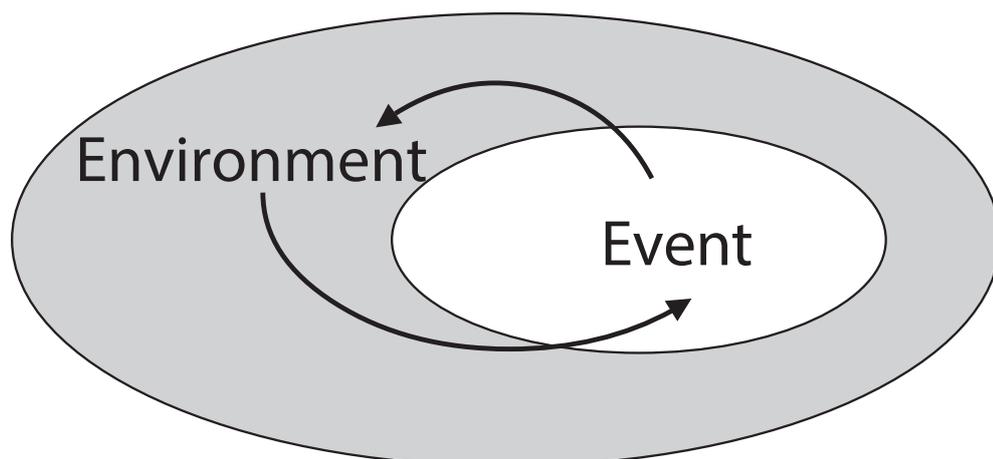


Fig. 4 The event system and its environment

How can these desired and spontaneous events be incorporated into a security observation that gives the unforeseeable behaviour of an artist/visitor a framework and actively demands the security of an event, and not just in declarations of intent? How does this define a danger to an event? By what criteria can these dangers be identified, how are the risks evaluated, and with which measures are they verified? **In other words: What dangers and risks arise from the event?**

Digression:

Events are described or determined with various attributes. Large, small, loud, quiet, great, boring - none of these words describe the level of danger of an event. There is no binding legality by which large events are automatically dangerous and small events are safe.

Events can be both large and dangerous as well as large and not dangerous.

The security objectives of an event must be divorced from the observation of the quantity (size). An event always creates a bracket for the coming together of people and encompasses a spectrum of event types that can only be categorised and typified with difficulty.

To this end the public interest in the area of art and culture is institutionalised, indeed in the form of state or municipal sponsorship of the great theatres as an historic legacy, especially of the 19th century („subsidy theatre“), and further in the form of sponsorship of museums and the funding of alternative cultural sites. This portion of the cultural scene developed from the citizen initiatives of the 1960s and 1970s.

All other business premises and types in the event industry are indeed part of public life, although their execution is purely a private matter. This means that only the personal interest of the two „business partners“ of event company (earning business) and audience (customer) is decisive.

The historically manifested public and state interest in sports, together with the legal grounding thereof, leads to a significant tolerance of financial or other strains on the public budgets or municipal infrastructure during sporting events.

Sports, especially football, are thus a political and economic occurrence of general interest. This is made especially evident by the fact that sports, with all of their components, are always part of the respective government programme and are, among other things, a major business area for the interior ministry portfolios. On top of that are the truly extensive state and federal programmes from a financing perspective. Both the popular and top-class sports are national concerns. Their influence in politics can thus not be underestimated. The evaluation of the security of sporting events must thus be observed in its own context.

A.5 Needs, Goals, and Behaviours of Visitors

The control and guidance of visitors is subject to aspects of security, well-being, and comfort, as well as building law. Most visitors only pay attention to comfort and intuitive behaviour control is usually enough to prevent uncertainty. This means that the implementation of the conceived plan can automatically occur without having the constantly reevaluate the goal or plan. Yet if circumstances become adverse, the original goal takes a step back while security and well-being become the priority objectives. A reevaluation (selecting a new objective) or a change in the activity chain or route selection (change in planning) thus occurs.

How can this personally perceived security be measured?

That is why the question of when a situation is perceived to be unsafe or uncomfortable is central to planning visitor flow. The influences that determine and that can impair well-being are depicted in the illustration „Well-being“.

There are four different zones:

- **Comfort,**
- **Bearability,**
- **Troublesomeness and**
- **Unbearability**

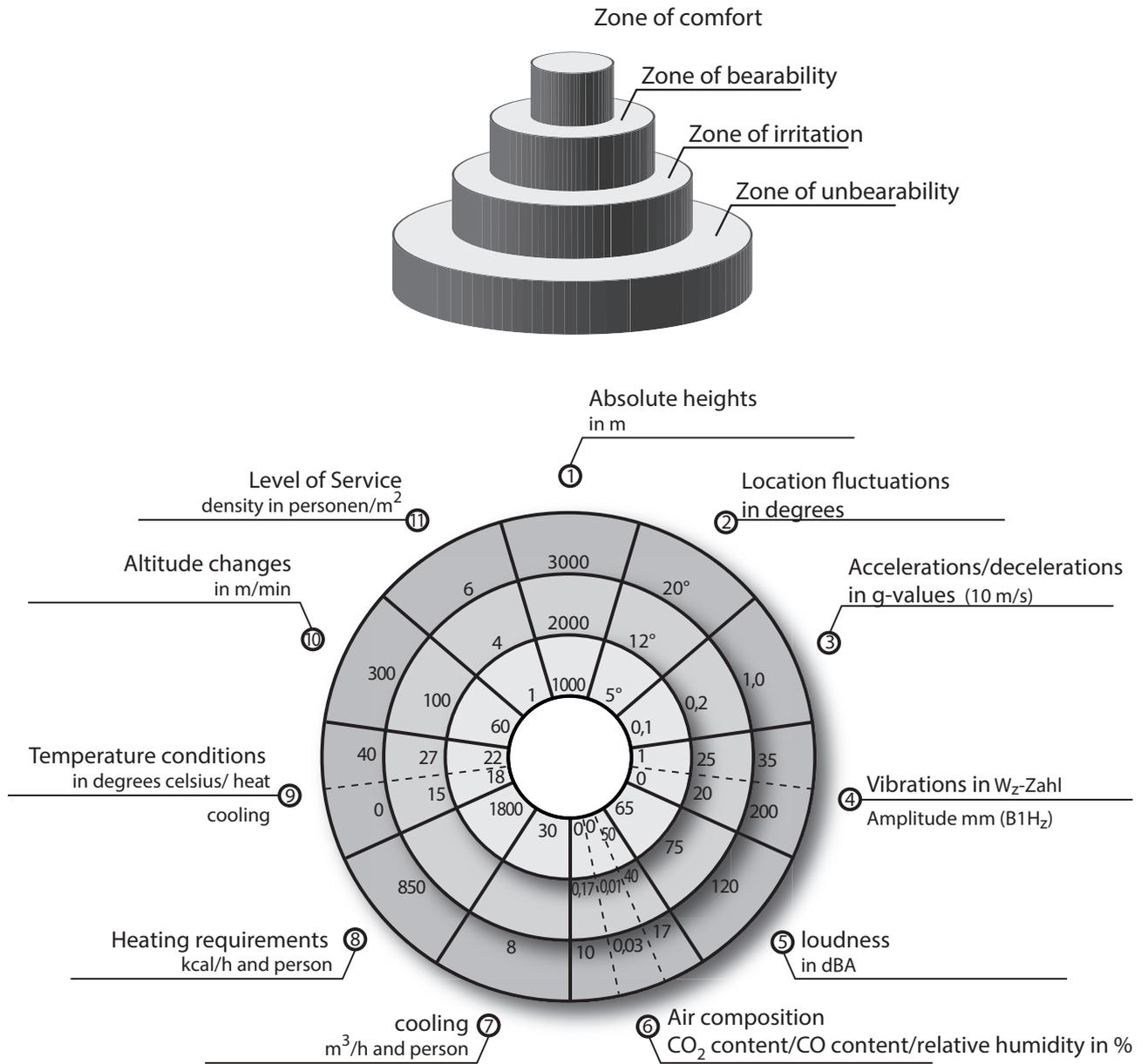


Fig. 5 Well-being

Fruin's „level of service“ concept designed and adapted for pedestrian traffic is applied to the assessment of movement of a large number of people.

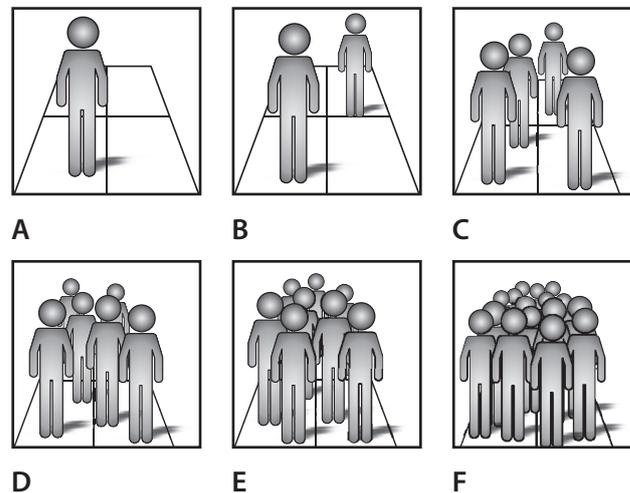


Fig. 6 Level of Service (LoS)

Level of Service A to F for mobile people is shown according to the original categorisation. These levels are grouped into categories A-F.

Category A and B Comfortable
comforting

Category C and D Secure
bearable to bothersome

Category E and F Insecure
unbearable

The insecure area is defined by LoS F for the dimension of crowd density. For movement on walkways the level of service is achieved at 2.2 P/m², for stairs at 2.8 P/m². The quality of a facility for pedestrians can thus be measured, namely by crowd density. Yet of course, the personal perception of a person will not depend on the local crowd density, i.e. the size of the crowd. Along with this and other objectively measurable criteria, personal preferences play a crucial role.

A.6 The Term „Panic“

The term „panic“ plays a special role. The widespread perception throughout society of „mass panic“ cannot be 100 % confirmed from a scientific perspective and should thus be independently assessed as part of a security concept.

In order to prevent a flight response due to the sudden appearance of an outside influence, a schematic risk assessment must occur as per the procedure defined in item 3. The term „panic“ should thus be used responsibly, especially in terms of panic prevention.

The term „panic disorder“ is known and recognised for an individual. Individuals can thoroughly exhibit such behaviour. However, one should not fear individuals suffering from a panic attack „infecting“ others in a crowd. The seven myths of mass psychology that concern the behaviour of people in crowds and in times of stress should be applied to the observation of the term „panic“ in the context of visitor groups. The tradition of this manner of thought is attributed to LeBon. According to this, people in a crowd behave in accordance with seven myths:

1. irrational (unreasonably)
2. emotional (perception)
3. suggestible (extent of the perception)
4. destructive (harmfully)
5. spontaneous (involuntarily)
6. anonymous (unidentified) and
7. uniform (consistently)

Naturally the extent to which these attributes describe individuals will always depend on the circumstances. However, there is no empirical evidence that people in dangerous situations act irrationally. Normally the behaviour is subjective and the individual believes it to be sensible. For instance, this is the case with people who appear to react irrationally to a fire. This behaviour is not rational, but rather the better of two bad alternatives. It is similar to when people make decisions due to their limited information, although these decisions may seem irrational from the outside. They are logically understandable given the circumstances (limited knowledge).

The idea of the emotional mass goes back to LeBon's theory of deindividuation („collective soul“). There are also no observations for this in the respective area (i.e. what is generally referred to as „panic“, e.g. at mass events) that support this hypothesis. Suggestibility can occur in groups in some circumstances, although in general due to a shared prior experience. This is thus more significant for political or religious groups. Destructiveness, for example, can be seen from football hooligans. However, this is no mass phenomenon and is not caused by a meeting of people. It has much more to do with an individually planned and premeditated behaviour that uses the crowd as a place to hide and football as a stage. It behaves similarly with spontaneity and anonymity. Fan groups prefer uniform clothing and shared rituals, and to be part of the fan culture or the „event“ experience. But here, too, uniformity is desired and planned. It is brought about not by the crowd, but at the individual level. It can occur in small groups not generally considered a crowd or mass group. All of this leads to the observation that „panic“ does not stem from the crowd. It has much more to do with the external circumstances that can lead to panic. In other words:

Danger is not caused by panic, **panic is caused by danger.**

The most important aspect of this consideration is that freely selected immobility does not present any problems, while involuntarily selected immobility certainly does. With this definition it is possible to permit a dense crowd onto a dance floor, as this is freely selected immobility on behalf of the visitor. For that reason it must always and everywhere be ensured that people can move around freely and unimpeded for the secure flow and positive experience of an event. Once the freedom of movement is impaired, this causes stress, and if the impairment is so great that progress is no longer possible, this may result in dangerous situations.

Restriction of the freedom of movement can be recognised with the following criteria, among others:

1. Congestion in the flow of people
2. Clearly visible lateral (side) movement (not making progress)
3. „Stop and Go“ waves

All three phenomena may not arise unexpectedly and in combination if possible.

A.7 The First-Aid Service

The role of the event's first-aid service (FAS) is to tend to general health issues of the event's participants and perform any necessary extended first-aid measures. This service may also be available to actors/employees of the organiser. Depending on state laws the service provider of the FAS may also perform emergency medical service if they have authorisation to work with the public law emergency medical service. The service provider's role with the first-aid service may also include other care-related services.

The responsibility for the medical / emergency medical care of the event participants lies solely with the organiser. The organiser may transfer the task of medical / emergency medical care to a suitable FAS service provider. The organiser may commission the FAS as a voluntary service or based on official legal requirements.

The commissioning of a third party to implement an officially required obligation of the FAS does not relieve the organiser of their responsibility to the authorities, whereby the official legal requirements must absolutely be fulfilled.

A contentual exceedance of the requirements in the FAS service provider's planning is possible, especially because the official legal requirements do not include the necessary aspects of incident command or service and logistics services, as well as event- and location-specific details.

The personal/material and technical establishment of the FAS should comply with the generally recognised calculation methods for the FAS. These are based on the security objective definition clearly coordinated between the organiser and the service provider at the beginning of the planning process for the FAS.

The commissioning of the FAS service provider should take place as soon as possible. An early beginning of the planning process allows for questions about emergency and escape routes, set-up areas for the FAS, special security measures, accreditation of the emergency crews, supply and disposal matters of the FAS, etc., to be clarified between the partners and authorities involved. The result of this FAS planning should be replicated in a written assignment or assignment order (as per service regulation 100 for non-police hazard prevention) for the FAS and be incorporated into the organiser's security concept.

The service provider's plans for the FAS must cover regulatory needs and contain a small amount of reserves to cover bandages. Weather effects and other external influences may lead to this preliminary planning and buildup of reserves not being sufficient, even without the presence of a „major incident“ that demands the deployment of public emergency teams. Necessary additional claims by the FAS service provider in this regard must be coordinated with the organiser and the responsible authorities.

In addition to caring for the event's participants, it may also be necessary to ensure medical care for actors of the event as per internal/additional regulations of the central organisations/accident insurers.

The following points should absolutely be considered when selecting the FAS service provider:

- Do they have technical experience in planning and executing FAS?
- Does the service provider have sufficient personnel and materials?
- Do the employees utilised have corresponding medical qualifications (e.g. paramedic, ambulance crew, ambulance paramedic) and/or management qualifications (e.g. group or station officer)?
- If the employees are regularly trained, were the legal/state regulations on the extent of training and the content thereof adhered to and can this be verified?
- Is the service provider for the FAS associated with non-police hazard prevention?
- Does the FAS service provider have sufficient damage liability coverage and are the employees utilised covered by the employers' liability insurance association?

The FAS service provider must be carefully selected, because failure on behalf of the FAS service provider can have a significant impact on the event or even lead to necessary cancellation of the event. Both of these occur at the expense of the organiser.

A written agreement on the assignment and scope of services must always be finalised between the organiser and the FAS service provider. The assignment order for the first-aid station can be consulted as functional/requirement specifications. The observation of and adherence to legal regulations and medical standards is the role of the assigned FAS service provider. After the event is over the FAS service provider should submit a service report under consideration of legal regulations (e.g. privacy protection).

During the event the incident commander of the FAS should regularly communicate the FAS situation with the organiser at safety group meetings. The organiser must keep the incident commander of the FAS up to speed with current information on the proceedings of the event (e.g. visitor count, disruptions, etc.). At large events or in case of extraordinary incidents during the event, the incident commander of the FAS or their representative is part of the organiser's coordination team.

A.8 The Security Service

The establishment of a security service at events depends on state regulations. In other words, **„If the type of event requires, the operator must compile a security concept and establish a security service.“** The tasks thereof are more closely specified thereafter. According to this, the security service is especially responsible for the

- monitoring of entrances and exits, and access to visitor blocks,
- observation of maximum permitted number of visitors and arrangement of the visitor areas,
- adherence to the prohibitions of local ordinances,
- security announcements, and
- orderly evacuation in the event of danger.

The necessary qualification of the security service depends on the respective tasks it is given. There are various perceptions of this, especially regarding the demarcation or demand for the establishment of a security service in accordance with local regulations.

Essentially the verification or expert assessment is the obligatory minimum requirement for companies and their personnel deemed responsible for „the monitoring, organisation, and security“ of events. This includes, for instance, monitoring the entrance area of night clubs. Other activities often branch off from this, such as checking bags or identities. The allocation of parking or seating, as well as the invalidation of visitors' tickets and their categorisation by the permit and security authorities as an order/security/customer service differ greatly by state in some ways. The lines between security and order are thus not always clear.

However, as a rule of thumb an examination and years of professional experience with personnel and management responsibility at events should be considered a minimum requirement.

A.9 Can an Event be Secure?

If you imagine the definition of events as an open, dynamic system with the term of security divided into various dimensions, which are in turn evaluated from the perspective of the organiser, the visitors, and the security authorities and organisations (SAO), it seems almost impossible to theoretically and overall validly describe the ideal road to a secure event. Each type of event has its own potential for security and insecurity. The depiction of these secure and insecure areas with only one, two, three, or more methods of risk observation will not lead to a stronger event in terms of resilience.

However, in the past there have been countless events that have been held securely with no special form of security observation. What factors play a role here? Are events that undergo a purely theoretical and, partially, purely judicial security assessment automatically more secure? To answer the question, „Can an event be secure?“, we should place our focus on real life practice. On events that are securely experienced and held within a broad social spectrum. This not only includes a large event or a large festival. Rather, it is about the question of how one, when observing event security, can present a spectrum of small events in cultural and communal buildings and traditional events, classical venues, up to temporary events in the public, urban space, all of which present a path to practical and comprehensible implementation.

Real life practice is shaped by the preventative observation of all actors, following the motto:

„Better safe than sorry!“

This view of practical implementation should not digress from the fact that this motto neglects unknown factors confronted by events that no longer guarantee visitor security.

That motto shows the direction of the observation. This mostly unconscious prevention by the actors involved does not aim to create security, but to prevent insecurity. This occurs in discussions and coordination that decide what measures will be used to combat risks and dangers. It is a preventative process that presents those involved with the possibilities of various paths toward a response. This also occurs from the focus of an event and draws back on its pattern of behaviour.

A.10 Prevention as a Basis for Secure Events

When one preventatively considers the question of an event's security, they try to make undesired occurrences less likely in the future. From an analytical perspective prevention initially designates a counteractive effort to prevent or control the occurrence of a potential state. While the narrower definition of prevention is perceived to mean that „only one possible version of the future is ruled out“, the practical strategies of prevention often include the attempt to implement a specific version of the future.

The strategy selected for the secure holding of an event thus builds upon a preventative strategy that is intended to prevent problems that do not yet exist.

From this arise ten questions that will be answered from various perspectives for purposes of the event:



Question 1

What are the objectives of the event?

This question focuses on knowledge of the event, resulting in problem definitions, foreseen objectives, assumptions of causality, and plausibility strategies.

- > What is the objective of the organiser?
- > WWhat is the objective of the visitors?
- > What is the objective of the operator?
- > What are the objectives of the residents?
- > What are the objectives of the SAO?
- > ...

Question 2

Who bears the economic risk?

This question supplements the question about the event's objectives and presents the economic environment/area of conflict in which the event is being held. Only with the knowledge of the economic relationships is it possible to integrate preventative considerations in an early planning phase and implement them in reality:

- > Who bears the economic risk?
- > How many parties bear the economic risk?
- > What sponsors support the event?
- > What revenues are generated by the sale of TV rights?
- > Is the event financed by ticket sales?
- > Can the economic risk be insured?
- > Can an economic risk be compensated?
- > How has the event developed in the past?
- > ...

Question 3

Have the responsibilities been clarified?

The responsibilities in homogeneous, clearly definable systems are based on the assumption that the individual actors are equally as dangerous as they are in danger. The system of the event is, however, an open and dynamic system in which the responsibilities cannot always be 100 % clarified. These overlap, change, and cannot be clearly defined by the somewhat complex system. This state can only be preventatively counteracted via extensive transparency of the individual by being alert to internal and external threats.

It is a highly communicative process. If this is not possible due to unclear structures, language barriers, cultural differences, or non-attainability, one must build upon the self-responsibility and self-effective accountability of the individual actors.

To this end it must be clear that this is not possible in crisis situations or dangerous scenarios, as one can end up playing the role of victim as well as perpetrator. In this case you are powerless as the victim, and all-powerful as the perpetrator.

Prevention aims for a clear definition of the accountabilities. In areas in which this cannot be clarified, one must find communicative ways to ascertain these regardless. If this is not possible, this is an indicator of a solution that cannot be found preventatively and which must be resolved with the methods of risk management.

- > Can the responsibilities be comprehensibly determined in a flow chart?
- > Can the demand for a technical service standard be transferred?
- > Are there undefined responsibilities?
- > Is there overlap in the responsibilities?

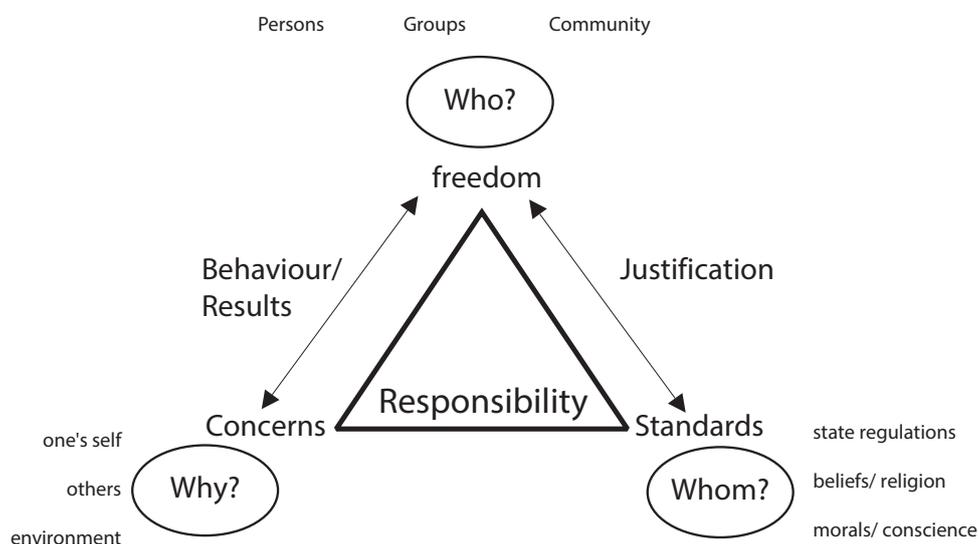


Fig. 7 Basic relationship of responsibility

Question 4

Was the feasibility of the event assessed?

Events can occur spontaneously, cyclically, or with different preliminary planning times. All planning processes are similar in that before implementation, it must be assessed whether the event can be held at this point and in this special context with the actors involved. This is thus the question of the feasibility of the event.

To this end strategically preventative actions are coordinated to realise a specific version of the future. One acts with foresight and identifies the dangers in clear, homogeneous systems (clear visitor structure, precise knowledge of ticket sales, years of experience with events, etc., while following the motto, „**Forewarned is forearmed.**“ This motto usually becomes clear to the individuals in charge of the event.

However, this is not easily possible in self-regulating systems. The question of feasibility cannot be definitively answered with regard to events at which, for example, the visitors are highly heterogeneous, at events that are „free and outdoors“, or at events that have never happened at this point and in this format. The dangers are isolated in a risk assessment, independently observed, evaluated, negotiated, and implemented.

If events are confronted with threats (storm, terrorism, non-categorisable bags, etc.) then prevention and the associated risk assessment come into play. The risks are not tangible, and usually cannot be described with probabilities. However, events are held that are faced with these threats. The likely probability is not the main focus in this case, but rather the unlikely. The unexpected is both envisioned and expected.

- > Is this a cyclical event?
- > Is the event being held for the first time?
- > Are the visitor groups homogeneous or heterogeneous?
- > How were past experiences evaluated?
- > How are these experiences being utilised?
- > Can dangers and risks be listed?
- > What threats are to be expected
- > ...

Question 5

Who can have an influence on the event, and how?

The influence on an event varies greatly and can be exerted by authorities, the residents, the artists, or by the visitors. In clear structures and homogeneous events, disruptions and dangers can be recognised/identified and then removed/eliminated. Checking all guests at the entrance to the venue is an effective way of discovering and eliminating disruptions and dangers. This preventative strategy can be broken down in different ways and must be customised to suit the event format.

Isolation and filtration is not easily possible in heterogeneous systems (and those which regulate themselves more strongly such as Christmas markets, family events, „free and outdoors“ events for everybody who wants to come, etc.), as the dangers and disruptions are part of the system. Intervention thus generally occurs upon changing the incentives. The risk factors, not the risk causers, are the focus of the change. Disruptors are not isolated as they are in homogeneous systems, but rather consciously affected by a change in incentive. The position of refreshment stations such as toilets, concession stands, or video screens is a common way to positively influence the incentives/needs of the visitors.

In threatening circumstances the two aforementioned aspects of intervention are approached and strengthened by legal prohibition. This may be a prohibition of outside drinks referred to by the building regulations in advance or upon entering the event venue.

Aside from these factors events are also influenced by external social processes, trends, and tendencies. These must be considered in the observation and can change completely independently at any time.

- > What is the event's radius of influence?
- > How are non-participating residents involved?
- > How can one react to disruptions?
- > Are disruptions such simple booing from the crowd an accepted form of disruption, or do these entail involvement by the security service?
- > Is there a clear overview of the expected visitors?
- > Will the visitors be checked or scanned?
- > ...

-->

Question 6 What dangers and risks arise from the event?

Dangers arise from external disruptions (intruders). Because disruptions must always be expected, events cannot be homogeneously represented, regardless of the expense with which they are being held. With very homogeneous event formats, a disruption that is not in itself dangerous can develop into a danger/risk.

These disruptions are counteracted in the preventative observation of the self-regulation/heterogeneous events alone, or active support from the hazard prevention teams prevents the danger from turning into a catastrophic event.

This observation is supplemented by the list of risk sources in the chapter „Methods and Procedures“. All preventative actions are intended to precisely name and gauge the dangers and risks that cannot be preventatively removed, as well as how and in what manner these can be processed with a risk management system.

- > Are the disruptions covered by the list of risk sources?
- > What disruptions are known?
- > What disruptions can be ruled out?
- > How do the visitors react to dangers and risks?
- > What dangers and risks arise from the event concept?
- > ...

Question 7 What behaviour is to be expected at the event?

The fear of danger, risks, and the threat of catastrophe shapes our daily behaviour. **If this fear is to be banished or at least restrained, it must first be triggered.**

Preventative considerations in pure and clear structures/ homogeneous event formats can thus quickly turn into compulsive and paranoid processes. Everything must be pure and clear. The proper placement of the guests is a diplomatic masterful feat and a spontaneous change in this results in rash behaviour by the actors involved, who then lose focus of any potentially significant dangers and risks in the periphery. The visitors perceive a minimal change (e.g. in the acoustics at a classical concert) as disruptive and leave the event early, or a brief wait for a service leads to discontent among the guests.

This behaviour is not so quickly observed in self-regulating systems, however these tend toward fatigue and exhaustion as everybody soon feels responsible for everything. This affects the event organisation level as well as the visitor level.

Threatening circumstances can usually not be envisioned and when they arise, one's reaction is usually frantic and irrational. For that reason it is important to address these threatening circumstances and perceive them realistically.

- > What expectable visitor behaviour patterns can arise from the results of discussions and coordination, experiences, and the danger and risk assessment?
- > What sources/information are considered re. visitor behaviour in situations?
- > Is a possible (reaction) behaviour – from outside, etc. – considered?
- > ...

Question 8

Who makes decisions about the event?

In order for decisions to be made there must be corresponding decision makers who are aware of their position and the associated responsibility. As part of a preventative observation, processes and arrangements must be selected that methodically affect individuals or groups and influence their behaviour either directly or indirectly. To this end, either power must be exercised (by official regulations for holding the event) or anticipatorily treated or preventively intervened, so that balance can be struck among everybody involved in the event.

With homogeneous event systems everything is meticulously planned and there is a high degree of discipline among all involved to fulfil this task if the parties involved have the necessary power. Like the allocation of seating (block 7, row 3, seat 5), access control is a common way to give the event a certain structure that clearly defines the room for making decisions. For instance, this is how a movie theatre can be operated with no active security service or usher despite the rather high and regularly changing number of visitors.

This changes in self-regulating systems and the monitoring is expanded to individual areas to enhance self-regulation. This requires constant and clear monitoring at various levels, as it is not clear whether the decisions can be made by the individual actors in the way required by this. Should this result in deviations (the fans are no

longer standing for three hours in front of the venue because of the free selection of seating, but rather three days), the organiser must gauge the extent to which they will react, who will make decisions in this area, and how these will be implemented.

It becomes problematic when threatening circumstances arise. Then the organiser must explain how they expand their autonomy and which legal and economic precautions must be made to rule out situations that restrict this autonomy. The protection of life and body is thus the top priority when considering cancelling an event (e.g. due to an unexpected storm).

Should the threat no longer be the exception but rather develop into a permanent state, the organiser loses their sovereignty over the event and can no longer act of their own accord.

- > How are the contracts between the organiser and the operator finalised?
- > Are all actors aware of their decision-making domains?
- > Do the decision makers know one another?
- > How quickly can decisions be made?
- > Are quick decisions prevented by the structure?
- > Which decisions are made by the organiser and which are made by the SAO?
- > ...

Question 9

What information is available about the event?

The information available about the event varies significantly by the respective position of the actors involved in the event. The operator has different information than the organiser, the security service works closely with the visitors and sees which information they have.

The artistic performance can work with the visitors' information (question from the stage: „You all feeling good?“) or completely ignore said information and not integrate it into the creative process.

The knowledge that the parties involved have plays a big role in evaluating the available information. The information about an event can be categorised into the following groups:

**Available
information:**

Observed events that have happened at least once before („known knows“) must result in reliable prevention of said events by the organiser. The quality of the measures must be technically, organisationally, and personally defined. Prevention is a tried and true resource.

**Uncertain
information:**

The „uncertain“, not clearly describable dangers (illogical, coincidental, not systematic), „known unknowns“, result in the failure of preventative measures of dynamic processes. The point in time and/or location are unknown and the limitation of the effects must be prepared by organisational measures, e.g. determining a crisis team. You cannot simply act preventatively, you must react to events.

**Unknown
information:**

Unknown and unplannable events are difficult or impossible to ascertain, and are depicted by the Black Swan theory („unknown unknowns“). You must rely on damage control and a strong culture of security.

	Knowledge (knowns)	Lack of knowledge (unknowns)
Knowns	known knows	known unknowns
Unknowns	unknown knows	unknown unknowns

Tab. 1 Knowledge/Lack of Knowledge

The available knowledge or lack of knowledge of events increases at events with a homogeneous character, from the „known knows“ and „known unknowns“ of self-regulating systems up to looming „unknown unknowns“.

This may occur over multiple steps. Hazard prevention should eliminate dangers in a homogeneous event, or at least control them. This is not necessary in self-regulating systems/heterogeneous event systems because the cause is not combatted, rather the ability to manage the conditions increases. If the unavoidable, a catastrophe, has occurred, the priority is keeping the damage low.

- > What knowledge is available about the event?
- > What lack of knowledge is there, or in other words: What knowledge

- is not available?
- > How does a learning curve form during preparation?
 - > How is new information considered before and during the event?
 - > ...

Question 10

How are the parties involved prepared for the event?

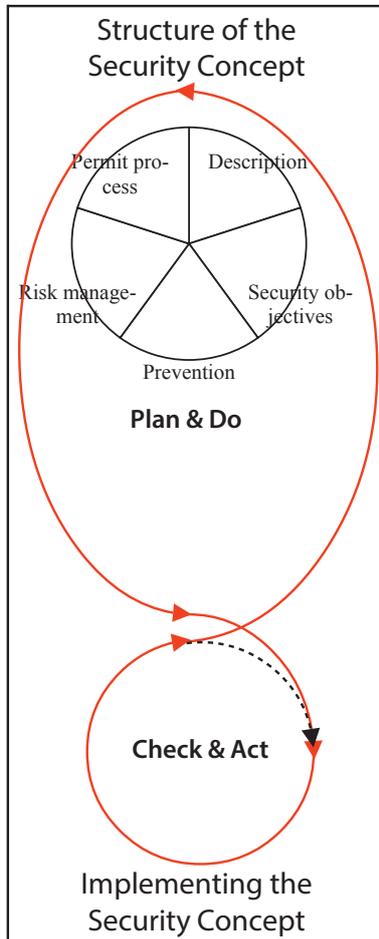
The principle of „You can never be too cautious too early,“ shapes the mindset of the question of the preparation of the parties involved. The preventative consideration never ends and is always being questioned and reevaluated. To this end it must be considered that the parties in homogeneous systems/events are never finished improving these preventative measures. One should never stop beginning in self-regulating systems/heterogeneous events. And if threatening scenarios are impending, you must expect the worst.

- > How are the visitors included?
- > When will the visitors be included?
- > What preparation is available to the parties involved?
- > ...

The Security Concept

B

B Structure of the Security Concept



The breaking down of the security concept is a crucial point that should be considered in the necessary coordination of everyone involved in drafting the security concept.

If the description of the event, the definition of the security objectives, the expected dangers and risks, and the corresponding measures at various locations are mentioned in this step or further described in another step, you quickly lose the overview and cannot separate these considerations from one another. The opposite of the desired approach of „creating clear structures and responsibilities“ can be achieved by such a document.

The security concept is a concept, not an assessment. The security concept must divide the complex, open and dynamic system of an event into sub-areas and provide a structure that allows all parties involved to engage in different processes. The following structure provides a clear framework for this:

1. Description
2. Security objectives
3. Prevention
4. Risk management
5. Permit process

This conceptual approach to event security is integrated in the „Plan-Do-Check-Act“ cycle (PDCA). A continuous processing of all five points occurs in coordination with all parties involved.

1 Description of the event

1. Parameters of the event
2. Special terminology
3. Operator <--> Organiser
4. Event organisation (flow-chart)
5. Partners: availability and presence
6. Technical/organisational communication
7. Security and coordination team of the organiser
8. Structural situation on the event premises
9. Structural situation outside of the event premises
10. Technical facilities
11. Security facilities
12. Walkway and space usage
13. Security service



14. Fire protection / fire safety team
15. First-aid service (FAS)
16. Visitor capacity
17. Escape routes and emergency exits
18. Accessibility of the venue
19. Radius of influence/draw area
20. Visitor information
21. Security announcements
22. Target group of the security concept
23. Enclosures
24. Post-processing

2 Security objectives

1. What should be protected against?
2. What should be protected?
3. To what extent should these be protected?
4. How should this objective be achieved?

3 Prevention

1. Processing the ten preventative questions
2. Summary
3. Defining the identified dangers and risks

4 Risk management

1. Risk identification
2. Risk analysis
3. Risk assessment
4. Risk response
5. Monitoring and evaluating

5 Permit process

1. Integration of public administration by the organiser
2. Defining the process
3. Declaration of unanimity among the parties involved

B.1 Description of the Event

1.1 Parameters of the Event

The type of event and the necessity to develop a security concept does not primarily stem from the demarcation of various types of event (large or small, indoors or outdoors, loud or quiet, peaceful or wild, joyful or aggressive, etc.).

The basis for the assessment of the event is the observation of the expected visitor behaviour and both the desires of interest to the visitors as well as the local parameters. The visitors' expectations are multifarious and overlap. The good perspective of the scene, protection from environmental influences, a brief waiting period in the entrance area, or experiencing an artist as closely as possible constitute visitor desires. The visitors can thus be actively led through attractions (desires). Areas in which the visitors have no view of attractions do not invite them to linger.

The parameters should be depicted as precisely as possible with the following points:

- How is the presentation conducted (programme description)?
- Where does the event take place (note on structural situation)?
- When does the event take place (date, time)?
- How long does the event last (duration over time)?
- What types of visitors are expected (happy, calm, aggressive)?
- How are the visitors arriving (form of transportation)?
- How are the visitors included in the event (action/reaction)?
- What are the visitors' expectations (definition of desires)?
- ...

1.2 Special Terminology

List of special terminology and designations not explained by common linguistic usage. This is especially important at international events with a multilingual organisation.

- Clearly define consistent terms
- Glossary
- Common thread between planning and security concept
- ...

1.3 Operator <--> Organiser

Clarification and demarcation of the responsibilities between the operator of a venue and the organiser, and naming the:

- representative of the operator
- representative of the organiser (event leader)
- head of the security service, and

- people responsible for event technology
- ...

1.4 Event Organisation (Flow-Chart)

The event organisation should be depicted with a flow chart in which the most important functions are defined. This can be supplemented with a description of the qualification, task descriptions, and interfaces. Furthermore the local and organisational responsibilities must be defined with regard to the security authorities and organisations (SAO).

1.5 Partners: Availability and Presence

Listing of the personal availability of the functionaries named in the event organisation, with information including:

1. Surname
 2. First name
 3. Function
 4. Telephone/mobile/wireless
 5. E-Mail
 6. Representation regulation
 7. Presence
 8. Function in the security and/or coordination team
- These include the operator's contacts from the areas of
- Management,
 - Technology,
 - Security service,
 - First-aid service,
 - Service
- as well as those of the organiser from the areas of
- Management,
 - Artists/cooperators,
 - Security service,
 - Technology, and
 - Service.
- Security authorities and organisations (SAO) from the areas of
- Police,
 - Fire department,
 - Emergency rescue service,
 - Security office

- and additional specialist authorities from the areas of
- Building supervision,
 - Environmental office,
 - Traffic authority, or
 - Office for the protection of historic sites and monuments

- and additional partners from the areas of
- Public transit,
 - TV and radio stations,
 - Press.

1.6 Technical / Organisational Communication

The communication concept must address the technical and organisational needs of the event, and is based on Item 1.5 and the partners named therein, as well as the availability thereof. Furthermore, the composition of the organiser's security and coordination team is precisely defined. Along with the personal composition and overview of availability, the redundant means of communication must be named. These may be:

- Availability via wireless devices
- Telephone (landline)
- Mobile network (not ensured at events)
- ...

1.7 Security and Coordination Team of the Organiser

In order to ensure that the security and coordination team can functionally convene and work continuously, the following points must be named:

- Space and meeting place of the security and coordination team
- Threshold to convene the security and coordination team
- Tasks of the security and coordination team

The tasks of the security team include:

- Operative coordination of all measures from beginning of event
- Coordination of all internal and external measures
- Informing the visitors and workers
- Informing the security and specialty authorities

The tasks of the coordination team include:

- Exchanging/comparing information between the parties involved directly before the event with the so-called „cold status“
- Operative coordination of all measures in a crisis (e.g. during a disruption)

- Demarcation from the area of deployment of the fire department, emergency services, or police
- Coordination of all internal and external measures in a crisis
- Informing the visitors and workers in a crisis

1.8 Structural Situation on the Event Premises

- Structural facilities (venue, business premises)
- So-called floating (temporary) structures (stands, tents, amusement rides, special structures)
- Infrastructure (fences, guide elements, water supply and drainage, toilets, waste disposal)
- Barrier-free access
- ...

1.9 Structural Situation outside of the Event Premises

- Roadblocks
- Guiding elements
- Other structures and facilities
- Usage of the public infrastructure
- ...

1.10 Technical Facilities

- Event technology (lighting, audio, video, SFX, energy supply)
- Catering
- ...

1.11 Security Facilities

- Security technology (lighting, sound exposure)
- Fire safety technology (fire extinguishers, smoke vents, sprinklers)
- ...

1.12 Walkway and Space Usage

- Walkways in front of the venue
- Walkways on/within the venue
- Steering the visitors with attractions
- Space usage (visitors, collaborators, storage areas, set-up areas, mobile areas)
- ...

1.13 Security Service

In the Federal Republic of Germany the state holds the monopoly

on the legitimate use of force. The application of direct force against people and things - except in emergency self-defence situations - by civilians (e.g. security personnel) or service providers is thus not permitted. The permissible measures are restricted to the following items and should be conducted by certified companies:

- Monitoring entrances and exits
 - Guiding to the visitor areas
 - Ensuring maximum visitor numbers
 - Adhering to the permitted arrangement of visitor areas
 - Enforcing adherence to building regulations
 - First-aid
 - Implementing bans (smoking, fire, pyrotechnics)
 - Securing production areas at events
 - Parking management
 - Conducting a proper evacuation and opening the emergency exits
 - Security announcements in coordination with the organiser
 - Clearing the emergency and escape routes
 - ...
- Should disruptions occur in these tasks which require direct force against individuals, this is a task for the police.

1.14 **Fire Protection / Fire Safety Team**

Coordination with the fire safety team and preventative fire protection concerning the regulations they feel apply to the event is extensive, and is not restricted to establishing a fire safety team. The following questions, among others, must be answered:

- Does the venue have a comprehensive fire protection concept?
- How is the fire protection concept assessed?
- How is the fire protection regulation implemented during operation?
- Where is there overlap between the security concept and fire protection concept?
- Requirements of the materials (e.g. decoration)
- Usage of open flame or pyrotechnics
- ...

1.15 **First-Aid Service (FAS)**

The organiser must consider the following points for deploying the FAS in the security concept:

- Clear description of the tasks and responsibilities of the FAS within the event area
- Differentiation between the tasks of the private law FAS and the public law tasks of the non-police hazard prevention team (definition of the interfaces!)

- Clarification of any official requirements concerning the FAS
- Is the assignment/deployment order of the FAS part of the security concept?
- How is continuous communication between the event leadership and the incident command of the FAS ensured?
- How is the organiser informed of the current situation during the event, especially in the event of deviations from the planned deployment area of the FAS?
- How is the incident command of the FAS incorporated into the organiser's organisation in the event of extraordinary circumstances?
- Determining/defining quality requirements
- Evaluating/documenting the data after the event
- ...

1.16 Visitor Capacity

Visitor capacity is an important criterion when developing the security concept and must combine different visitor prospects with the requirements of the respective state ordinances.

- Definition of the visitor density caused by the event format
- Visitor capacity (maximum number of visitors according to space usage)
- Seating plans
- ...

1.17 Escape Routes, Emergency Exits and Special Areas

- Escape routes (arrangement, length, height, width, evacuation areas)
- Emergency exits (number, width, signage)
- Police areas (position, access points)
- Fire department areas (position, access points)
- Emergency crew areas (position, access points)
- First-aid service areas (position, accident treatment areas, access points),
- Mass casualty incident areas (MCI; position, access points)
- ...

1.18 Accessibility of the Venue / Transit Concept

- Arrival and departure of guests (footpath, car, public transit, etc.)
- Pathway guidance
- Incorporation of the venue in the local infrastructure (footpaths, streets, motorway, rail, airports)

- Parking capacity at the venue
- Roadblocks and stopping restriction
- ...

1.19 **Radius of Influence / Draw Area**

Each event more or less works beyond the venue's scope of influence. In order to ensure security and order, the organiser must determine in advance how far their event's scope of influence will be: This may extend from a few metres outside of the venue to regional or national impacts on the public space. It must then be determined which points are relevant for the security concept so that clear differences can be drawn between the security concept and the transit concept. The transit concept is attached to the security concept.

1.20 **Visitor Information**

Events are announced in different ways, starting with simple word of mouth or personal invitations up to social networks or the classic advertisement. This communication should be accompanied by a supplementary risk/security notification for the visitors as needed.

The purpose of this risk/security notification is to,

- inform the visitors of any potential risks and clarify them,
- show how the visitor can contribute to a safe event with their own behaviour (reference to park & ride, bus shuttle, sunscreen, etc.)

This notification can be supplemented with the following points:

- Ticket status
- Notes on arrival and departure
- First-aid stations
- Programme
- General information on security topics
- Building regulations
- Escape and emergency route layouts
- ...

1.21 **Security Announcements**

The security announcements are an independent component and are separate from the visitor information. The security communication must be adjusted to the needs of the event and should always be given a personal touch. Well-known stadium announcers have a better effect on the public than a neutral, unknown voice. The same applies for the waiting areas in lobbies

or train stations, where a personal, direct, and possibly entertaining approach can have a greater impact than the strict tone of a stranger.

1.22 Target Group of the Security Concept

The addressees of the security concept must be clearly differentiated. Demarcations are made between the preparation of the security concept for the official permit process and/or the introduction of special planners or experts for developing assessments and certificates. The process manager is responsible for distributing the security concept to the right partners.

Furthermore, the security concept lays out the framework for cooperation with special planners and experts and determines the interfaces of the respective work. Excerpts from the security concept may also be used to

- instruct the workers, and
- ensure the flow of information at the operative level.
- ...

A clear demarcation must be drawn between the concept and operative planning.

1.23 Enclosures

The following documents may be used as enclosures:

- Applications
- Floorplan
- Detail plans
- Assessments and certificates
- Communication plan
- Flow-chart
- Audit
- Results of a mediation process
- ...

1.24 Post-Processing

The post-processing of an event based on the security concept should be a component of cooperation between partners. The main focus here is a target-actual comparison and an analysis of the event. Ideally these points will be systematically addressed and forwarded anonymously (data protection) in the future. It should have a simple structure with questions on one or two DIN-A4 sheets in which report criteria have been determined. This analysis should be recorded into a database.

B.2 Security Objectives

The various concepts can be condensed down to four core questions for the security of an event and its security objectives. Questions that cover the topic of security objectives are:

- What is being protected against?
- What should be protected?
- To what extent should these be protected?
- How shall this objective be achieved?

So-called protected goods can be determined as items to be protected for the first question. These questions are also partially legally fixed, such as in the precautionary laws.

Along with the pure protected good or item, a security objective also consists of standards and values. There is a great need to reassess the objects and principles of life to be protected as with the model of the basic functions of existence.

The question as to the extent of the protection contains aspects of a level of protection, a size of the objective. Security objective and level of security are often used synonymously. „Security objective“ will be used as the superior term hereafter.

Acceptance and tolerance are two key terms for objectives pertaining to risks. With regard to risk analyses these are often referred to as „acceptable“ or „tolerable risk levels“. It should be pointed out that there is no individual „risk level“. Instead, there are various different levels: individual acceptance, acceptance of multiple individuals, internal system acceptance, social acceptance, and expert acceptance. Tolerance parameters such as the ALARA principle 31, but also terms like „remaining risk“, describe desired objectives or parameters. The security objectives thus formulate desired states and examples. These may be:

„How safe is safe enough?“

The question of an acceptable risk arises once one has come to see that there is no absolute security. When holding events the likelihood of potential damage can never be ruled out with absolute certainty. When assessing the acceptability of a dangerous situation, objective criteria as well as subjective factors of risk perception must be considered. Determining an acceptable / tolerable risk

thus belongs to. The basis of this observation is the definition of security objectives set at the beginning, which describes the risk as the potential, ever possible occurrence of undesired circumstances. Special challenges in the risk analysis for events include

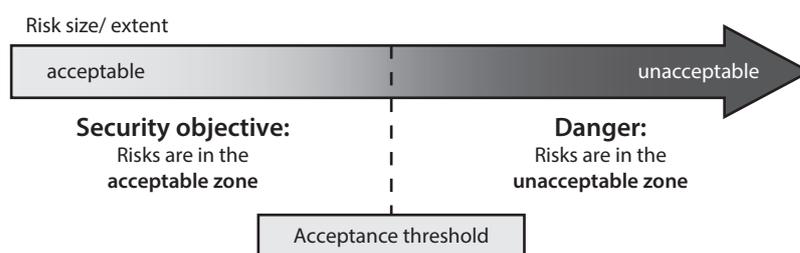
1. artistic freedom, which must be considered and which can only partially be planned, and
2. the double role of the visitors as items to be protected as well as potential sources of danger due to their unpredictable, only conditionally controllable behaviour.

Dangers are circumstances or situations that trigger an undesired, harmful effect upon occurring.

Some risks are accepted in our society, some are considered unacceptable. Attending events will always be associated with risks, as much as any other part of life.

The security concept attests that the risks are in the acceptable zone. If they lie across the acceptance threshold and are thus in the unacceptable zone, measures must be taken to reduce the risk. The goal is to be able to allocate all risks into the acceptable area, taking measures to do so as necessary. Thus:

The security objective separates the acceptable and unacceptable zones.



Figg. 8 Security objectives – acceptance threshold

The security objectives include:

1. Protection of the lives and health of the event attendees
2. Other security objectives that can be attested in the security concept:
 - Personal safety of the
 - Cooperators (artists, presenters)
 - Workers
 - Residents
 - Protection of materials on the event premises and in the vicinity
 - Infrastructures
 - Property/monuments
 - Structures
 - Technical installations
 - Environmental protection
 - Water
 - Soil
 - Air
 - Emissions
3. Other security objectives as per the definition of those involved in the creation

It is attested in the security concept that the security objectives will be achieved and the necessary measures to do so are described therein.

B.3 Prevention

The preventative observation of the event's security occurs as part of a constant process and a continuous processing of the following ten questions:

1. What are the objectives of the event?
2. Who bears the economic risk?
3. Are the responsibilities clarified?
4. Was the feasibility of the event assessed?
5. How can one influence the event?
6. What dangers and risks arise from the event?
7. What behaviour is to be expected at the event?
8. Who makes decisions concerning the event?
9. What information is available about the event?
10. How are the parties involved prepared for the event?

These preventative considerations play a role in the entire development of the security concept and are summarised here. The coordination and clarification occur parallel and at different points in time, with varying significance.

The objective of this processing is to transfer the dangers and risks that cannot be resolved with preventative measures into a risk management process, where they can be addressed with various measures and methods. These may vary greatly and must be individually coordinated.

B.4 Risk Management

4.1 General

Holding events comes with risks. That is why these risks must be identified, analysed, and evaluated. This is part of the risk assessment described in ISO 31000 and which will later be briefly summarised in the context of an event. The risk assessment consists of three components:

1. Risk identification
2. Risk analysis
3. Risk evaluation,
and results in risk management.

The individual components are described in further detail below.

4.2 Risk Identification

Risk identification is the process of finding, recognising, and describing risks (source: ISO 31000). The causes of risks and their potential effects must be identified. Achieving the goal of holding a safe event can be impeded, degraded, or delayed by risks. Risks that may not appear possible at first glance should also be considered. If they are not listed at this time, they may not be considered in the subsequent analysis. Risks not included in the organiser's scope of influence are considered as well. The subsequent consequences of specific effects should be examined in the list.

It is important to very carefully conduct this step of the risk assessment. The more comprehensively the identification is conducted, the less risks are forgotten and the less unpleasant surprises that can arise at the event itself.

Inexperienced organisers and organisers with new types of event formats should systematically walk through the event with a team and address any potential sources of risk.

4.3 Risk Analysis

In this step, an understanding of the risk should be developed. The sources and causes of the risks, their effects, and their likelihood of occurrence are considered. Factors are identified that can impact the effects and likelihood of occurrence, and other signs of risk

are analysed. This step is very important and should be conducted with care, as events have a multitude of effects and can affect various security objectives. Risk controls already in place (e.g. security measures already conducted) are considered here as well and analysed for efficacy and efficiency. This step thus lays the foundation for the decision of whether the risk must be eliminated or reduced. The levels of risk are generally entered into a risk matrix consisting of the likelihood of occurrence and the possible extent of damage. There is also a variety of other procedures that describe the type of risks.

4.4 Risk Evaluation

The results of the risk analysis are the foundation of the risk assessment. This is when the results are compared with the previously formulated security objectives and legally determined parameters. Then it is decided whether measures must be taken to respond to the risk. Risk response can also be given priority, which will then show which risks must first be addressed. One simple method for comparing the actual risk with the permissible tolerable risk is the general risk matrix

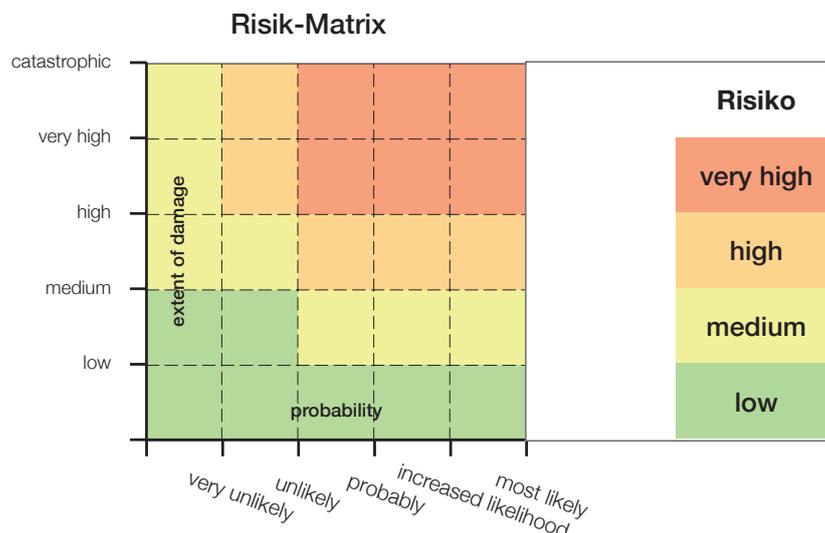


Fig. 9 Example of a risk matrix

If the risk lies in the green area, minor measures must be taken to reduce the risk. In the yellow area it is advisable to respond to the risk and reduce it to an acceptable level (the green area). The principle here is that minimisation of the risk should be kept proportional to the effort to do so. However, it is recommended that the objective be to minimise the risks of the yellow area as much

as possible in order to increase the event's level of security. If a risk lies in the red area, measures must be taken to manage it. If these cannot be reduced down into the yellow or green areas, it must be discussed whether the event can be held under these circumstances and which other measures may be successful

Digression

Risk response

The risk response should occur based on the risk analysis and risk evaluation. Only then can efficient response strategies be ensured. The following series of steps should be observed when selecting the security measures for work protection:

- preventing/removing sources of danger, e.g. smoothing out irregularities in the floor
- technical security measures, e.g. enclosing sources of danger
- organisational measures, e.g. compiling emergency plans
- behaviour-based measures, e.g. informing the security personnel of specific dangers

After the measures have been selected a measure plan should be compiled that clearly defines the priorities for implementing the individual measures, including the respective individual responsible and date of implementation.

- Reasons for selecting the measures, including the intended use
- Individuals responsible for the permit and implementing the plan
- Recommended action
- Resources required, incl. for the unexpected
- Performance assessment and restrictions
- Requirements of reporting and monitoring
- Schedule and implementation plan

It must be considered that new risks can arise from security measures or the combination of various security measures, which must also be assessed and responded to.

Supervision and monitoring that ensure that the security measures have been implemented and are effective are important. In addition, incidents such as near accidents should be analysed and the risk management improved accordingly. This also means that newly arising risks are to be recognised and assessed. The results of the risk management process are continuously documented.

B.5 Unanimity

As the „cause“ of the event, the organiser is responsible for obtaining all necessary permits for the event and for fulfilling the associated legal requirements/conditions.

5.1 Integration of Public Administration by the Organiser

Depending on the management structure at the venue, it must first be clarified which office is the permit-granting authority for the desired event, and which consent is required from other authorities for technical supervision. These may be:

- SAO (security authorities and organisations)
 - Public order office
 - Police
 - Fire department
 - Emergency response team
- First-aid service
- Building supervision office
- Environmental protection office
- Traffic authority
- Historic monuments protection authority
- ...

The circle of individuals involved in coordinating the security concept is defined by this information. The organiser must determine their process official who will moderate the parallel process of drafting the security concept and the coordination process with the public administration and authorities involved.

5.2 Definition of the Process

In conjunction with the process official of the organiser, the public administration clarifies the extent and schedule of the permit process and includes the necessary authorities in the process. The two types of events in this regard are:

1. one-time events and
2. recurring events.

The organiser would thus be able to estimate the „permissibility“ of the event they wish to hold before the process begins, and they would have the opportunity to prepare all necessary documentation.

5.3 Unanimity among the Parties Involved

The process official must ensure that all relevant partners for the secure execution of the planned event are determined in advance and that they are contacted. Communication with them is important so that their needs and expectations can be coordinated during the permit process, so that at the end of the process the desired unanimity of all involved is achieved and confirmed by their signature.

Methods and Procedures



C Methods and Procedures

C.1 Risk Management

Information on methods and procedures that can be applied when compiling the risk assessment can be found in the IEC/FDIS 31010 risk management - risk assessment techniques. It is recommended that the process be conducted in a team, as none of the methods presented in the directive are suited for one person. Furthermore, most procedures include multiple steps for risk assessment. It is thus scarcely possible to find a proper method for each step.

1. Finding, identifying and assessing risks

According to ISO 31000 risk identification is the process of finding, identifying and assessing risks

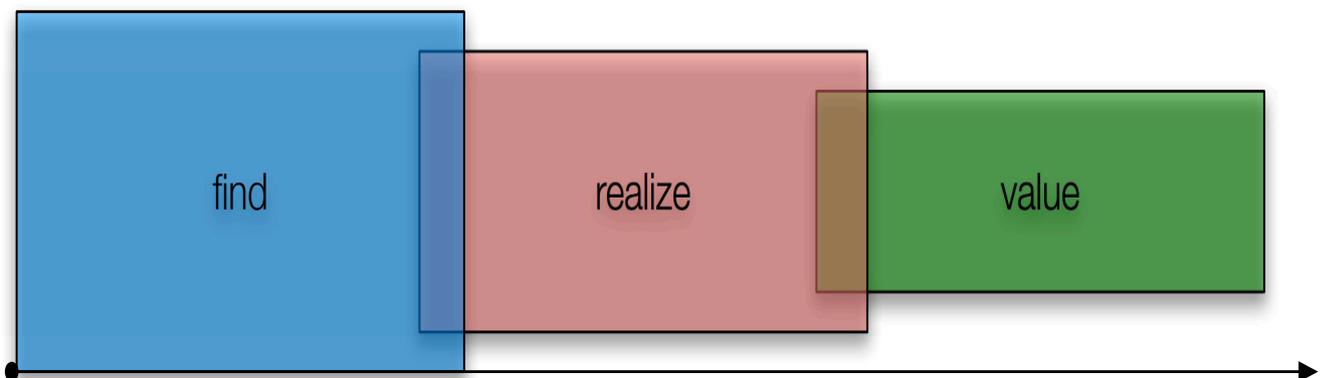


Fig. 10 Finding, identifying and assessing risks

The causes of risks and their potential impacts must be identified. This is to be described using a specific feature that enables clear identification. The difficulty lies in having to list risks that do not seem possible at first glance. If they are not listed at this point, they cannot be taken into consideration in the subsequent analysis. They include risks that are not within the sphere of influence of the organiser. When drawing up the list, the secondary effects of certain impacts should also be investigated. Using preventive considerations, this is much easier, because prevention is the basis



for reliable risk identification and clearly distinguishes this from speculation. The following parameters and guiding questions can be used to describe the scenarios:

Danger

- Which event is being looked at?

Place

- Where is the event taking place?

Space

- Which area is affected by the event?

Intensity

- How strong is the event in terms of its effect?

Time

- When is the event taking place? (time of year / time of day if necessary)

Duration

- How long is the event and/or its immediate effects?

Development

- What leads up to the event?
- How does the event develop?

Warning period

- Was the event expected?
- Can the people affected adjust to the event?
- Can the authorities and organisers adjust to the event?

Being affected

- Who/what is directly/indirectly affected by the event? (people, the environment, the stage, technical facilities, forecourt, etc.)

Reference events

- What similar events have there been?

Additional information

- How well are the people involved prepared/qualified?

- Information about susceptibility and/or toughness of the people/ elements affected
- What is important for the scenario, but not yet recorded?

2 List of dangers | Checklist

The list of dangers is the basis of risk identification. This can be divided into five areas. For each area, there will be a list of possible dangers, which have to be considered in detail.

1. Structural susceptibility of the venue

This is determined by the available area, the expected number of visitors, the entrances and available rescue options; Other factors include the general condition of the venue, the way the audience is arranged, the structures, technical facilities as well as lines of sight and acoustics.

Technical dangers

- Fire
- Explosion
- Energy supply (electricity and gas)
- Defective safety equipment
- Other technical malfunctions, breakdown of event technology
- Risk of tripping & collision
- Collapse of building components
- Breakdown and/or excessive use of visitor-related infrastructure (cloakrooms, toilets, catering, ...)
- Transmission of infections & germs as a result of excessive use of sanitary facilities
- Breakdown of fixed telephone network
- Breakdown of mobile network
- Breakdown of radio network
- Environmental damage, environmental degradation
- Noise emission
- ...

2. Weather

The weather, especially at open-air events, has a great impact on the safety of the crowd; the weather can also be relevant for indoor events, because it can have an effect on outside escape routes and on people streaming in and out.

An effective weather management system must be in place to avert dangers. Such a system consists of reliable weather observation and

defining measures, which have to be implemented when certain weather events occur. Dangers as a result of the weather

- Storm
- Hail
- Heavy rain
- Thunderstorm, lightning
- Flooding or low water
- Heat and sunshine
- Cold, black ice, snow
- Hypothermia/burning (sunburn etc.)/dehydration of people
- ...

3. **Outside influences**

Outside influences are either a deliberate attempt to disrupt the event, an accidental disruption, or they are the result of incidents that are outside the event, but have a direct influence on it. Deliberate disruptions can be caused by visitors or non-visitors; there is a wide range of possible disruptions, from booing, violence, demonstrations, blocking access to attack threats. Incidents outside the event can include a parallel event or breakdown of transport systems.

Dangers from outside

- Disruption of the event
- Vandalism, pyrotechnics
- Objects that cannot be assigned
- Bomb threat, attack threat
- Attack, killing spree
- Breakdown of transport systems
- Demonstration
- Parallel event
- Global events (attacks, weather disasters, other reports)
- Artist or guest cancellations
- Deliberate false reports of any kind
- Breakdown or excessive use of traffic routes
- Breakdown and/or traffic jam – personal traffic
- Breakdown or overly full car parks
- Blocked emergency & escape routes (parking offenders, objects, bicycles, ...)
- ...

4. Visitor composition and behaviour

The composition of visitors and their behaviour are mostly determined by what type of event it is.

Factors such as the event format, average age, visitors becoming emotionally charged by the event programme, the consumption of alcohol and other drugs all have an influence on personal behaviour.

Dangers from visitor and audience behaviour

- Unusual programme elements (e.g. candles)
- Security-relevant groups of people
- Flash mobs
- Throwing objects
- Violent people
- Climbing over barriers, destroying the surroundings
- Broken glass
- Pushing and shoving
- Overcrowding
- Visitor pressure
- Noise emission
- Crime (consuming and selling drugs, pickpocketing, sexual offences, etc.)
- Artists asking audience to do certain things (circle pits, wall of death, stage diving, ...)
- Dangerous trends (selfies at stupid places, sunburn art, ...)
- ...

Immediate danger to life and health

- Personal injuries and diseases
- Drug and alcohol abuse
- Missing person announcements
- Deaths
- Hygiene (toilets, food, ...)
- Huge number of injured people (according to DIN 13050)
- ...

5. Organisation

The required organisation, planning and management of events depends on many factors. Human error as a result of misjudgement, psychological stress, overwork and, for example, a lack of overview of the situation as a whole can all put an event at risk and endanger visitors. Other factors include spontaneous unilateral actions and

a lack of overview of the situation as a whole. Visitors can be put at risk in many different ways.

Dangers as a result of human error

- Unknown concepts
- Unclear responsibilities
- Overwork
- Psychological problems
- „Meant well – done badly“
- Lack of or inadequate communication
- Overconfidence
- Personal differences/dislikes
- ...

3 PFAC Procedure

This facility safety procedure is the German-language equivalent to the so-called HAZOP analysis. This procedure is used to assess the processes of system parts on the effects of potential deviations. The procedure is described as follows in the assessment (IVSS 2000):

P Prognosis of Disruptions

ZBreaking down the system into comprehensible functional units or sequences

Formulating associated target functions that precisely and verbally describe the observed unit as a requirement (target)

Using the key words for the target function and interpretation

A Finding the cause

A Assessing the effects

G Countermeasures

The following key words are available for the analysis according to Preiss (2009):

- none (complete negation of the target function)
- more / less (quantitative growth or reduction)
- both...and (qualitative growth)
- partially (qualitative reduction)
- inverse (the logical opposite of the target function)
- other than (complete switch, e.g. different location)

This process is used for parameters yet to be analysed (e.g. visitors, crowd density, crowd flow, heat, cold, rain, etc.). Table 2 shows an example of how this process can be applied.

Deviation	Cause	Effect	Countermeasure
Crowd flow is GREATER	People are arriving too early	Hunger/thirst	Set up aid stations
		Exhaustion	No countermeasures required
		Boredom	Entertain people/keep them in a good mood
		Need for sanitary facilities	Provide toilets
	People are not spreading out	Congestion	Crowd guidance/regulation Provide instructions
	Lack of crowd guidance	Congestion	Provide instructions
Crowd flow is Smaller	People are spreading out	No security-relevant effects	No countermeasures required
	Crowd guidance	No security-relevant effects	No countermeasures required
Temperatures are INCREASING	Sun is shining	Injuries	Provide cooling
		Thirst	Set up drink stands/distribute drinks
	Body heat among the crowd	Injuries	Provide cooling
		Thirst	Set up drink stands/distribute drinks

Tab. 2 Sample application of the PFAC process

4 Index Method

The experiential values gained from a multitude of various events can be used to develop a method that weighs various risk potentials and that inquires about the individual aspects in a questionnaire. Hereafter this will be called an index method. Attached, the Bavarian capital of Munich provides a template to document the security-coefficients of fire protection and first-aid service assessment (fire recommendation Munich, 2011). The method consists of the multiplication of the presented risk factor and the presented security factor. The result is used to determine which measures must be taken for the event from a fundamental/standard perspective. For example, if a security concept has to be compiled or if a fire protection service must be present. In order to compile such a method the organiser must have experience with the most diverse range of events. Furthermore, the process must first be thoroughly tested before it can be used as the sole instrument for assessment. It is beneficial if the responsible authority provides such a process for the organiser. It is thus also useful for inexperienced organisers. However, it is only conditionally applicable, as it can only present a small portion of the risks to be considered.

5 Bow-Tie Analysis

The bow-tie analysis consists of a simplified fault tree analysis and

a simplified event tree analysis (s. Fig. 10). The two methods are connected by a core point, the so-called top event, so that the result of the fault tree analysis is the starting point of the event tree analysis. The graphic depiction is reminiscent of a bow-tie, hence the method's name. The fault tree analysis is used to find causes and cause combinations of undesired events (top events). Attached to the top event is the event tree analysis, which is used to convey the subsequent events. These processes are supplemented with the description of security barriers that disrupt the chain. The purpose of the bow-tie analysis is the depiction of the components of security management to avoid incidents (fault tree) and restrict the effects thereof (event tree).

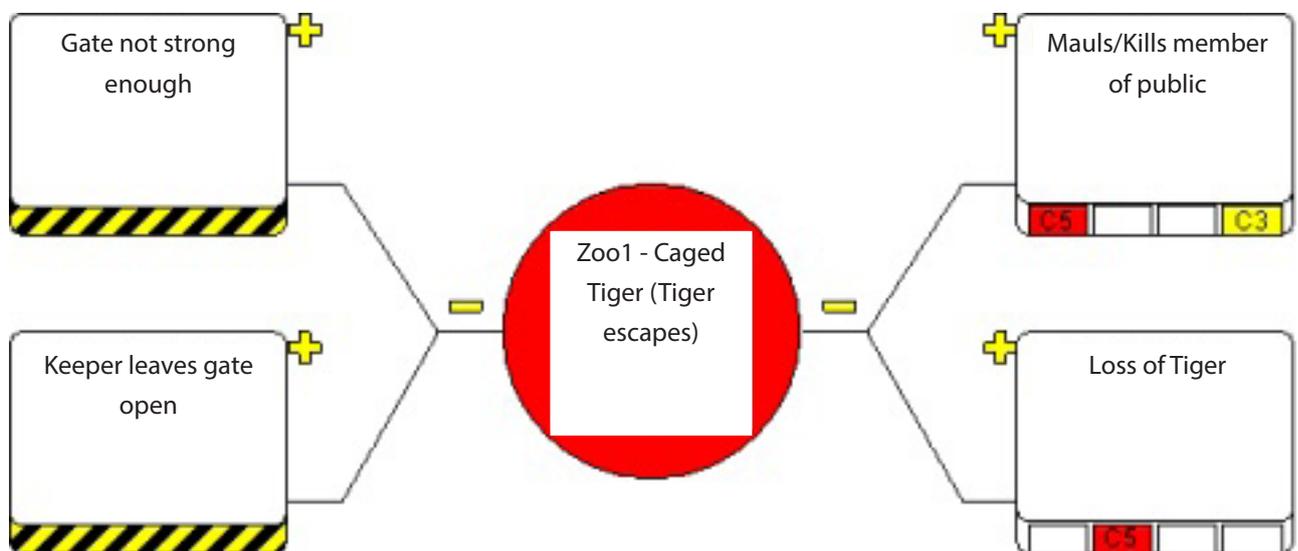


Fig. 11 Bow-tie analysis (http://www.bowtiepro.com/bowtie_process.asp)

This process cannot identify risks, which requires experience on behalf of the organiser so that they can implement the security barriers and assess the effects. The application of this method is not as intuitive as using the risk matrix, and must thus be tested. It may facilitate the determination of security barriers, and the systematic usage of the method may determine additional potential effects.

The process of this method is as follows:

- Step 1 Definition des Top-Events. Der erste Schritt bei der Methode ist die Defining the top event. The first step of this method is the definition of the top event, e.g. the tiger's escape from its enclosure at the zoo.
- Step 2 Assessing the causes. The second step is identifying the causes. In this case, the possible causes could be that the cage is not properly sized or a caretaker left the door open.
- Step 3 Assessing the effects. In this step the effects should be determined. To keep with the same example, it could be possible that a person or the tiger will be injured.

- Step 4 Determining the proactive security barriers. The proactive barriers are analysed here. These should prevent the top event from occurring, e.g. the door closing on its own or an alarm sounding when it does not close.
- Step 5 EDetermining the reactive security barriers. Then the reactive barriers are determined, e.g. the tiger is tranquilised with a dart or shot.
- Step 6 Identifying disruptions in the security barriers. This step is about identifying the extent of the factors that can disrupt the efficacy of the security barriers. A disruption may be a defective electrical connection or a self-closing door, for instance.
- Step 7 Identifying barriers against the possible disruptions of the security barriers. Once again, this step concerns barriers that counteract a disruption. In this case the closing mechanism could be regularly maintained. It is recommended that as many security barriers as possible be implemented to prevent this disruption. This process is also recommended in the risk management of patient safety in hospitals, where it is referred to as the Swiss cheese model (Tönneßen, 2009).

6 Swiss Cheese Model/LOPA (Layer protection analysis)

This model is based on the assumption that work in a specialised and complex system facilitates errors. Defects in organisation and communication can lead to more frequent errors. Multiple consecutive security barriers, shown like slices of Swiss cheese, should prevent the occurrence of errors.

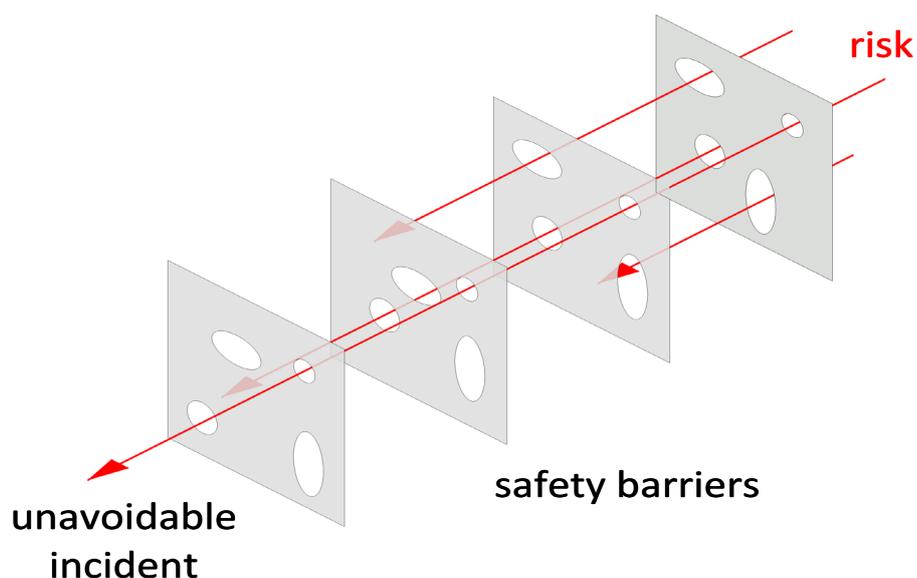


Fig. 12 Swiss cheese model

However, if the security barriers are not yet properly arranged or too

few security barriers are planned, an error may still slip through the security barriers and lead to an undesired situation or effect.

Scenarios from different danger analyses (e.g. from the PFAC process) are needed to use this model. A scenario begins with the triggers (triggering conditions) and severe consequences must now be prevented using various security barriers. Preventative measures (prevention) should prevent the occurrence of damage (e.g. injury from severe crowd pressure); reactive measures (mitigation, emergency response) serve to limit the damage.

The Swiss cheese model and bow-tie analysis thus complement each other. The permit-granting authorities are recommended to arrange the security discussion after the steps have been taken to conduct a bow-tie analysis, especially with inexperienced organisers, in order to identify the causes, effects, and security barriers. Only then can the organiser implement the resulting knowledge in the event planning and execution.

C.2 Assessment of the First-Aid Station

The first-aid team / resources can be assessed using various first-aid algorithms. The most well-known currently are the Maurer and Kölner algorithms. However, algorithms do not sufficiently consider the event- and location-specific details, which generally result in deviations from the purely statistically calculated defaults.

The local situation and special features of the event, as well as experiential value from past or related events, must be considered when determining the quantitative and qualitative arrangements of manpower and resources. Considering these parameters allows for an objective estimation of the actual needs, which may deviate from the calculation provided by the purely mathematical method.

The assignment/command prompt for the first-aid station should comply with the stipulations of the non-police hazard prevention (regulation 100 „Guiding and leading when deployed“), when structure and content are concerned

C3 Security service

Assessing the security service using an algorithm (i.e. based on clearly defined individual steps which, by entering individual values, yield one or more output values) turns out to be too complex given the currently available methods.

In order to nonetheless be able to assess the steward and security service using a reliable method, below we will describe an approach where various parameters (which the assessment is largely contingent on) are considered and evaluated individually.

This is the easiest way to achieve the objective of reformulating the complex requirements of an event with regard to the steward and security service using measurable quantities and numerical values.

Four features are defined as parameters, which are considered in detail and taken into consideration when drawing up the assessment:

1. **Feature: fixed positions**

Fixed positions must always be staffed; they are spatially limited and are important for property security, when controlling flows of people, vehicle movements and for management duties.

Examples of fixed positions:

- Control centres – radio control units
This is the workplace of the heads of operation and security operation managers (for example), who always have to be in contact with the organiser, the operator and the authorities and organisations with security responsibilities.
- Buildings – property security
The main task is to secure the property against unauthorised access and against people climbing up the buildings or the technical facilities; the lower the safety precautions of the building, the more staff is required.
- Entrances and exits with flows of people
This includes entrances for visitors with the necessary checks (admission control), providing security for entrances to the production and VIP areas (entry control) and securing the emergency exits as well as escape routes and rescue routes such as stairs on grandstands.
- Access and exit roads with vehicle movements

Examples include access roads to production areas or roadblocks. The number of staff mainly depends on the type and extent of the vehicle checks. These positions have to be differentiated from the tasks of car park and traffic management.

2. **Feature: mobile positions**

Mobile positions are not tied to a fixed location; they are either allocated to a spatially limited area or to certain tasks. Examples of mobile positions:

- **Securing barriers**
Boundaries between different areas separated by barriers (site fence, police barrier, stage barrier) must be supervised by staff. The number of staff depends on the type of barrier and the number of expected visitors; depending on needs, patrolling may be enough or a permanent presence.
- **Personal protection and escort protection**
Artists or VIPs, especially if they are in direct contact with the audience, and individuals with safety classification require special protection.
- **Transport of cash and valuables**
Transports of cash boxes, valuable exhibits, documents, etc., have to be accompanied to prevent robbery or theft; in the case of particularly valuable items, armed security guards may be required.
- **Staff for special deployment (sfsd)**
Intervention and reserve staff are deployed where existing staff need support or new tasks arise that could not be planned in advance.

3. **Feature: management structure and organisation**

All members of the security organisation must be allocated to their field of activity, their role and the associated qualification.

- **Spatial allocation**
For larger events, the event area is divided into sections which in turn can be divided into subsections. Within the sections, teams are formed that consist of a group of employees. For fixed meeting places or smaller events, the structures are adapted accordingly.
- **Role of staff**
Within the organisation the staff members assume different roles; here, a hierarchical system with four organisational levels has become established:

1. **1st level: Security operation manager**
The level on which decisions are coordinated with the organiser and that directly communicates with security and coordination staff
2. **2nd level: Section head/ supervisor**
The level that is in charge of preparing decisions on the operational level and supervises their implementation in accordance with the defined areas (e.g. there is an area manager for a southern and a northern area)
3. **3rd level: Subsection head**
The level on which the areas were further divided into smaller units. For example, there is a section head for the entrances, one for security in the backstage area or for the car parks
4. **4th level: Task force, security guard, assistant, evacuation helper**
The individual security guard, managed and instructed by the subsection head or, if the subsections are larger, by a team leader

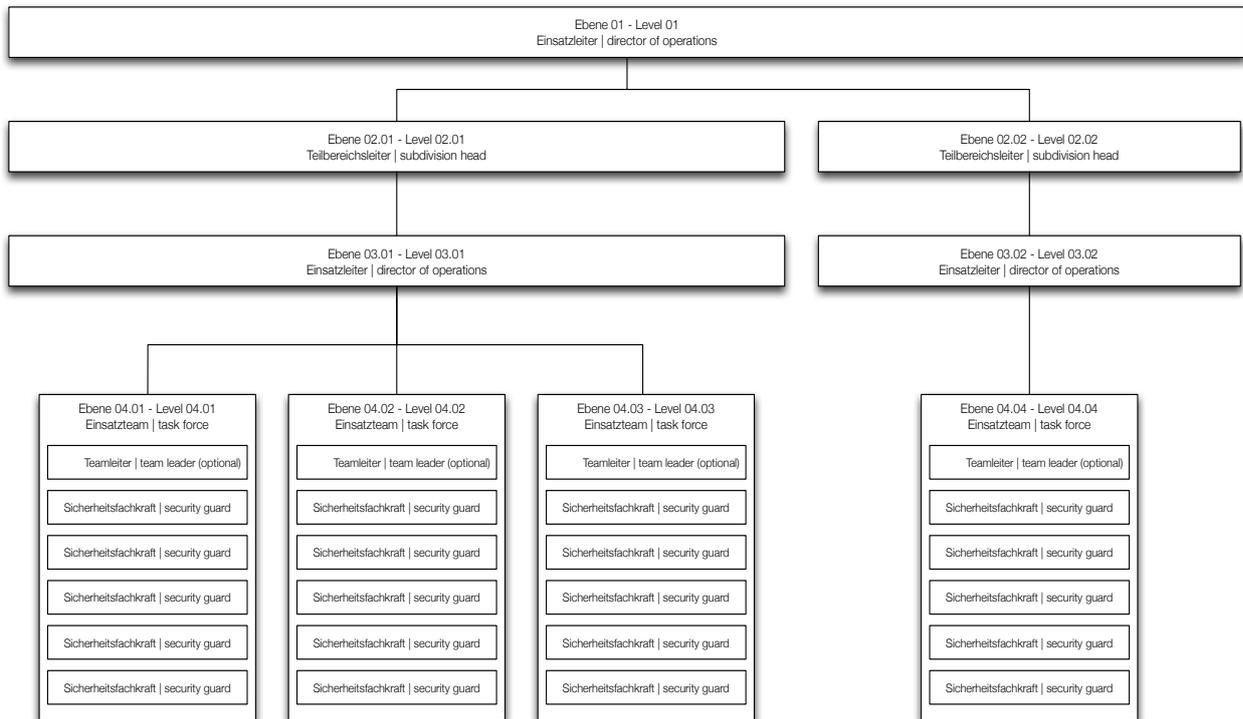


Fig. 13 Levels for the structuring of the steward and security service

- Qualification
The role of the employee within the security organisation as well as legal requirements (e.g. trade regulations, security services act, weapons act) determine the minimum qualification of the employee. Staff without special qualifications can also be used (e.g. parking attendants, ushers or volunteers), but their work has to be specified and if necessary coordinated with the authorities. Examples of qualifications of stewarding and security staff:

- training according to the law
- certified protection and security officer
- certified master of protection and security
- Specialist for visitor safety

In addition, they need to have special qualifications to perform certain tasks, such as in fire protection:

- Operational self-help officer (evacuation helper, fire protection assistant)
- Intervention officer
- Weaponry expertise exam

4. **Feature: time schedule**

The scope of the job and the place where the staff work are based on a time schedule. It has proven useful to plan and divide an event in different phases; there are different guidelines and instructions for the staff in the different phases. The time schedule could be as follows:

- **Assembly and disassembly**
Other assessment factors could be phases with and without assembly tasks or the progress of the assembly work (e.g. erecting structures).

- **Rehearsals**
The mere presence of artists can mean additional manpower. For public rehearsals with audience or if the rehearsals for events in a public place are a visitor magnet, manpower planning has to be adjusted accordingly.

- **Event**
The event should be divided into different time periods in order to be able to better plan staff positions and number of staff.

An example of how an event could be divided:

1. Phase – visitor influx, arrival of artists
2. Phase – admission
3. Phase – main programme
4. Phase – visitors leave, artist(s) depart

- **Other assessment factors**
Taking into account the above four features, it should now be possible to perform a quantitative and qualitative assessment of the steward and security service. However, there are additional factors that have a significant influence on the assessment other than the above features.

Other factors influencing the assessment may be the existing fire protection, evacuation and security concepts, the organiser's need to maintain their reputation, the current security situation and, last but not least, the regulations of the authorities who approve the event.

5. Position plan

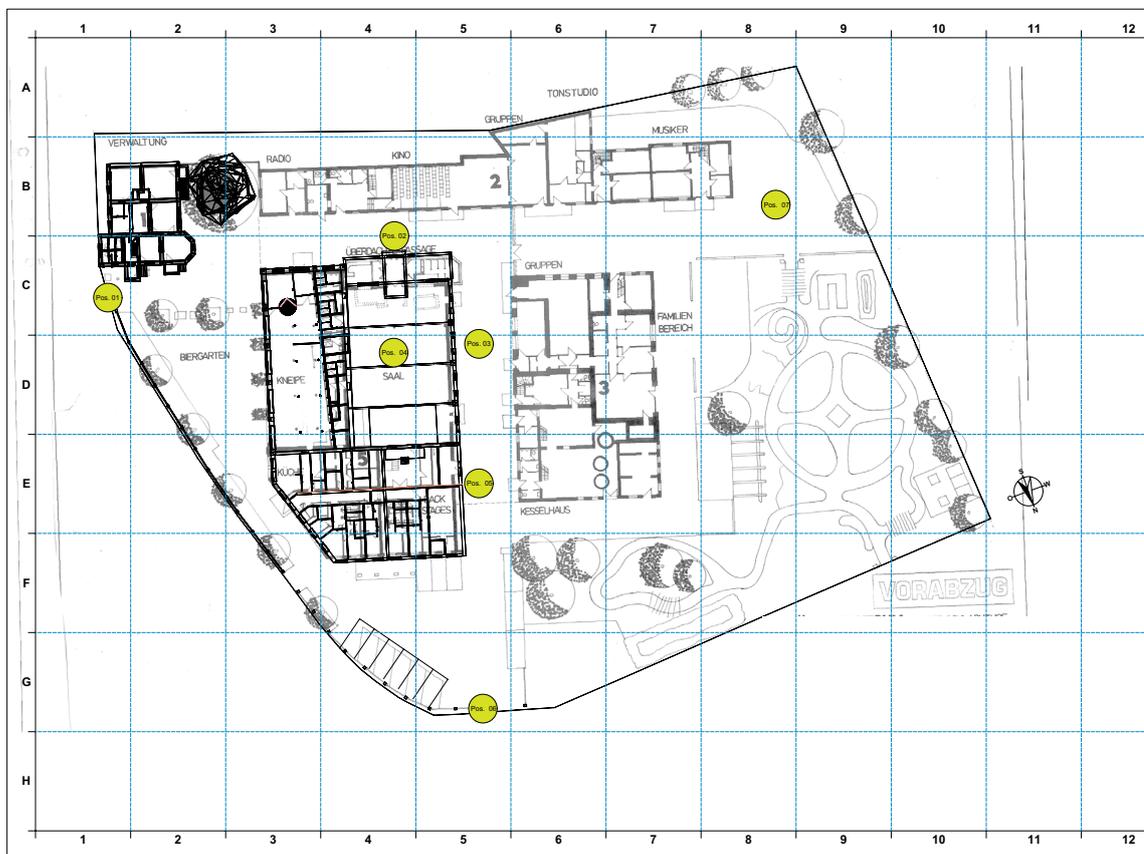


Fig. 14 Position Plan

5. Briefings and work instructions

The above method for assessing the steward and security service defines a clear organisational structure as well as specific tasks.

To ensure that the individual organisational levels work well together and the staff are able to work purposefully, all staff have to be provided with information necessary for operations. Staff are generally provided with the relevant information in the form of a briefing or a work instruction; this can either be done verbally or in writing.

The special briefings for the steward and security service must be synchronised with the briefings and work instructions for the event or the assembly venue, such as for fire protection, occupational safety and health protection as well as weather management.

It still makes sense to brief staff on the levels 1 to 3 and as part of the advance briefing; however, from level 4 and in the operational units the extent of the personal briefing increases disproportionately and the important and useful information has to be separated from the unimportant and redundant. Since events are open and dynamic systems, it is not possible to take into account all possible disruptions in the briefings.

Briefings therefore have to be drawn up such that they provide clear specifications for standard processes as well as instructions on how to act when the situation is not clear.

At the time the briefing is drawn up, all relevant information should be available if possible, and it has to be completed so that it can be passed on to the staff in good time before the event.

The briefing can be drawn up based on the following principle:

- Who does what, when, where, how and why?

A distinction must be made between

1. a general briefing, and
2. a work instruction based on position

The following can be used to draw up a briefing or a work instruction:

Defining the assignment

- Description of tasks and associated objectives
- Description of specifications and limits
- The correct behaviour in an emergency and unusual or ambiguous situations, interfaces to BOS

Description of site, position and other circumstances

- Site plans (e.g. building or site plan, escape and rescue route plan)
- Description of event site, dividing the event site into sections and explaining the sections in detail
- Position plan
- Signposting plan, roadblock plan
- Access permissions, ID

Time schedule

- Construction schedule, rehearsal plan
- Event schedule, programme, disposition

Organisation

- Communication channels and means (e.g. radios and their use)
- Responsibilities, instruction and reporting channels
- What to do at the start and at the end of work
- Information about occupational safety and health protection
- Dress code

Proof of briefings and work instructions should be documented.

Debriefing

After the event a debriefing may be carried out; here, the employees' experiences and insights are gathered, discussed and evaluated.

Reasons for debriefings can include:

- Regular monitoring of current manpower planning
- Identifying positive and negative influences on the assignment
- Improving future operations and work processes
- Drawing conclusions for the planning and implementation of follow-up events
- Comparing experiences with other departments or service providers

C4

Structural complexes, based on the German building code (MBO) must be arranged, erected, changed and maintained such that public safety and order, especially life, health and the natural bases of life, are not endangered. Furthermore, structured complexes must be such that in case of fire people and animals can be rescued and effective fire-fighting operations can be performed.

The corresponding regulations for places of assembly contain the

model ordinance governing places of assembly deals with the routing and dimensioning of escape and rescue routes as well as the request to draw up an evacuation concept when there are more than 1,000 visitors and definitely requires a security concept when more than 5,000 people come together.

The German building code allows you, in individual cases, for special structures a deviation from the general regulations regarding fire protection systems, facilities and precautions. In addition to complying with building regulations regarding permissible rescue route lengths and the required exit widths, for buildings which are regularly used by a large number of people, evacuation calculations are recommended as part of an integrated fire protection concept.

The same applies to special structures, especially in the case of the above-mentioned deviations, and in both areas this is kept as evidence with the help of so-called engineering methods. Information is available from the „vfdb guideline on engineering methods of fire protection“ | TB04-01; 11-2013.

The comment for the regulations for places of assembly also contains a reference to evacuation simulations: „[...]In the case of complex places of assembly, an evacuation simulation may be necessary.[...]“.

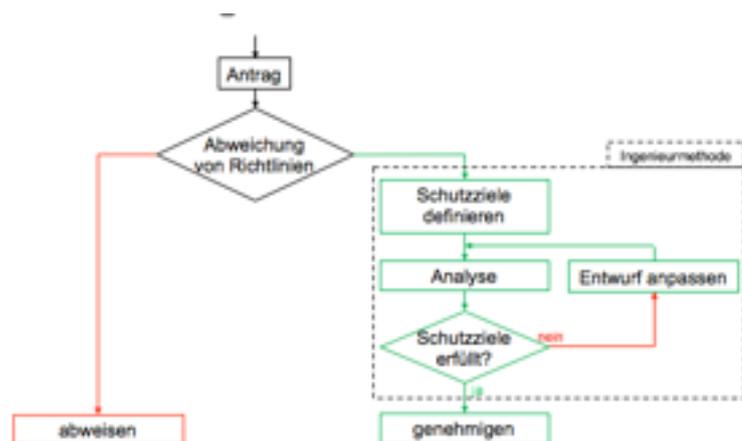


Fig.. 15 Vorgehen bei Abweichung von den allgemeinen Vorschriften im Einzelfall

A people flow analysis can be useful in the following cases:

- Reviewing the evacuation concept
- Compensation, equivalence proof in the case of non-compliance

with standards , e.g.

- Escape routes not wide enough
- Escape routes too long
- Approved number of people exceeded
-

Uncovering critical points

Virtually testing what-if scenarios (e.g. rescue route unavailable, uneven distribution of visitors on event site)

Assessing capacity limits

The aims of an evacuation calculation include:

To (statistically) determine the overall time it takes to evacuate the building or the time its takes to evacuate structures or parts thereof and analysing this taking security-specific aspects into account.

Providing proof in individual cases that the planned or existing escape and rescue routes are sufficient despite deviating from the size requirements laid down by the building law or the MVStättVO.

To show that the escape arrangements are sufficiently flexible in the event that certain escape and rescue routes or secured areas are not available due to an incident.

To identify as much as possible significant congestion that can occur during the evacuation due to the normal movement of people along the escape and rescue routes.

The most common analysis methods can be subdivided into a macroscopic and a microscopic approach. The macroscopic analysis maps the movement of persons as collective flows, from which the duration of the egress process and the congestion points can be calculated by means of a manual calculation scheme (e.g. applying the Predtetschinski-Milinski-Method with the help of a spreadsheet-program). For microscopic analysis, computer programs are used to simulate the movements and interactions of all individual person. In addition to the duration of egress and areas of congestions, these simulations consider the time dependent evolution of the evacuation process on an individual level. Therefore, the user can visualize and analyze the progress of egress at any time, which also provides a more realistic insight into the evacuation dynamics of complex buildings and terrain structures.

The use of computer-based methods for evacuation verification creates new challenges for the building supervisory authority. Standardised criteria are needed for the scenarios and parameters assumed when performing a people flow simulation in particular. The same applies to the assessment of the reliability and accuracy of software programs. In this regard, the RiMEA guideline is a good reference work – both for the creators of such analyses and for officials. (RiMEA guideline, version 3.0) It must be understood that people flow analysis cannot take into account

- all real-life influences. Psychological aspects, such as those that influence choice of route and the
- behaviour of individuals, have so far not been thoroughly scientifically investigated and can only be approximated by using assumptions and different scenarios. A simulation is thus an idealised case, where individuals move in accordance with the user's parameters and route specifications. Making calculations with different specifications also allows us to make an assertion about the range of these influences and thus the robustness of the results, which are essential for the implementation of a security concept.

Input parameters for the simulation of flows of people:

To perform a simulation, the following input values should be available:

- Formulation of the question
- People's space requirement
- Demographics
- Escape route allocation, escape route choice (e.g. escape route plan)
- Distribution of people on the area to be simulated

Formulation of the question

Before a simulation is carried out, the question that should be answered by means of the simulation should be clearly stated. Only then are the results of benefit and can help with the planning of the event.

Demographics

The age distribution of the population has an influence on the walking speed of the agents.

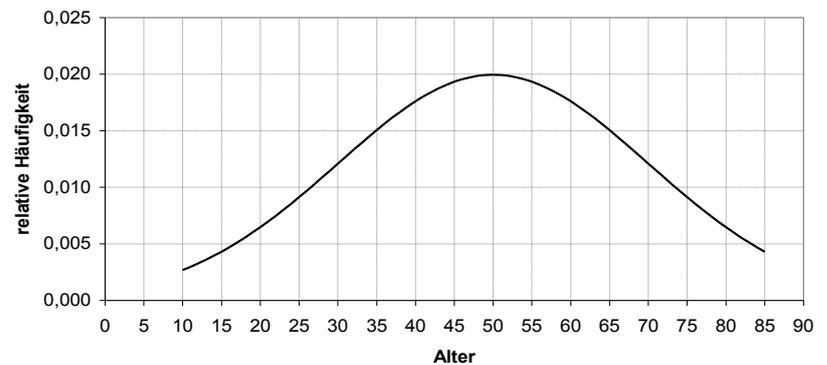


Fig. 21 Age distribution of the RiMEA standard population, which consists of 50% men and 50% women

Please note:

If no data are available, the following standard population should be used. It consists of 50% men and 50% women whose ages, as shown in Figure XX, are normally distributed between the minimum and maximum value. The mean age is 50 years; the standard deviation is 20 years. The minimum age is 10 years, the maximum age 85 years.

People's space requirement:

Depending on occasion, time of year, type of event, the model must include different space requirements for people. Weidmann (1993) has developed guidelines.

Walking speed on flat ground

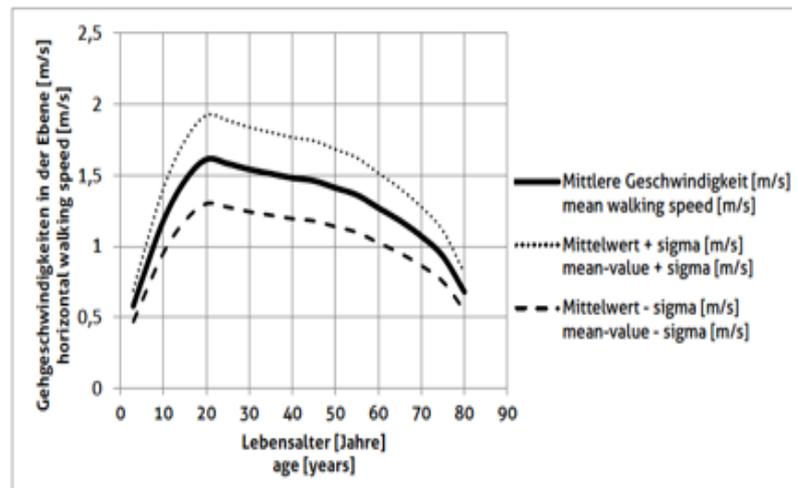


Abb. 22 Walking speed on flat ground depending on age, following Weidmann

On average, the walking speed of men, according to Weidmann, is 10.9% higher than that of women. For men, this means a mean free walking speed of 1.41 m/s and for women of 1.27 m/s. Walking speed on flat ground (m/s) of persons with impaired mobility
Minimum: 0.46 m/s Maximum: 0.76 m/s

Walking speed on stairs

Group of persons	Mean walking speeds on stairs (m/s)			
	downstairs		upstairs	
Under 30 years of age	0,76	0,81	0,55	0,58
30 to 50 years of age	0,65	0,78	0,50	0,58
Over 50 years of age	0,55	0,59	0,42	0,42
Persons with impaired mobility	0,42		0,32	

Tab 4 average walking speeds on stairs, following Fruin

Please note:

Walking speed on stairs can either be identified through speed distribution

or a reduction in speed. Simulation models must sufficiently and accurately take into account the trends described in the literature. In

a simplified way, walking speed on stairs can be calculated based on horizontal components in both directions (up the stairs and down the stairs) corresponding to half of the walking speed on flat ground (Figure XX).

Distribution of people on the area to be simulated

People densities:

Building type	Density of persons (persons/m ²)	Source
Department store	0,18 - 0,36	NFPA 101
Office building	0,11	NFPA 101
Warehouse	0,04	NFPA 101
Trade fair	1,00	MVStättV
Meeting rooms	2,00	MVStättV
Standing areas in spectator facilities	3,50 - max. 4,70	DIN EN 13200

Tab. 5 Guide values as densities for the initial distribution of the population

Please note:

The initial distribution or number of people specifies the basis for which people densities or numbers or which seating or layout plan must be distributed at the beginning of the simulation. If specific data are available, they should be included in the analysis (stating the source).

The age distribution of the population has an influence on the walking speed of the agents.

Escape route allocation / escape route choice (e.g. escape route plan)

A goal must be assigned to each agent of a simulation. This goal assignment can either be done using an existing escape route plan (e.g. to review evacuation concept) or based on other criteria, such as the fastest route out of the building, escape route = entrance. The assignment and the reason must be comprehensively documented.

Hinweis:

The results of the numerical calculations must reflect in a qualitatively correct way the interdependencies between people densities ρ [people/ m^2] and the reduced walking speed v [m/s] when densities are higher (left diagram). The specific people flow J_s [people/ (m s)] based on the fundamental diagram (right diagram) in particular specifies the achievable throughput of people as a result of constrictions

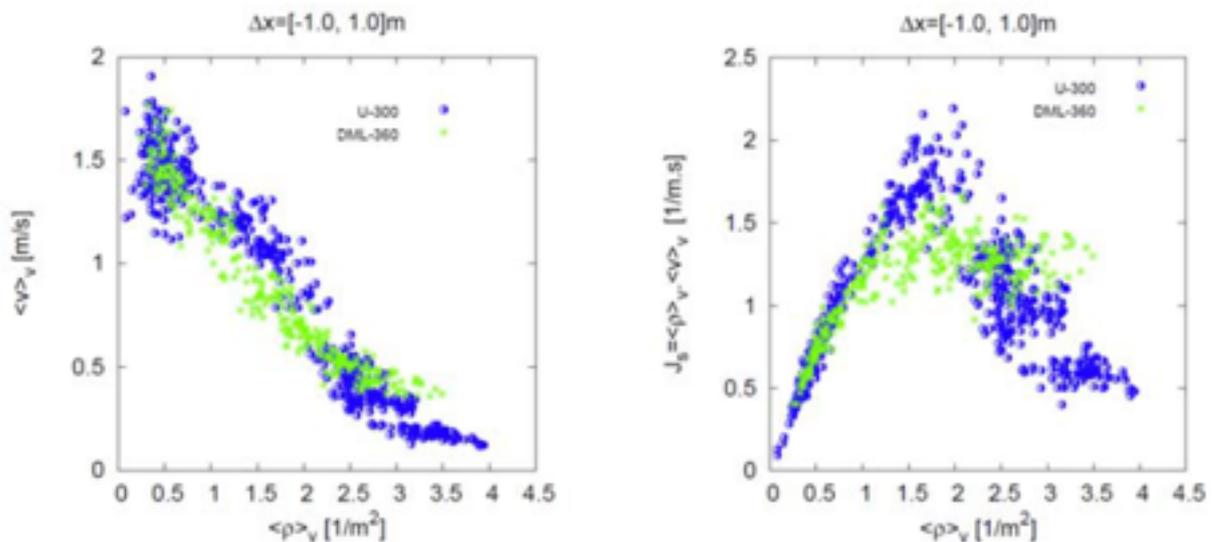


Abb. 23 experimentally determined fundamental diagrams for a unidirectional (blue) and a bi-directional (green) flow of people (source: Jun Zhang; A. Seyfried; Jülich 2014)

More information can be obtained from the guideline for microscopic evacuation analysis – version 3.0 dated 10/03/2016. www.rimea.de

Literature and References

D

D Literature and Reference

Fuhrmann, Ursus (2011): Beitrag in Tagungsband Forum
Veranstaltungswirtschaft, Baden-BadenDPVT

Maunz/Düring (2012): Grundgesetz-Kommentar. 66.
Ergänzungslieferung, Rn 154. München: Beck Online

Compes: Modell zur Unfallkausalität und zum Störfall im
„Mensch-Umgebungs-System“

DIN ISO 31000:2011 (Entwurf)

Abschnitt B der Bundestagsdrucksache 13/3540: Begründung zum
§ 4 des ArbSchG DIN ISO 31000:2011 (Entwurf)

Starke/Scherer/Buschhoff (2007): Praxisleitfaden
Versammlungsstättenverordnung, xEMP, Berlin

Starke/Buschhoff/ Scherer (2006): Pocketguide Sport Events, xEMP,
Berlin

Buschhoff/Scherer (1/2013): Besuchersicherheit als oberste Maxime,
in „Stadt und Gemeinde“,

Buschhoff/Scherer (09/2014): Die Kultur der Verantwortung als
Baustein einer sicheren Veranstaltung, DStGB, Stadt und Gemeinde

Maurer, Jürgen: Sicherheit ohne Angst: Terrorismusbekämpfung im
21. Jahrhundert, Mainzer

Daase, Christopher: Der erweiterte Sicherheitsbegriff

Daase, Christopher: Bedrohung, Verwundbarkeit und Risiko
in der „Neuen Weltordnung“. Zum Paradigmenwechsel in der
Sicherheitspolitik, in: Antimilitarismusinformation, Jg. 21, Nr. 7,
S. 13–21

Wolfers, Arnold (1962): „National Security as an Ambiguous Symbol“,

Was sind komplexe Systeme? Komplexität als integrative
Wissenschaft, Grundlagentexte zur integrativen Wissenschaft,
Prof. Dr. Klaus Mainzer,

URL: [http://www.integrative-wissenschaft.de/Archiv/dokumente/
Mainzer-14_10_04.pdf](http://www.integrative-wissenschaft.de/Archiv/dokumente/Mainzer-14_10_04.pdf)

Ziegler, Holger: Prävention – vom Formen der Guten zum Lenken
der Freien, in: Widersprüche, Zeitschrift– Hefte – Heft 79

- Bröckling, Ulrich: Dispositive der Vorbeugung

Meyer König et al. (06/2015): Und sie bewegen sich doch, Menschen bei Veranstaltungen sicher und komfortabel lenken, 1. Auflage, xEMP

Fekete: Ziele im Umgang mit „kritischen“ Infrastrukturen im staatlichen Bevölkerungsschutz

Preiss, R. (2009): Methoden der Risikoanalyse in der Technik. Wien: TÜV Austria

International Electrotechnical Commission (2009): IEC/FDIS 31010 Risk management – Risk assessment techniques

Branddirektion München (2012): Sicherheit von Veranstaltungen – Teil A: Handreichung für Veranstalter, URL: https://www.muenchen.de/rathaus/dms/Home/Stadtverwaltung/Kreisverwaltungsreferat/fachspezifisch/HA-IV/Dokumente/VB/Veranstaltungen/Sicherheit_Grossveranstaltungen_A_Veranstalter.pdf, Stand: 30.10.2014

Branddirektion München (2011): Sicherheitsrechtliche Beurteilung und vorbeugender Brand- und Gefahrenschutz bei Großveranstaltungen – Anlage 1: Vorlage zur Ermittlung des Sicherheitskoeffizienten Brandschutz und Sanitätsdienstbemessung, URL: http://www.agbf.de/pdf/Vorlage_zur_Ermittlung_des_Sicherheitskoeffizienten.pdf, Stand: 30.10.2014

IVSS (2000): Das PAAG-Verfahren – Methodik, Anwendung und Beispiele. Internationale Sektion der IVSS für die Verhütung von Arbeitsunfällen und Berufskrankheiten in der chemischen Industrie. Heidelberg: IVSS

http://www.bowtiepro.com/bowtie_process.asp, Stand: 30.10.2014

<http://www.aerzteblatt.de/bilder/2011/01/img151626.gif>, Stand: 30.10.2014

International Organization for Standardization (2009):

ISO 31000 Risk management – Principles and guidelines

- drawing Evacuation calculations | pedestrian flow by Dr. Tim Meyer-König, TraffGo HT GmbH and by RiMEA e.V.