Bundesamt
für Sicherheit in der
Informationstechnik

Analysis of Critical Infrastructures
- The ACIS methodology -

(**A**nalysis of **C**ritical **I**nfrastructural **S**ectors)

Developing an awareness of the challenges entailed in the protection of Critical Infrastructures is an important first step. Before one can take effective measures to improve the protection of Critical Infrastructures, it is necessary to understand how these function and to identify and analyse the critical processes within the Critical Infrastructures. The ACIS methodology described in this paper is intended to facilitate this task.

1. Protection of Critical Infrastructures – the challenge

Today's society depends strongly on the smooth functioning of information technology. Recognition of this fact is not confined to the experts. Demands for the continuous availability of information and the preoccupation with raising economic efficiency specifically encourage still greater reliance on information technology.
Many nations have conducted studies and initiated programmes aimed at analysing these dependencies and assessing the possible consequences. Measures aimed at protection from and rapid recovery after damaging incidents are being developed in partnership with industry. As part of this exercise, "Critical Infrastructures" have been identified. These are the infrastructures on which the smooth functioning of society is particularly dependent. In the case of Germany, the federal government has come up with the following definition:

> "Critical infrastructures are organizations and institutions that are important to public welfare; such that failure or disruption of them will result in long-lasting supply bottlenecks, significant disturbances in public security or have other dramatic consequences."

According to this definition, the following infrastructural sectors count as "Critical Infrastructures" in Germany:

- transportation & traffic
- energy
- hazardous materials
- telcommuniations & information technology
- finance & insurance
- services
- public administration & justice system
- other (media, major research establishments,cultural assets)

However, this way of looking at things merely establishes that a breakdown of these infrastructures may be expected to have serious consequences for the population. No statement has yet been made as to how such a breakdown could come about or quantifying its probability. This is where the “Analysis of Critical Infrastructural Sectors” (ACIS) methodology developed by the German Information Security Agency (BSI) in 2002 comes in. This methodology is outlined below.

2. Introduction to the ACIS methodology

2.1. Risk analysis versus assessment of criticality

Analyses aimed at identifying the probabilities of failure and their possible consequences and damaging effects typically fall into the specialist area of risk analysis and risk management. There are many different methods of conducting a risk analysis, both in the area of IT security and also in a business context. Frequently these entail a very similar structure under which objects, threats, vulnerabilities and probabilities are catalogued and links between them are defined. The outcomes of such methodologies are quantifications of the losses that may be expected or categories of risks.
However, these methods are not sufficiently focused to be helpful with regard to the analysis of Critical Infrastructures. At present no useful statistics for possible damage and failure probabilities exist, and it would appear that there is no way of cataloguing objects, vulnerabilities and threats from the perspective of individual businesses through to the economy at large.
A modified analytical approach in the form of an “assessment of criticality” has therefore been adopted.
The starting point here is the business processes that are found in the infrastructural sectors and in businesses. These are considered at a very high level. Examples of business processes include the provision of cash to the public in the financial sector and invoicing in virtually every sector.

In this context it is not relevant who or what is threatening the functioning of these processes but simply whether it is possible for a given process to be massively disrupted or rendered inoperative. Thus, for example, we are not concerned with the question of how the operation of a computer centre might be disrupted, but rather with the impact that failure of the computer centre has on the relevant process.
Using relatively high-level modelling of business processes, it is possible to work in an object-independent manner that does not require either that computer systems are listed or that extensive catalogues of damage types are created. Only the core components of the processes are considered.

2.2. “Critical” and “criticality”

To understand the methodology, it is necessary to appreciate the distinction between the terms “critical” and “criticality”.
A “critical” infrastructural sector is one whose disruption would have a serious impact on the public. But a business process in an enterprise is also referred to as “critical” if its disruption would jeopardise the survival of the enterprise. The term used here is “business-critical”. The possibilities can be reduced to a “Yes/No statement”.
“Criticality” on the other hand can be represented on a graduated scale. For example, a process can have either a high or a low “criticality”. Here the probability and the expected consequences of failure are assessed.
The terms “critical” and “criticality” can be applied at different planes of reference. Thus, an infrastructure whose failure endangers the continued existence of an enterprise is a “business-critical infrastructure”. A process with these characteristics is a “business-critical process”.
But how does the failure of a business-critical process affect the sector or society at large?

To answer this question it is necessary to consider some other factors as well. The failure (of the services) of a single enterprise may have no relevance to society. However, at this abstraction level it could lead to massive harm if the enterprise under consideration has a large market share in the sector, for example, or is the sole provider in the sector. Accordingly, the individual terms must also be defined for the abstraction levels sector and society.
Here one would expect that although there may be a large number of business-critical processes, only relatively few sector-critical processes exist. Since, however, the failure of one sector generally also poses a massive problem for society, the number of sector-critical and society-critical processes will be virtually identical.
Now that we have explained the meaning of these terms, the key question that runs through the entire methodology should also be clear:

> "What are the critical processes in the critical infrastructural sectors and what is their criticality?"

3. The ACIS methodology

The ACIS methodology always refers to the analysis of a single sector. Figure 1 illustrates the general process.

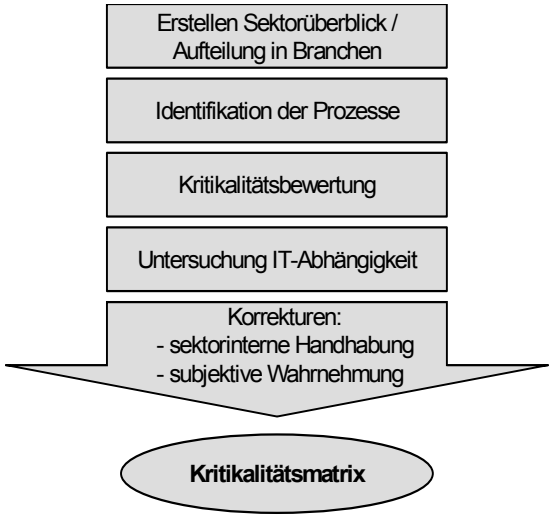

Figure 1: ACIS procedure

It is necessary first to gain an overview of the sector and then to break this down as appropriate. The critical processes must now be identified and their criticality assessed. The processes whose criticality is significant or high are then examined in terms of their dependence on IT. The next stage is to consider how the sector already deals with these critical processes, following which a criticality matrix is drawn up.

The various steps outlined above will now be explained in more detail.

3.1. Preliminary work

The first step involves two important tasks. First of all it is necessary to describe the sector under examination in appropriate detail. This entails, for example, explaining how the sector functions, what the influencing parameters are in this particular sector, how important the sector is to the economy and who the major players in this sector are.
Moreover, in many cases it is not sensible to analyse a sector one unit. Thus, for example, in the transport sector we have to consider both road traffic and aviation, i.e. two industries that have quite different structures and requirements. The sector to be examined must therefore

be further structured.

A number of different models are available here. In each case their suitability will depend on the sector concerned.

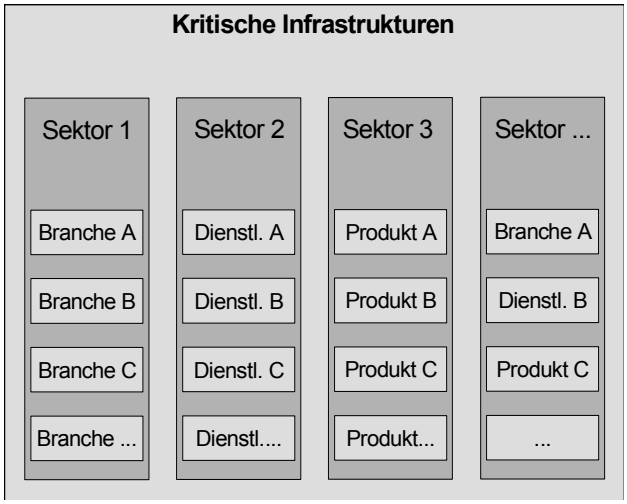

Figure 2: sector structures

The set of Critical Infrastructures can be subdivided into individual infrastructural sectors, such as telecommunications or energy. These sectors can then be subdivided in turn, for example into industries (for example, in the case of transport, into aviation, shipping, road transport and rail transport), into services (this breakdown is appropriate in, amongst other areas, telecommunications, where we have landline voice services, mobile voice services and broadband cable services) or, quite generally, into products. Which of these possibilities is appropriate for our purposes will depend on the sector concerned. Combinations of the various subdivisions are also possible.

3.2. Identification of business processes

Having arrived at this structure, the business processes that are relevant to the various industries, services and products must be identified and defined. These should then be assessed for their criticality.
This step is important for the overall analysis. Processes that are not considered here will not be relevant to the assessment of criticality either. If on the other hand the definition of processes has been carried out at too low a level and in too much detail, the result will be that a huge number of processes is identified, so that there is a danger that the wood will get lost among the trees. The amount of work involved will also rise enormously.
A number of aids are available to help identify the processes. In particular, in sectors that are very important to the economy process models have already been developed by academics. These should be supplemented as appropriate by consulting with experts. In other sectors, for example, the emergency services and public agencies/public administration sectors, generally experts are the only available source.
In this context, an expert is a representative of an enterprise or public agency from the relevant industry who is actively involved in the processes and hence can draw directly on personal professional experience.
Different industries require that experts are consulted in different ways. In some industries, workshops can produce rapid and valuable results, while in others further information that is especially important when it comes to the assessment of criticality can be gained only from personal interviews. It is important to the success of the analysis that the contributors are assured that the information they provide will be treated in confidence.

The processes identified must be described at a high level. As the individual processes are usually implemented differently in different enterprises and we are aiming with this methodol-

ogy to arrive at a view of Critical Infrastructures which is valid across sectors, detailed, scientifically accurate definitions are not required at this point.
As an example of a process as described above, let us consider petroleum supply, which falls within the wider energy sector.

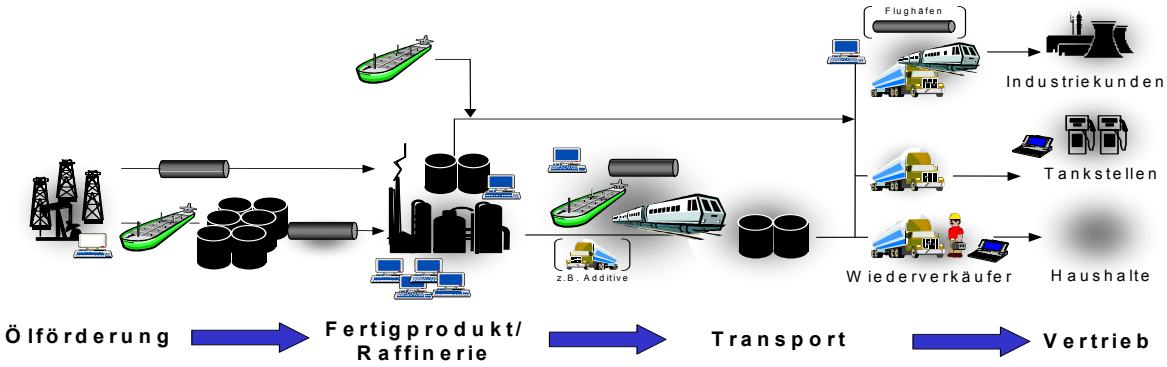

Figure 3: petroleum supply business process

The business process “Petroleum supply” can be presented initially as comprising only four stages. If the experts expect particular criticalities for a particular process step, the individual process steps can be broken down into further detail, as shown in Figure 3 in the case of “Transport” and “Distribution”.

3.3. Assessment of criticality

The business processes must then be assessed with regard to their criticality. The key question here is:

> “What happens if one component in the process breaks down and what is the probability of this occurring?”

It is unlikely that the answer can be found from historical or statistical data. Fortunately, too little data is available for this. Power blackouts are not a regular occurrence and hopefully there will never be enough terrorist attacks to permit a statistical evaluation. Therefore the primary source of information must once again be experts.
What is important here is the assessment of the experts as to whether the far-reaching disruption of a process is feasible, what the consequences of this would be and what effect the disruption would then have. If possible, several experts should be consulted for each process. This allows the subjective assessments to be consolidated.

To make the assessments comparable – and, if possible, the results of the analysis should enable comparisons to be drawn between the individual sectors – multi-point rating scales must be specified both for the effects to be expected and also for the estimated probabilities of failure. Five intervals would appear to be sufficient for this purpose without being too coarse: e.g. ratings of damage can range from “trivial” to “catastrophic” and of the probability of failure from “extremely unlikely” to “virtually certain”.
The significance and order of magnitude of each rating can be explained to the experts / interviewees using examples and scenarios. The use of specific numerical values should be specifically avoided, since that approach would imply an unrealistic level of comparability. For example, requirements for failsafe performance differ considerably between nuclear

power stations and airport baggage handling operations.
The criticality of the process is then derived from the combination of effects and failure probability.

Failure probability						
	Virtually certain	Significant	Significant	High	High	High
	Probable	Intermediate	Significant	Significant	High	High
	Possible	Low	Intermediate	Significant	High	High
	Improbable	Low	Low	Intermediate	Significant	High
	Highly unlikely	Low	Low	Intermediate	Significant	Significant
		Trivial	Low	Moderate	Extensive	Catastrophic
		Effects / degree of damage				

Table 1: assessment of criticality

Under this scheme and following evaluation of the survey data, the individual processes can then be entered in the criticality matrix. This is done first of all at the “Business” abstraction level.

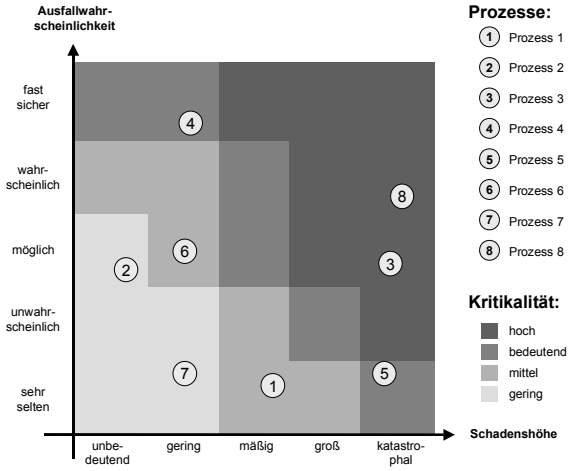

Figure 4: criticality matrix – processes

During the process of consulting with the experts, their judgement of the effects of failure of the process on the sector must be recorded. As explained above, very few business-critical processes are also sector-critical. However, industry structure is an important factor here. If the industry under examination is one that is dominated by one or only a few enterprises, the business-critical processes of these enterprises are likely to be sector-critical as well. Business-critical processes in industries characterised by a large number of competitors on an equal footing are generally not critical to the sector. However, when the abstraction level under consideration changes from business to sector, a shift in the criticalities in favour of the sector is invariably found.

If one then projects this picture at the level of society, once again a shift is possible, but the effect is not significant. Finally, the definition “Critical Infrastructure” itself implies that failure of the sector will have lasting effects on the public good. Thus, when processes are identified which, while endangering the services provided by the sector, nevertheless exhibit significantly lower criticality in relation to society, then there are discrepancies in the logical chain.

Looking at things this way, all the processes are assessed for criticality for the abstraction levels “Business”, “Sector” and “Society”. On the other hand, if the assumptions set out above are valid, then the procedure can be designed more efficiently.
Processes whose criticality is recognised as “low” or “intermediate” cannot be classed as “significant” or “high” in the next abstraction level. They can be directly ignored. Only those processes whose criticalities are judged to be “significant” or “high” then need to be considered in subsequent steps (see also Figure 6).**Investigation of dependence on IT**

The primary aim of ACIS is not, however, to identify those processes that have high criticality. This is only the preliminary work necessary to then determine the nature and extent to which the processes and hence the sectors under investigation are dependent on IT.

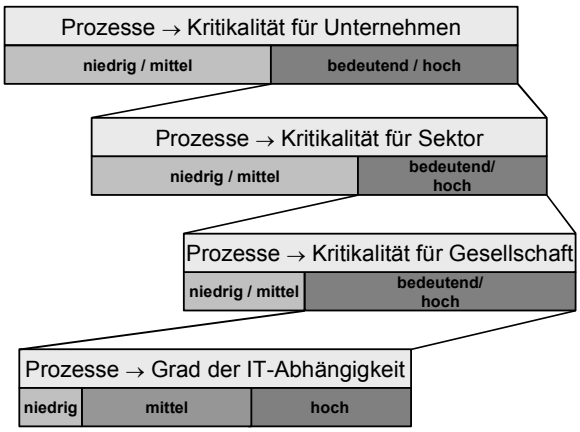

Figure 5: simplified ACIS procedure

In order once again to contain the amount of work required to an acceptable level, the investigation of dependence on IT is confined to those processes whose criticality is significant or high at the level of society.
The process descriptions already prepared can once again serve as the basis here, especially the opinions of the experts. The degree of dependence on IT is then roughly scaled, in this example using the ratings “low”, “intermediate” and “high”. Under this rating scheme, processes whose IT dependence is “high” cannot function at all or only to a limited extent without IT support.

3.5. Correction factors

Having described the general methodology, two factors which can influence the criticality matrix must now be addressed.
The first of these is the already available mechanisms internal to the sector: individual sectors have already recognised that the functioning of the entire sector depends on certain processes and have already taken appropriate protective measures. These measures extend both to the preventive and also the reactive area. In particular, measures which contain the effects of failure and ensure rapid recovery have an impact on the criticality of the individual processes.
Secondly, it has to be borne in mind that the results provided by applying the methodology are based on the subjective impressions of the sector experts. However, (in the personal opinion of the authors) it is fair to say that in Germany expectations regarding the resilience of infrastructural services are relatively high these days. In fact, however, effects on the public which in Germany are regarded as material or “extensive” are viewed in other countries as “trivial” and a part of everyday life.

Taking into account the two factors mentioned, the final criticality matrix can be slightly modified if appropriate. The effect of this will be to reduce criticality.

4. Results of the analysis

Once every critical infrastructural sector has been subjected to this analysis, then the following results will have been generated:

- An overview of how the individual sectors function, how important they are to the economy and how they should be structured for the purposes of the analysis of criticality;
- Generic descriptions of important business processes;
- For every sector, a society-level criticality matrix, processes with significant and high criticality identified;
- The dependence on IT of these processes – and hence also of the sectors – will have been identified.

This analysis approach also produces some other results which, even if they are not at the focus of the investigation, are still very interesting:

- As well as IT dependence and threats, this process-oriented investigatory approach also identifies conventional threats;
- Any requirement for further, in-depth investigation will have been identified (e.g. in the course of interviews with experts);
- Sector representatives will have been made aware of the issues (partly as a side-effect of the workshops and interviews).

5. Summary

The findings on Critical Infrastructures obtained using the analysis approach outlined are not sufficiently detailed to serve as the basis for specific measures, nor do they claim to guarantee that every critical process will be identified. Nevertheless, ACIS allows an impression of the dependence on IT of Critical Infrastructures to be gained rapidly and hence provides a good knowledge base that will help state and industry to work together systematically to ensure the reliability of our infrastructures in the future.