

Protection against Sabotage of Nuclear Facilities: Using Morphological Analysis in Revising the Design Basis Threat

Adaptation of a Paper delivered to the 44th Annual Meeting of the Institute of Nuclear Materials Management - Phoenix, Arizona, July 2003

[Downloaded from the Swedish Morphological Society: www.swemorph.com]

Stig Isaksson¹, Tom Ritchey^{2*}

¹ Swedish Nuclear Power Inspectorate, SE-106 58 Stockholm, Sweden and ² Swedish Defence Research Agency, SE-172 90 Stockholm, Sweden

ABSTRACT

The Swedish Nuclear Power Inspectorate (SKI) is the regulatory authority for nuclear activities in Sweden. It is responsible for the development of a Design Basis Threat¹ (DBT), as a basis for regulations on Physical Protection of Nuclear Material and Nuclear Facilities. SKI has recently revised its regulations concerning Physical Protection of Nuclear Facilities. The starting point for this task was to review the existing DBT. To accomplish this, SKI chose to use the method of morphological analysis (MA) as a tool to structure and analyse the problem, in order to arrive at a realistic DBT. The work was done with the help of the Swedish National Defence Research Agency (FOI). FOI has developed a computerised laboratory in which alternative scenarios can be formulated, developed, tested and evaluated. This paper will describe how MA was employed in developing scenarios and how the results of the work were used to revise the DBT.

[For more information on how Morphological Analysis was employed at SKI, see the other article presented at the INMM Meeting: "Nuclear Facilities and Sabotage: Using Morphological Analysis as a Scenario and Strategy Development Laboratory": www.swemorph.com/downloads.html.]

INTRODUCTION

The Swedish Nuclear Power Inspectorate, SKI is the regulatory authority for nuclear activities in Sweden. Its responsibilities include nuclear safety and security issues. Since the middle of the 1970's, in area of physical protection against theft of nuclear material and sabotage of nuclear facilities, SKI has applied the concept of Design Basis Threat (DBT). The DBT has repeatedly been reviewed over the years. For this purpose, SKI has employed traditional assessment methods in association with other relevant national authorities. The DBT has formed the basis for SKI in developing regulations on physical protection of nuclear material and nuclear facilities. Moreover the DBT has been an important input for operators when designing their respective measures for physical protection.

In the late 1990's, SKI decided to modernise its regulations in general, including the regulations on physical protection. The reason for this was to better reflect the new supervisory policy of SKI and to make the regulations more transparent. The starting point for revising these regulations was to make a thorough review of the existing DBT. This task was almost finalised in August 2001. Then came September 11th, 2001!

* Correspondence: T. Ritchey, e-mail: ritchey@foi.se

REVISING THE DBT

In the light of the terrorist attacks in New York City and Washington DC, it was obvious to SKI that the DBT needed to be revised once again, to properly take into account the experiences from 9/11. For this purpose, SKI decided -- for the first time -- to use a methodology provided by the Swedish Defence Research Agency (FOI). The objective was to use a well-structured method within which both the process and the results would be clearly documented, traceable and transparent. The method chosen -- Morphological Analysis (MA) - seemed to meet those objectives.

As mentioned above, SKI co-operates closely with other relevant national authorities when defining or revising the DBT. For this project, a multi-disciplinary working group was established with experts from the following areas:

- Nuclear security/physical protection
- Nuclear safety
- Nuclear systems engineering
- International terrorism
- Counter terrorism
- Security policy

Two senior morphologists from FOI supported the working group of 6-8 subject specialists. The MA process itself is supported by software developed by FOI – CASPER (Computer Aided Scenario and Problem Evaluation Routine). The software supports the entire analysis-synthesis cycle which MA involves.

Morphological Analysis (MA) is presented in more detail in Tom Ritchey's paper, "Nuclear Facilities and Sabotage: Using Morphological Analysis as a Scenario and Strategy Development Laboratory", also presented at this conference.

WORKING METHOD

The work was carried out in 8 workshops during the first half of 2002. The task was to develop a morphological field that described the total problem complex and then could be used as a laboratory in order to test various inputs against possible outputs.

The first step was to identify the variables that defined the threat scenarios relevant for nuclear facilities e.g. nuclear power reactors. The next step was to define a range of values or conditions for each variable. The variable and variable-condition matrix is the morphological field, which implicitly contains the solution space for the problem complex. However the matrix now contained hundreds of thousands of theoretically possible threat scenarios.

The third step was to assess the internal consistency of all pairs of variable conditions in order to weed out all inconsistent or contradictory pairs. This part of the process is the most cumbersome and time consuming but also very important. When making the internal consistency assessments, it becomes clear that the variable conditions often are poorly defined, i.e. "we don't know what we are talking about". This leads to a review of the first two steps and iteration between steps 1-3 until the internal consistency assessment begins to work smoothly.

The fourth step is to synthesise an internally consistent outcome space. MA/Casper facilitates this by going through all of the possible configurations in the morphological field and reducing the field by expelling those configurations, which contain internal contradictions. We are thus left with the "solution space" of the defined problem.

The last step is to iterate the whole process and to make adjustments to the variables and variable conditions as required. It should be noted that all of the steps in a morphological analysis are iterative and therefore somewhat time consuming. However, these iterations are both necessary and valuable, since the knowledge base of the expert group develops and grows over time.

RESULTS

The result of the work was a computerised threat scenario laboratory in which alternative scenarios could be formulated, developed, tested and evaluated.

Aggressor's group size	Purpose/goal	Level of knowledge concerning: W=weapons S=systems	Method	Equipment	Part of facility targeted	Consequences
One person No insider	Map/survey	W: high S: high	Reconnaissance	Hand tools	Perimeter	No radiological consequences
One person Insider	Influence opinions	W: high S: low	Illegal trespassing	Information technology (IT)	Protected areas	Loss of fissionable material
Group (< 7 pers.) No insider	Steal fissionable material	W: low S: high	Unauthorized access to computer systems	Handheld fire arms	Surveillance systems	Loss of secret information
Group (< 7 pers.) Insider	Disturb operations	W: low S: low	Threat to disturb the facility	HPM	Nuclear material storage	Limited emission
Group (7-20 pers.) No insider	Stop operations		Blackmail against employee	Explosives	Vital facility areas	Large emission
Group 7-20 pers. Insider	Take control of the facility		Infiltration	Car bomb	Reactor safety systems	Massive emissions
Group (> 20 pers.) No insider	Destroy and cause emissions		Sabotage from within	Short-range missile		
Group (> 20 pers.) Insider	Maximum destruction		Sabotage from outside	B-weapons		
			Massive armed attack a	Chemicals & C-weapons		
				Radiological substances		
				Aircraft		
				Middle/Long-range missiles		
				Nuclear weapons/ EMP		

Figure 1: One of the threat scenario fields developed in the DBT study

Figure 1 shows one of the threat scenario fields developed in the study, containing seven parameters. Originally containing over one million configurations, it was reduced to slightly over 40,000. Note, that for reasons of confidentiality, some of the variable conditions have been modified in this example.

The variables describe the attributes and characteristics of potential insider and/or external aggressors and the potential consequences of malevolent acts against a nuclear power reactor. (The variable cells, which have a small dot in the upper right corner, are defined in more detail in a larger text area associated with each cell.)

The following parameters or variables are employed in this particular field:

- Aggressors group size and insider status: i.e. the number of adversaries directly involved in an attack on a nuclear facility and whether there is an insider involved
- Purpose/goal: i.e. the purpose of an attack on a nuclear facility
- Level of knowledge: i.e. the aggressors' level of knowledge concerning equipment and weapons that are used and the process, safety and security systems in the targeted facility
- Method: i.e. the method used to support the goal
- Equipment: i.e. the equipment and/or weapons used to support the method and goal
- Part of facility targeted: i.e. the different parts of the facility that is subject to an attack
- Consequences: i.e. the possible consequences of an attack

ANALYSIS

After having received the computerised threat scenario laboratory, SKI studied many different scenarios with respect to their possible consequences. Furthermore, the impact of various variable conditions on the consequences was studied in depth in order to identify the critical conditions, i.e. those that have more relative weight than others.

Aggressor's group size	Purpose/ goal	Level of knowledge concerning: W=weapons S=systems	Method	Equipment	Part of facility targeted	Consequences
One person No insider	Map/survey	W: high S: high	Reconnaissance	Hand tools	Perimeter	No radiological consequences
One person Insider	Influence opinions	W: high S: low	Illegal trespassing	Information technology (IT)	Protected areas	Loss of fissionable material
Group (< 7 pers.) No insider	Steal fissionable material	W: low S: high	Unauthorized access to computer systems	Handheld fire arms	Surveillance systems	Loss of secret information
Group (< 7 pers.) Insider	Disturb operations	W: low S: low	Threat to disturb the facility	HPM	Nuclear material storage	Limited emission
Group (7-20 pers.) No insider	Stop operations		Blackmail against employee	Explosives	Vital facility areas	Large emission
Group 7-20 pers. Insider	Take control of the facility		Infiltration	Car bomb	Reactor safety systems	Massive emissions
Group (> 20 pers.) No insider	Destroy and cause emissions		Sabotage from within	Short-range missile		
Group (> 20 pers.) Insider	Maximum destruction		Sabotage from outside	B-weapons		
			Massive armed attack a	Chemicals & C-weapons		
				Radiological substances		
				Aircraft		
				Middle/Long-range missiles		
				Nuclear weapons/ EMP		

Figure 2: One of the more conceivable threat scenarios

Figure 2 (above) shows a threat scenario defined by the highlighted variable conditions. It describes a small group of aggressors supported by an insider. The group has a high level of knowledge both about the targeted facility and the weapons and explosives they employ. The purpose of their attack is to sabotage equipment in vital areas and/or reactor safety systems and possibly cause a radiological accident. Depending on the effectiveness of safety systems and physical protection measures, the potential consequence would either be no radiological consequences or limited emissions of radioactivity.

It turned out from the analysis that certain variable conditions are more important and need to be addressed specifically in the coming regulations. For example, certain equipment in the hands of an aggressor will increase the possibility of “successful” sabotage. Furthermore, certain parts of a targeted facility are more vulnerable to sabotage than others.

Based on the study and analysis of scenarios in the computer-aided laboratory, as well as a separate strategic threat assessment provided by the Swedish Police Security Service, SKI formulated and proposed a revised DBT. The proposal was further discussed with the authorities involved in the MA-study and appropriate adjustments were made. SKI's advisory board on non-proliferation issues was also consulted before the Director General of SKI finally decided on the DBT.

Given its sensitive nature, the actual DBT is a secret document. However, there is an obvious need to provide both licensees and outside response forces with detailed information about the DBT. In order to promote understanding and acceptance of the DBT, as well as providing information about the process behind its development, SKI has arranged half-day meetings with security managers from the licensees and representatives from central and regional police authorities. These meetings have been quite well received and have provided the opportunity for participants to query authorities -- which is also part of the process to establish the DBT.

After having established the revised DBT, the next step for SKI as a regulator is to revise the regulations on physical protection of nuclear material and nuclear facilities. SKI must formulate the requirements for physical protection measures necessary to counter the perceived threat. This process has already begun and the plan is to have the new regulations in force in early 2004.

SUMMARY

From a nuclear regulatory perspective, morphological analysis has been a new experience. The computer-aided threat scenario laboratory has proved to be an excellent tool in revising the DBT. Moreover it has shown to be a valuable tool also in vulnerability assessments of nuclear power reactors.

Furthermore, both the process and the results are well documented, transparent and traceable. This will be helpful in the coming reviews of the DBT. The starting point for future reviews would then be the now existing threat scenario laboratory.

¹ The international recommendations "The Physical Protection of Nuclear Material and Nuclear Facilities", INFCIRC/225/rev.4 (Corrected) defines Design Basis Threat as “The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorised removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.”