Implementing international security guidelines*** into the Belgian regulatory framework – practical issues

G. Vanderschelde (Bel V), D. Marloye (Bel V)*, R. Dresselaers (FANC)***

* Bel V, Subsidiary of the Belgian Federal Agency for Nuclear Control,
Rue Walcourt 148, B-1070 Brussels, Belgium

** Federal Agency for Nuclear Control, Rue Ravenstein 36, B-1000 Brussels, Belgium

*** guidelines also include commitments

Abstract:
Whenever international security guidelines need to be "translated" into a national legal framework, problems surface when implementing the rules into daily practice. Although legal pleadings don't represent the subject of this paper, they at least trigger the discussion on the implementation, control and inspection of the legal directives in the (near) future. The emphasis lies here on the "lessons learned" and the application of its contents as added value. What follows are the practical and technical perceptions from the point of vue of the TSO (Technical Safety Organisation).

1 PREFACE

Approximately two and a half years ago, FANC and Bel V, the Federal Agency and its TSO, faced a huge challenge. The legal framework for the physical protection of nuclear materials, installations and transports needed to be updated by taking into account the most recent revisions of the international guidelines and by applying the most recent international commitments. This was done by the co-workers from our Federal Agency for Nuclear Control (FANC) who made up the legal texts for approval by our Government.
At the same period, a dedicated working group started up with representatives of the FANC and BEL V in order to work on how both organisations could work together in the field of nuclear security. The purpose was to look for possible synergies taking into account the processes of collaboration that already exist in the fields of safety.
In order to implement this new legal framework, different initiatives to assist stakeholders were started up, such as workshops, round tables on specific topics, and the IAFA (Initial Action File Agreement) tour. The IAFA tour was launched on a voluntary basis by the FANC in close co-operation with the management of the different nuclear installations and transport firms. The goal of this action was to explain the new legal and regulatory framework and to help the operator to prepare an effective version of the (future) definitive authorization request file by means of an effective exercise. It was especially useful in order to determine which actions needed to be taken to upgrade the contents of the request file, drawn up by the owners of the different nuclear exploitations. This was also the first time that there was a close cooperation between FANC en BEL V, together with the stakeholders, on the field of nuclear security.

Basically they used the following drivers and triggers:

- **INFCIRC 274: - rev. 1**: Convention on Physical Protection Nuclear Materials (CPPNM)
- **Amendment to the Convention** on the Physical Protection of Nuclear Materials
- **INFCIRC. 225 – rev. 4**: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities

The Belgian law and its royal decrees were published in the Belgian Monitor during the year 2011.

2 MISSION

Implementing a new regulatory framework is not only limited to an improvement of the physical protection of the installation but also has an impact on the way of working at the different facilities. Our mission statement was to define the **Key Success Factors (KSF's)** in order to implement an effective **Integrated Inspection and Control (IIC)** approach, based upon the national security framework.

Arriving at this stage of the process, the most challenging task surfaced:

"The laws and regulations on enforcement, by their very nature, are expressed at the highest general point of view. How to further improve the possible gap between these laws and regulations on enforcement and the concrete and real-world surveyors and controllers?"

Building an implementation strategy seemed logically the next step in the process flow.

2.1 Building an implementation strategy

Any company undertaking strategic planning will at some point assess its **strengths** and **weaknesses**. When combined with an inventory of **opportunities** and **threats** in (or even beyond) the company's external environment, the company is effectively making what is called a SWOT analysis [1], as shown in the graph below.

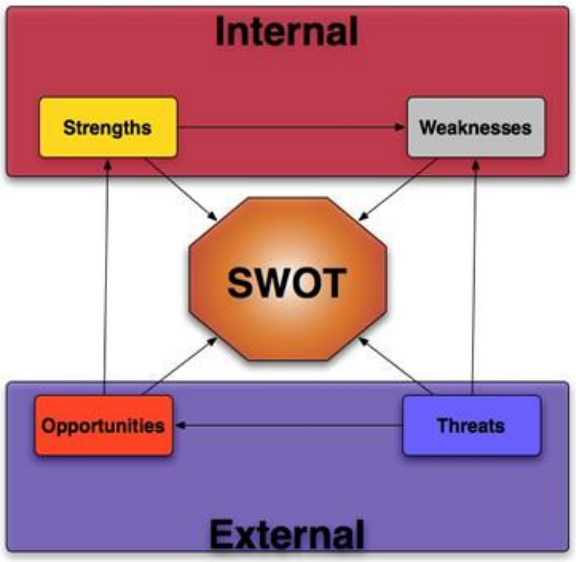

Figure 1: The SWOT-process

It is important to note that strengths and weaknesses are intrinsic (potential) value creating skills or assets. Opportunities and threats, however, are external factors, not created by the company.
Strengths and weaknesses can be measured in an internal or external audit. Both opportunities and threats can be classified according to their potential impact and actual probability, as illustrated below.

	Strengths (S)	Weaknesses (W)
Opportunities (O)	• **SO Strategies** Use strengths to take advantage of opportunities	• **WO Strategies** Take advantage of opportunities by overcoming weaknesses or making them relevant
Threats (T)	• **ST Strategies** Use strengths to avoid threats	• **WT Strategies** Minimize weaknesses and avoid threats

Table 1: SWOT-analysis: theoretical approach

2.2 Identifying the strengths, weaknesses, opportunities and threats

In order to accomplish this task different working groups were set up and **some of the results** of their findings were gathered below. During the evolution of the SWOT-analysis it is imperative that the amount of elements stays limited to a maximum of 16. Literature [1] and experience feedback tend to withold this amount of elements to be a manageable limit in one analysis.

Strengths	Weaknesses
S1: Combining the competences of FANC and BELV	**W1:** No sufficient security training programs available on the open market
S2: Creating a reference framework for control and inspection	**W2:** National rules and regulations on security scattered over a lot of different regulatory and regional bodies (i.e. insurance, construction business line, economics department,…) in Belgium
O1: Structured approach of the credible threats (DBT)	**T1:** Contents of the authorization file, issued by the management of the nuclear plant, are not compliant
O2: Evaluate the interaction between nuclear safety & security	**T2:** Treatment of "sensible" information in the authorization file by the management of the nuclear plant
O3: Identify the delay time of the PPS and the response time of the intervention team(s)	**T3:** How to handle the aspect "insider threat" (URC(*) included)?
	T4: The possible impact of beyond DBT threats (BDBT))
	T5: The use of foreign standards and guidelines in the local (nuclear) security policy
Opportunities	Threats

INTERNAL

EXTERNAL

Table 2: SWOT-analysis: the practical findings

(*): Unacceptable Radiological Consequences

2.3 Determining the Key Success Factors for an IIC approach

Listing the SWOT was not that easy as it seemed to be. However, the second step is even more difficult: what actions should we take, based on the identified strengths, weaknesses, opportunities and threats ?

In many cases a confrontation matrix will be drawn up and ranking by weighing of the different interactions is needed.
Another approach is the qualitative way, the members of the working group prioritize their findings and formulate their conclusions.

Now Key Success Factors (KSF's) have to be defined. Determining strategic alternatives is a possible option, but does that suffice as definition ?

Believing in the basic principle that if explanations become really complicated, they are the reason for failure or inadequacy in the future, many professionals recognize this description as the KISS-principle [2].

Referring to Table 2 above, the interaction between the different elements needs to be determined on a qualitative basis.

	O1	O2	O3	T1	T2	T3	T4	T5
S1	OK	OK	NR	OK	OK	KSF#01	NR	KSF#02
S2	OK	OK	OK	OK	KSF#01	KSF#01	NR	KSF#02
W1	KSF#03	KSF#03	KSF#03	KSF#03	NR	KSF#03	NR	KSF#03
W2	NR	NR	NR	KSF#04	OK	NR	NR	KSF#05

Table 3: Confrontation or decision matrix

Legend:
OK*: topic sufficiently covered by internal and external elements*
NR*: no relevancy or no legal competence*
KSF#*: Key Success Factor #number*

After identifying the KSF's there is a real necessity to enlarge upon the different factors. The purpose of this paper is not to go into detail into each KSF but to have a closer look at some of them, especially if they certainly will impact the day to day work at the different facilities and if they request an another mindset.

2.3.1 Insider threat or more general "the impact of human factors" ***(KSF#01)***

Due to the fact that people usually represent the weakest link in the chain (of protection), the aspect "Insider Threat", sabotage included, needs our full attention. An effective risk analysis and procedure, drawn up by the owners of the nuclear facilities, is mandatory.

We all know that in 2008 the IAEA published an implementing guide, reporting on the "Preventive and Protective Measures Against Insider Threats" [3], but there is maybe an added value hidden in other resources. Nobody will deny that the implementing guides embody useful, but mostly general information on the discussed topic.
Furthermore it should be noted that the aspect "Insider Threat" is a human factor, based upon an intentional act. On the other hand, the accidental act also belongs to the broader picture of human factors.
Recently the Draft International Standard-version of the ISO 10018-standard [4] was published as a supporting code of best practices on human factors as part of a quality system. Although it is still a draftversion, it gives some "food for thought" on the matter of human factors.

Especially chapters 5 till 8 present and suggest some concrete actions on 15 identified human factors. Whether these factors only treat the accidental aspect or not, that's an open question that needs to be answered in the (near) future.

Early 2012 FANC organised a workshop on this topic. The presentation on "Human factors and Insider Threat" listed the synergies and contradictions between both aspects.

Summarizing, it may be stated that one has to be aware that:

- safety (human and organizational factors) strives to open communication, crew resources management, group synergy, shared mental methods,…, while security (insider threat) aims at discretion and limited distribution of sensitive information;
- the actions of an insider are more or less related to his former behavior;
- organisations develop activities like recruiting, training, promoting and dismissing; those activities are convenient tools to manage, detect and prevent insider risks;
- tools like security awareness, motivation screening, detection of dissatisfaction and/or emotions of injustice aid the perception and prediction of insider threat.

If one speaks about human factors, the link with procedures is not far away. On this matter INPO (Institute for Nuclear Power Operations) wrote in 2009 a good practice-document, titled "Procedure Use & Adherence" [5].

Although this document aims to upgrade the use and adherence of procedures, one aspect is very important and that is the amount of procedures that a co-worker must govern with the possible threat of saturation. A derivative of the Peter-principle is here nearby: "in a hierarchy, every employee tends to rise to his level of incompetence" leads to "in a world of procedures, everyone tends to govern that amount of documents to rise to his level of ineffectiveness".

Another point of particular interest is how the authorization file will be handled in daily operation. Handling nuclear documents are covered by law, but the distribution of the information during audits, inspection and controls needs special attention. The latest version of the ISO 19011 [6] reflects on the risks linked to the execution of audits.

*2.3.2 National safety/security culture versus the use of foreign standards and codes of best practices **(KSF#02)**.*

The Belgian policy is strongly in favor of a strong nuclear security culture. Therefore, the more critical aspects are an actual training of the staff of the nuclear installations, a robust regulation and its enforcement. Recognizing that investment in human capacity building is fundamental to promoting and sustaining such a strong nuclear security culture, all stakeholders should be encouraged to fully commit to enhancing security culture and to maintain robust communication and coordination of activities.

In this perspective, it should be underlined that the nuclear security culture is mainly elaborated at national or even local level. International cooperation in this matter must take into account the subsidiarity principle, and can only help, especially by promoting best practices sharing (it is of common sense, for instance, that a management 'tactic' could be especially efficient here, but completely aimless or counterproductive elsewhere, in another cultural context).

As an illustration of the „local" aspect of the security culture, Geert Hofstede made in his book on cultural differences [7] for over one hundred countries a benchmark in 5 dimensions.

The Uncertainty Avoidance Index (UAI) [7] is one of these dimensions, useful in the evaluation of the applicability of the foreign standard into Belgian practice.

UAI tends to rank the degree to which people in a country prefer structured over unstructured situations. In cultures that score high on uncertainty avoidance, people have an increased level of anxiety about uncertainty and ambiguity. Such cultures tend to emphasize laws, regulations, and controls that are designed to reduce uncertainty. In cultures that score low on an uncertainty avoidance, individuals are less dismayed by ambiguity and uncertainty and have a greater tolerance for a variety of options. Such countries are less rule-oriented, take more risks, and more readily accept change.

In countries with high Uncertainty Avoidance Index (UAI) employees prefer formal rules to be created and avoid actions that do not go along with these rules. Employees as well as their bosses believe that everything that is new or different is dangerous and risky. They are usually worried about the future and resist changes. Cultures described as open and innovative always have a low Uncertainty Avoidance Index [7].

For example: Application of USA-standards in Belgium.

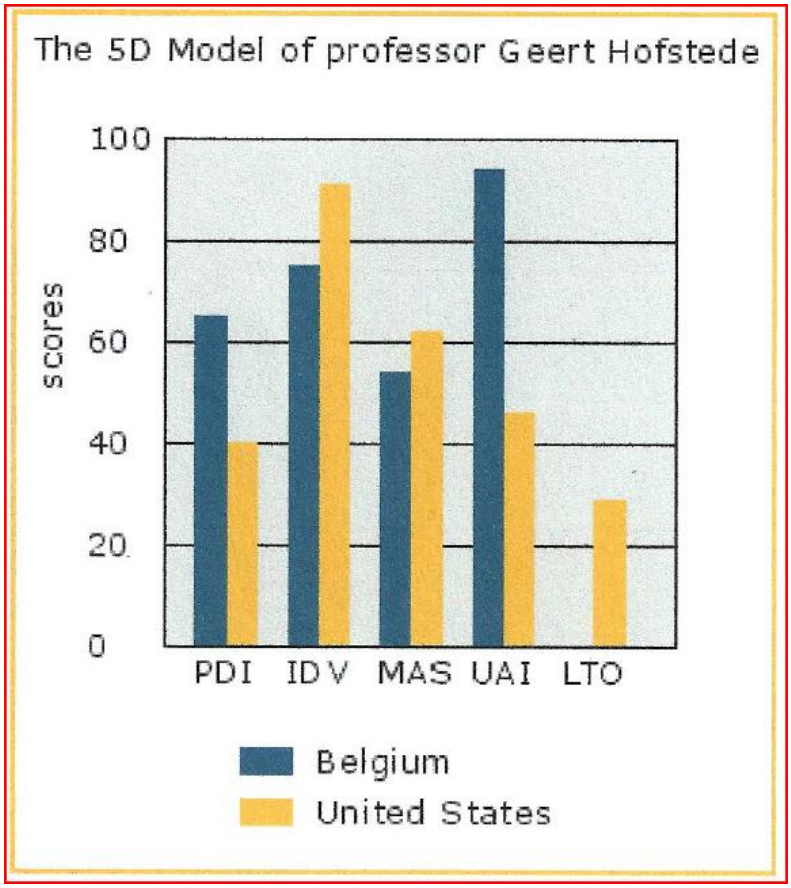

Figure 2: *5 D model for Belgium/USA*

Conclusion: The UAI-score for Belgium is 97 and the score for USA is 46, what means that Belgian engineers will be having troubles to implement and enforce the directives from the American standards. A scrupulous evaluation of the contents is needed before application. A national (Belgian) addendum is sometimes advisable.

Another interesting dimension is the individualism index (IDV) as a benchmark for use in Belgium.
The fundamental issue addressed by this dimension is ***the degree of interdependence a society maintains among its members.*** It has to do with whether people´s self-image is defined in terms of "I" or "We". In Individualist societies people are supposed to look after themselves and their direct family only. In Collectivist societies people belong to 'in groups' that take care of them in exchange for loyalty.

The figure below [7], visualizes the coherence of different nations, regarding UAI and IDV-dimensions.

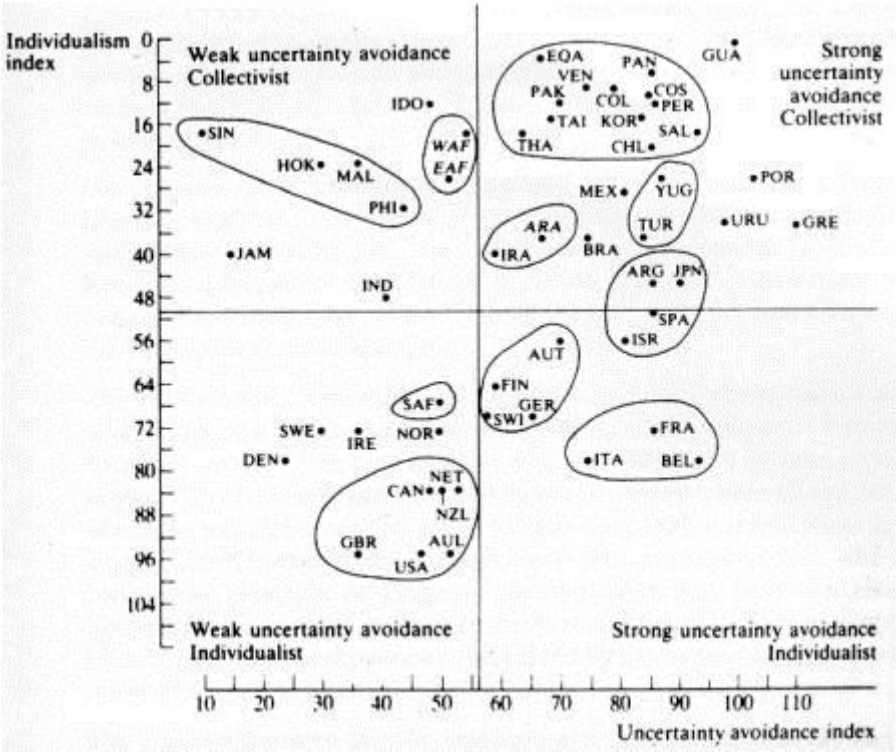

Figure 3: *IDV- UAI clusters of nations [7]*

Conclusion: Countries with high IDV are protectionist regarding their own standards and will difficultly accept modifications or remarks from third parties [8].

Not only culture has an influence, it is also advisable to remain sceptical about technical facts and figures.
One example to illustrate this statement: bollards tested and classified, according an American standard, garantuees nothing while installed in Europe. Reason: the American trucks, used for the classification test, don't have the same morphology as the European trucks. A PAS 68-rating is to be preferred over a K12-rating.

*2.3.3 No sufficient trained resources available **(KSF#03)**:*

After having made this conclusion, the Federal Agency started with hiring new co-workers less or more experienced in the physical protection branch. Bel V initiated a new TRC (Technical Responsability Center) on Nuclear Security. If we compare the number of trainings available in the field of nuclear safety we only conclude that in the field of nuclear security not a lot of training courses are available. This is definitely a challenge not only for the competent authorities and their TSO organisations but also for the different operators to have sufficient personel trained in physical protection. This problem can't be solved only by organising training programmes on a national basis, or by closer cooperation between the different competent authorities and TSO. Actually, it should be advisable to establish more regional training courses.

A table-top exercise Bel V–FANC was launched to have a first practical experience on the evaluation of a (fictive) authorization file. Bel V acted as managing owner of a nuclear installation on Belgian soil. As demanded an authorization file was drawn up and sent to the Federal Agency. Analyzing this fictive file gave us already some impressions on the possible problems that could occur.

*2.3.4 No structured view on current regulations, standards and codes of best practices in Belgium and across border (**KSF#04 & KSF#05**):*
A Knowledge Base on Physical Protection was drawn up to back-up the control function of the authorization files (see Figure 4). With the different chapters of the law on physical protection as guidance, an overview of the existing laws, standards and codes of best practices were collected.
The above mentioned Knowledge Base is also fitted with the possibility to note down the foreign standards and codes of best practices. One should establish also a selection matrix to prioritize the different documents treating the same topic.

KNOWLEDGE BASE PHYSICAL PROTECTION

PILAR	PART	QUALIFYING PARAMETERS	REGULATORY FRAMEWORK									TERMS & RESTRAINTS REGULATORY FRAMEWORK
		Guidance words (AOT = Advanced and Other Technologies)		LAW	STANDARD	BEST PRACTICES	National	European	International	Priority	Nuclear specification	
1.	**PERIMETERS**											
	FENCE	General	INFCIRC 225/rev.5 NRC 10 CFR 73		X				X	P4		§5.2.4.4

Figure 4: *Knowledge Base on Physical Protection (internal document)*

3 LESSONS LEARNED

Probably it is the most effective way to make an overview of all point of views that were made during the process. These conclusions lead to a number of “lessons learned”.

- The increasing importance of human factors (insider threat);
- The importance of the impact of the national (security) culture of the country of origin on the developed standards and codes of good practices;
- The absence of a clear overview of the existing standards and codes of best practices on the national level;
- Building an authorization file request equals gathering all the sensible information on Physical Protection at one file;
- The results of the IAFA-action showed that more clarifications were needed to avoid as much as possible weaknesses in the issued authorization files requests;
- Setoffs in safety and security policy will most probably emerge in daily practice whenever changes on installations have to be managed (MoCh);

4 REFERENCES

[1] S. ten Have, W. ten Have, F. Stevens and M. van der Elst, „Key Management Models: what they are and when to use them“, Pearson Education Limited, 2003, Edinborough Gate Harlow;
[2] W. De Keyser and J. Springael, „Why don’t we KISS!? Acontribution to close the gap between real-world decision makers and theoretical decision-model builders“, University Press Antwerp, 2009, Brussels;
[3] IAEA, Nuclear Security Series Publications, „Preventive and Protective Measures Against Insider Threats“, 2008, Vienna;
[4] International Standards Organization, „Quality Management – Guidelines on people involvement and competences“, ISO 10018, 2012;
[5] INPO, „Procedure Use & Adherence“, 2009, USA
[6] International Standards Organization, „Guidelines for quality and/or environmental management systems auditing”, ISO 19011, 2011;
[7] G. Hofstede, G-J. Hofstede and M. Minkov, „Cultures and Organizations: Software of the mind“, 2012, Mc Graw-Hill
[8] I. Krupinov, „Regional Training Course (RTC) on Nuclear Security Culture“, IAEA, 2010, Paris