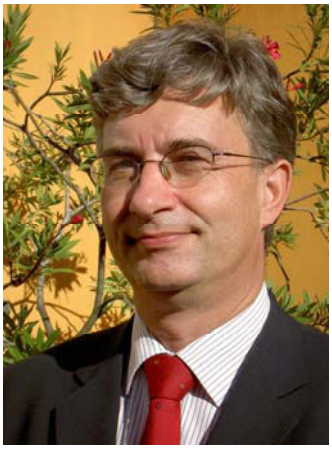
EURAM - EUropean Risk Assessment Methodology project

EURAM developed a uniform risk assessment method for Critical Infrastructures that scales across company, sector, cross-sector and European-wide levels.



Eric Luiijf MSc(Eng)Delft

Eric is Principal Consultant Information Operations and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0312
e-mail: eric.luiijf@tno.nl
Website: www.tno.nl

Marieke Klaver PhD

Marieke is Programme manager Security and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands.
Phone +31 70 374 0112
e-mail: marieke.klaver@tno.nl

Dealing effectively with threats to and vulnerabilities of critical infrastructures (CI) up to the European level requires methods for CI risk assessment and CI risk management. Risk management processes already exist or are under development for different critical and non-critical sectors in the EU Member States. These processes, however, deal with different sets of threats and different approaches. The European Commission European Programme on Critical Infrastructure Protection (EPCIP) requires a wider co-ordination of these risk management processes with common basic elements and a transversal approach within critical sectors, across critical sectors and/or cross-border while taking into account the (inter)dependencies of CI. To be able to accomplish this, there is a need for a common understanding and information sharing about threats, vulnerabilities and risk by all CI stakeholders, e.g., operators, emergency management centres, policy makers, and independent regulators, both with the CI sectors, cross-sector and at EU-levels.

Re-uses the outcome of existing risk assessment; only align along an agreed 'yardstick' and assess the CI dependencies

The EPCIP sponsored project EURAM - EUropean Risk Assessment Methodology project targeted these issues. EURAM had the following objectives:

- identify basic elements for a EU methodology for general risk assessment,
- identify elements for a common methodology for analysis of (inter)dependencies,
- support information sharing by defining procedures for creating qualified and trusted expert networks.

EURAM ran from December 2006 until November 2007. The work was performed by a TNO Defence, Security and Safety-led consortium consisting of THALES Security (United Kingdom), Ericsson (Sweden), ERTICO (Belgium), and The Netherlands Organisation for Applied Scientific Research TNO (Netherlands).

Business to European-wide

EURAM delivered elements for an overarching risk analysis method. This method allows a holistic approach at different levels of abstraction from the business level, via sector and cross-sector levels up to the European-wide multi-national level. In comparison with other risk methods, EURAM uses an approach that takes the CI dependencies into account and accommodates the outcomes of earlier risk analyses at lower levels of abstraction.

The TNO-led consortium also studied how the various public and private stakeholders, who are involved in providing resilient critical sector services, can share sensitive information on risk in a trusted way ('information sharing').

Based on broad expertise in CI

The EURAM developments are largely based upon the broad expertise of the consortium partners with critical infrastructure protection (CIP). The outcome of the study reflects the background knowledge by the partners stemming from dialogues with the CI operators in sectors like energy, telecommunication, drinking water, transport, and water management as well as with government agencies in various European nations.

Scalable, lean and mean

The EURAM holistic risk approach addresses the risk from a point of view where all expertise at a certain level of abstraction is involved. At the business level one can think of people responsible for and representing process control, information systems, human resources (e.g. awareness processes) and management.

By using a uniform approach with a single list of potential threats, multiple teams can work in parallel in various parts of the organisation on identifying and scoring risk factors. The use of uniform yardsticks (e.g. a five point scale) allows communication across the various teams.

The risk assessment method developed by Thales for a single organisation has been extended by TNO with a comprehensive set of example 'yardsticks' that match the EPCIP definition for CI. These yardsticks allow risk scoring on the axis for seriousness of the effects for the citizens, economic damages, environmental damages, political effects, psychological effects and health effects. This allows a transparent and seamingless use of the scales across all levels of abstraction. When moving up from the business level to the sector level, the cross-sector level and the EU multi-national level, the only additional step to be made is a careful analysis of the dependencies of other CI.

Additionally, a set of steps has been developed by TNO to identify the full set of CI dependencies at a certain level of abstraction. These include the second-level of dependencies which become critical when a primary dependency fails, e.g. after a power failure, the dependency of diesel fuel to run the power backup generators becomes critical.

Minimise sensitive exchanges

When moving up to the next level of abstraction, only the identified risk which could not be handled in total at the lower level, needs to be conveyed at the next level. For instance, a business can take care of the risk of power failures and flooding up to a certain extend. The next level needs to take care of the risk which exceeds the business level, e.g. prolonged power outages or major area flooding. At that level, the effects of catastrophic events will be much larger than at the individual business level paired with a much lower probability. On the earlier five-point scale at the business level, one or more risk categories will become of no importance while at the top-end new risk scoring categories will appear. In the same way, when moving up to a next (e.g. multi-national) level, some scoring categories will disappear and new ones will appear.

This approach allows the communication about risk and the handover of risk to the proper higher level of abstraction without additional efforts. As only the risk factors that are not totally controlled are communicated, the sharing of business or sector specific sensitivities is limited to the absolute minimum.

EURAM also encompasses the re-use of the results of an existing risk assessment in an organisation or by a CI sector. Such risk assessments are probably based upon another risk method. The only step required is to map the remaining risk along the EURAM 'yardsticks' and to communicate the CI dependencies which form a risk to the organisation to the next level.

Conclusions and outlook

EURAM has identified a set of elements for an umbrella-like risk assessment approach covering risk assessments from the business up to the EU-level which include the risk of CI dependencies.

The EURAM elements and method for risk assessment will be put on trial in the energy sector as part of the EURACOM project, which is also sponsored by EPCIP. EURACOM will start in the second half of 2008. Interested stakeholders who are interested in the trial and the method are invited to contact the authors.

Communicate and share the remaining risk and the CI dependencies with the next level