Cyber attacks – example of an emerging risk

Today, most large industrial plants and critical infrastructure facilities, such as power generation &distribution or oil/gas production & distribution, are increasingly controlled by webs of computers, commonly known as Supervisory Control and Data Acquisition (SCADA) systems. Because their critical information software is increasingly connected to global data and communications networks, these SCADA systems could be vulnerable to cyber attacks. The possibility of accessing and manipulating a facility's process control software was illustrated in 2010 when the SCADA system of an Iranian nuclear power plant was attacked through the Stuxnet computer worm.

Cyber attacks on SCADA systems may lead to failure of the impacted facility, energy blackouts, fire, explosion, injuries or even fatalities and contamination of the environment. In all these cases, the insurance industry would be directly affected. The World Economic Forum's Global Risks 2011 report (see page 24) concluded that "the complexity of cyber security is still not well understood and its risks could be underestimated". The very complexity and interconnectedness of systems in cyberspace and their rapid evolvement make this a challenging undertaking, but the objective must be to translate these threats into manageable risks.