TEES

MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Cyber Threats in the Chemical and Process Industry

Anita Matteini, Alessandro Tugnoli, Giacomo Antonioni, Ernesto Salzano, Valerio Cozzani

LISES – DICAM, University of Bologna, Italy

Chemical and process facilities (CPFs) are often characterized by the storage and processing of hazardous materials, frequently in large amounts and at severe temperatures and pressures. Thus, CPFs are recognized as an attractive target for a variety of criminal categories: from terroristic organizations to common thieves and vandals. A set of physical protection systems are usually installed and periodically revised in order to avoid intrusion and, eventually, to mitigate consequences that could arise from malicious attacks. However, less attention was posed to date to the possibility of interference with the process by intrusions via the cyber space. Basic control loops, frequently used in CPFs, are ruled by computers responsible for their correct operation. These usually are interconnected one to each other (assembling the plant net), and to the external internet via the corporate LAN. Process control system governs all the operative and safety functions in medium and large facilities, and hence it has the potential to create outcomes even more severe than those triggered by physical actions. Cyber-attackers belong to a wide range of sub-categories, each characterized by precise intents and tools. Several accidents due to cyber threats were reported in recent years, and the trend seems to be increasing. Cyber-attacks might target industrial facilities exploiting a focused intrusion via a hacker tactic, or employing intrusive tools as viruses or worms. Usually the worm/virus is not tailored for industrial control systems, but it breaches the company network protection compromising operations. Defense-in-depth concepts to address process interference and intentional releases due to cyber threats were developed. Hazard identification was carried out by a specific procedure to understand how the process system might react after a cyber intrusion: disturbances caused on the plant have been systematically analyzed and combined. Although no specific protection of software systems is required, a range of potential scenarios having different severity emerged. Results point out that cyber threats pose specific process hazards that need to be included in the safety assessment and management systems of CPFs.