Preventing and minimising acts of malicious intent

Malicious acts may arise in number of ways within an industrial facility. Such acts may be perpetrated inside the company by a staff member or subcontractor. The notion of industrial facility itself perhaps needs to be broadened, especially in light of the vulnerability of ancillary installations located on city streets (electrical or gas control boxes). Moreover, a computer hacker does not need to physically be on company premises to carry out a malicious act.

This document seeks to answer 2 questions, namely:

- *How is the risk of a malicious act manifested on an industrial site ?*
- *What solutions are readily available ?*

1. Malicious acts occurring in industrial settings

For the period between 1 January 1992 (date of BARPI's founding) and 31 December 2015, the ARIA database contains :

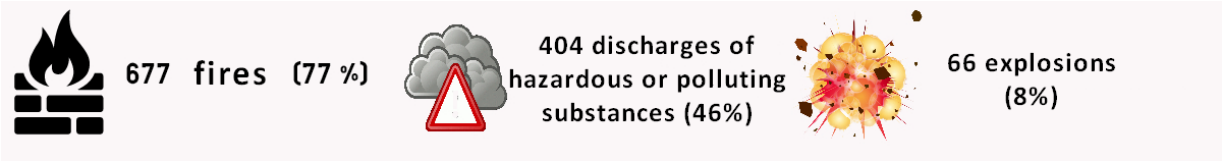
- 1,217 French events spanning all activities with either proven or suspected acts of malice :

Industrial activity	Number of events recorded between 1992 and 2015	Number of events related to acts of malicious intent	Percentage
Classified facilities	25329	881	4%
Dams	332	4	1%
Gas distribution pipelines	1775	50	3%
Transport of dangerous goods by pipeline	442	6	1%
Transport of dangerous goods by waterway	311	40	13%
Transport of dangerous goods by rail	645	7	1%
Transport of dangerous goods by road	2207	17	1%
Household use of gas	824	212	26%

- The malicious acts recorded on natural gas distribution networks or in the vicinity of gas control boxes (household use of gas) underscore the vulnerability of this infrastructure. Performing works on utility networks (gas, electricity) frequently requires cutting supply lines for the time it takes to complete repairs, which in turn leads to degraded operating conditions that must be managed across the entire site (ARIA 46632, 38534).

- Moreover, transport infrastructure, whether by road, rail, navigable waterway or pipeline, may also serve as a target for malicious acts (ignited delivery lorries when parked at an oil depot adjoining a Seveso-rated site: ARIA 40052 / hydrocarbon leak on a railcar after a theft at a marshalling yard: ARIA 35847).

- The 881 malicious acts committed at classified facilities were the cause of:



- Among all these events, only 15 involved SEVESO rated sites, 5 of which occurred in 2015 alone. These following accident scenarios are representative of what has been observed in other facilities :

  - ARIA 47919: Fuel oil spill inside a power plant subsequent to a labour strike ;

  - ARIA 47054: Damage to an electrical box located in the public domain, causing an energy outage at a chemical storage site ;

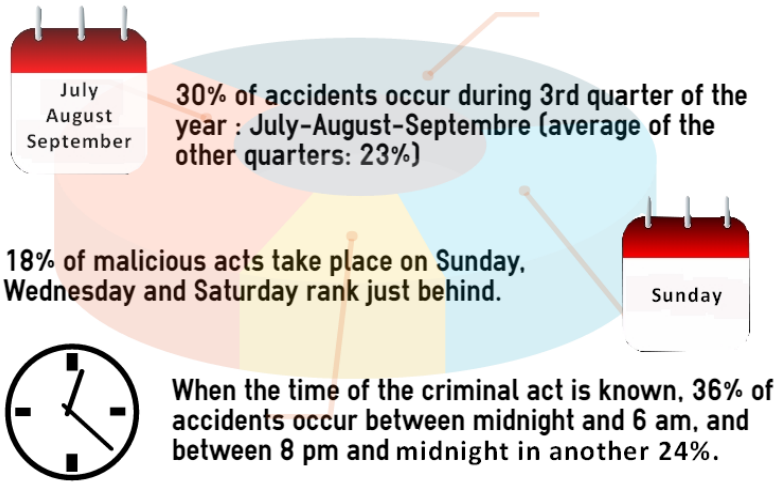
  - ARIA 46801: Fire outbreak on hydrocarbon tanks ;

  - ARIA 46767: Physical aggression in an industrial gas plant ;

  - ARIA 46508: Fire outbreak at a seed sorting and packaging plan t;

- Another 46 events occurred on industrial sites that were either abandoned or being dismantled. The theft of copper materials on electrical transformers (windings) often leads to spills of dielectric oils containing PCBs.

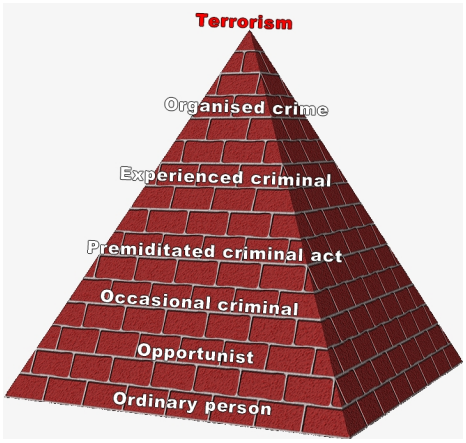
- Timing of the 881 events recorded on classified facilities



- The consequences of events are primarily economic in over 80% of the 881 events studied: based on available information, property damage has amounted to over 2 million euros in 50% of cases, with operating losses being valued at an average of 1.8 million euros for 30 known cases. Environmental pollution consequences can be observed in 46% of all events. Atmospheric pollution (smoke from fire) represents over half of the pollution recorded.

2. Which prevention strategies can be implemented ?

Whether the threat is from cyber attack, ordinary malice or terrorism, it is helpful to assess the risk of malicious acts by examining possible accident scenarios in conjunction with the vulnerability of installations. The nature of the perpetrators must also be taken into consideration when adopting a prevention strategy:



Among existing solutions, we note in particular :

- relying on a watchman performing rounds, the use of fences, video monitoring systems, anti-intrusion alarms or radio wave jamming technology (drones) ;
- strengthening collaboration with police authorities ;
- raising the level of employee awareness to better detect abnormal behaviour and report any observations up the hierarchical chain ;
- auditing of subcontractors or on-site risks (according to the Ineris Institute's guide);
- applying recommendations issued by the ANSSI Agency (https://www.ssi.gouv.fr/) for industrial process control systems and the corresponding computer networks ;
- attention to early-warning information systems (occurrence of malicious acts within a given geographic zone, terrorism alert notified by the SAIP system : http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Lancement-de-l-application-mobile-SAIP, site flyover by unmarked drones, etc.).

? For further information, a statistical accident study dedicated to malicious acts inside industrial facilities may be downloaded from the website: http://www.aria.developpement-durable.gouv.fr/