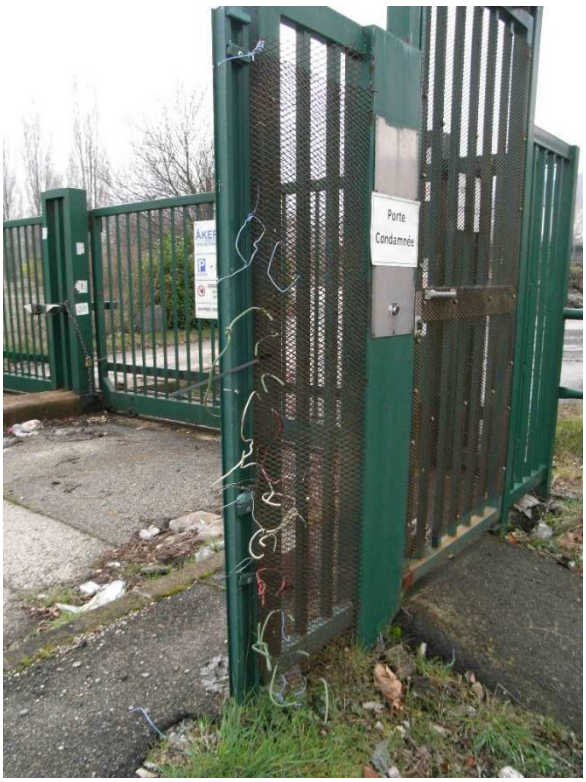
MINISTRY OF ECOLOGY, SUSTAINABLE DEVELOPMENT AND ENERGY



Accident study findings on malicious acts perpetrated in industrial facilities

- October 2015 -



Source : DREAL

ARIA
dgpr srt barpi

Introduction

An industrial accident may be caused in a number of ways. Amongst them, technical (e.g. equipment malfunction, faulty design), human and organisational (e.g. human error, insufficient training, poor organisation) and natural (e.g. lightning, flooding, intense cold weather) causes are often analysed, notably by the BARPI. However, malicious intent can also lead to accidents, whose severity becomes exacerbated since the specific nature of this cause often gets overlooked in risk analyses and safety reports.

Among the most dreaded acts of malicious intent, terrorism is of paramount consideration, whereby certain individuals or organisations seek to use a high-risk installation as a weapon. Such is the purpose of recent governmental edicts regarding the "Seveso" classified facilities. Yet as will be shown in the present document, "ordinary malicious acts" (e.g. theft, arson, deliberate pollution) must also be included as possible accident causes.

This synthesis report is based on an experience feedback analysis and proposes points of heightened vigilance and areas for improvement to protect against malicious attacks. It is addressed first of all to industrial facility operators, who are positioned on the front line of installation protection. These findings are also intended for the government agencies assigned to help resolve these issues. Even though the classified facilities regulations do not specifically target the safeguarding of sites against malicious acts (as the "security" of these installations forms a distinct body of regulations), input from the Classified Facilities Inspectorate also raises the level of protection against such acts. Regulatory prevention efforts underway to benefit classified facilities must serve as well to limit the potential for occurrence and consequences of a malicious act.

Framework of this study

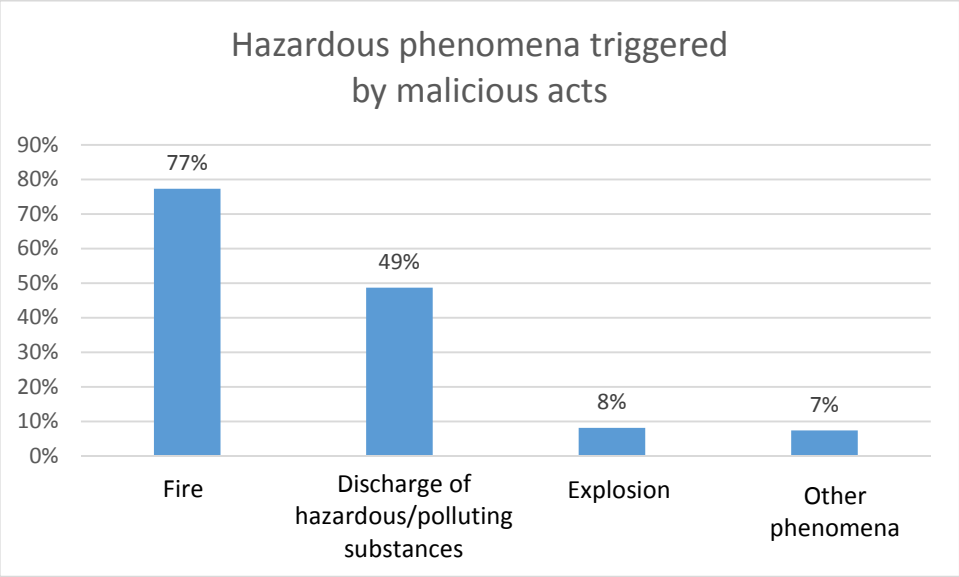
This synthesis report is based on a comprehensive sample of 850 accidents that have occurred in France since 1992 at classified facilities potentially hazardous to the environment (ICPE designation). The most recent accident within this selection dates from 29th June 2015. These 850 accidents represent 4% of the total number catalogued in the ARIA database over this period at French facilities with the same classification.

For purposes of this study, malicious acts will be interpreted in the broadest sense of the term. In addition to accidents directly related to such acts (i.e. carried out with the intention to inflict harm, damage property or cause bodily injury), other accidents occurring subsequent to an intrusion (i.e. site access without permission) were also taken into account. So even if the initial intention of an intrusion is not necessarily to cause harm, still an unauthorised presence often leads to accidental consequences. An analysis of this second category of events provides valuable findings as regards the determination of means for preventing intrusions.
Moreover, events associated with placing prohibited objects or products have been analysed, even if they took place without intrusion (e.g. during a recycling centre's business hours).
Let's note that purposely excluded from this analysis are "farm fires", i.e. accidents occurring in facilities under the jurisdiction of Departmental Civil Protection Agencies (notably recorded under NAF activity codes 01.4 and 01.5).

The summaries of all accidents included in the analysis are available in the document appendix as well as on the ARIA website: http://www.aria.developpement-durable.gouv.fr/?lang=en

Characteristics of accidents involving malicious acts: Key statistics

➢ Hazardous phenomena triggered by malicious acts: “fire” tops the list



A very pronounced trend favouring fire phenomena has been observed. These fires are often combined with a discharge of hazardous / polluting substances in the form of smoke.

In 151 cases (18% of the total sample), a discharge of hazardous / polluting substances (i.e. environmental pollution) actually occurred independently of the fire. One example involved the deliberate opening of valves on a storage tank enabling the product contained therein to flow into the natural environment.

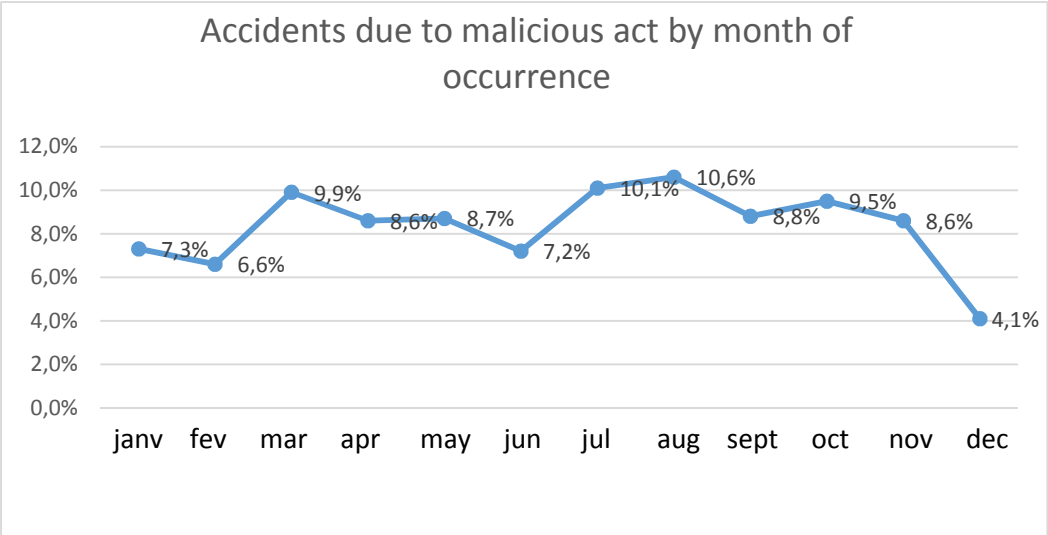
➢ Circumstances leading to malicious acts: beware of idle periods

Period of activity:

According to information held in the ARIA base, the loss-causing event took place during a period of reduced activity in 307 cases (i.e. over 36% of the time). This number is likely to be on the low side since information is not systematically available even if the accident occurred at night, during site closure, with personnel off-duty, etc.

Time of year:

Accidents arising subsequent to malicious acts take place throughout the year with relative regularity. Nonetheless, a **slight increase in their occurrence rates is observed during the summer period, in particular during the month of August**. This is the time of year when many sites actually shut down or at least slow down activity and, as such, are "easier" targets than over stretches of normal operations. On the other hand, a **slight decline is noted in winter** and more specifically during December.



➢ Consequences of these types of accidents

Human consequences in 14% of cases, yet **in general remaining minor** (just 1% of cases involving death, 13.5% with injuries).

Potentially significant social consequences (in 32.5% of cases), with in particular installation of a safety perimeter during the response (14.2% of cases) and personnel redundancies after the loss (15.5%). Redundancies are nearly always required whenever a fire destroys machinery or inventory.

Economic consequences tending to be very serious, as is often the case with "fire" type losses (damage necessitating repair expenses and operating losses in 84% of cases). It is quite rare for damage to extend beyond the site boundary and involve third parties (7.5% of cases have caused property damage to third parties and just over 1% have recorded third-party operating losses). The extent of damage therefore basically remains within the facility targeted by the malicious act.

Environmental consequences in nearly half the cases (46%), with the possibility of polluting the air (28%), surface water or groundwater (14%), or soil (10.9%).

➢ The sectors of activity affected

NAF code	Heading	Examples of affected installations	No. of accidents recorded	Share of total
38	Waste collection, treatment and disposal	Recycling centre, waste sorting facility, storage installation, automobile scrapyard, waste treatment facility	182	21.4%
46	Wholesaling (excluding	Warehouses/depots containing finished products of various types: furniture and household electrical appliances, cereals,	62	7.3%

	automobiles and motorcycles)	phytosanitary products, fertiliser, building industry equipment and materials, chemicals, pharmaceuticals, wood treatment products, shoes, fruit		
45	Sale and repair of automobiles and motorcycles	Mechanics, automobile sheet metal / paint shops, bodywork shops, auto dealers, spare parts warehouses	51	6%
47	Retailing (excluding automobiles and motorcycles)	Shopping centres, supermarkets and affiliated filling stations Specialised stores: hardware-DIY, gardening, electrical appliances	49	5.8%
52	Warehousing and ancillary transport-related services	Warehouses, hangars, logistics platforms	49	5.8%
20	Chemical industry	Factories producing paints, varnishes, fertilisers, pesticides, other agrochemical products, perfumes and personal hygiene products, plastics	35	4.1%
25	Metalwork (excluding machinery and equipment)	Factories outputting metal items (tooling, springs, screws, metal packaging), sheet metalwork, metal treatment and coating firms	35	4.1%
16	Woodworking and manufacturing of wood and cork articles	Joinery shops, sawmills, pallet/crate plants	33	3.9%
10	Food processing industry	Dairies, meatpacking plants, canneries, industrial bakeries, meat curing	32	3.8%
YY	Other	-	322	37.9%

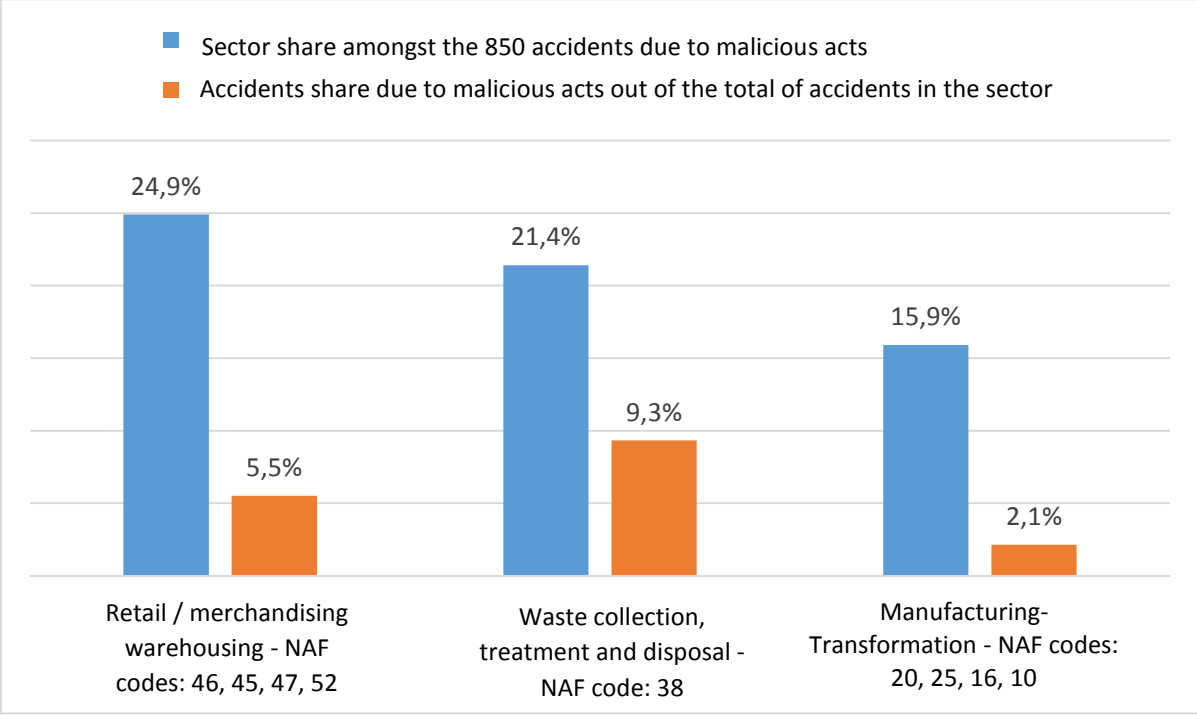
The **sizeable share attributed to the waste collection and treatment sector (NAF code: 38)**, which represents over 20% of all cases, is noteworthy, as is that of merchandise retailers and warehouses (NAF: 46, 45, 47, 52), amounting to some 25%.

The industrial **manufacturing-transformation** sector **(NAF codes: 20, 25, 16, 10)** accounts for approx. 16% of all cases.

For each of the major industrial sectors identified, in calculating the share of accidents associated with malicious acts compared to the total number of recorded accidents (in still focusing on French accidents since 1992 at potentially hazardous classified facilities), it can be noted that the waste management sector remains in first place. Overall, 9% of accidents arising in this sector are tied to malicious acts. For the other sectors, the ranking is slightly altered compared to the previous table.

NAF code	Heading	Number of accidents involving malicious acts	Total number of accidents	Accidents due to malicious acts as a % of total accidents
38	Waste collection, treatment and disposal	182	1950	9%
45	Sale and repair of automobiles and motorcycles	51	734	7%
47	Retailing (excluding automobiles and motorcycles)	49	810	6%
46	Wholesaling (excluding automobiles and motorcycles)	62	1255	5%
52	Warehousing and ancillary transport-related services	49	1033	5%
25	Metalwork (excluding machinery and equipment)	35	929	4%
16	Woodworking and manufacturing of wood and cork articles	33	1301	3%
10	Food processing industry	32	1495	2%
20	Chemical industry	35	2555	1%

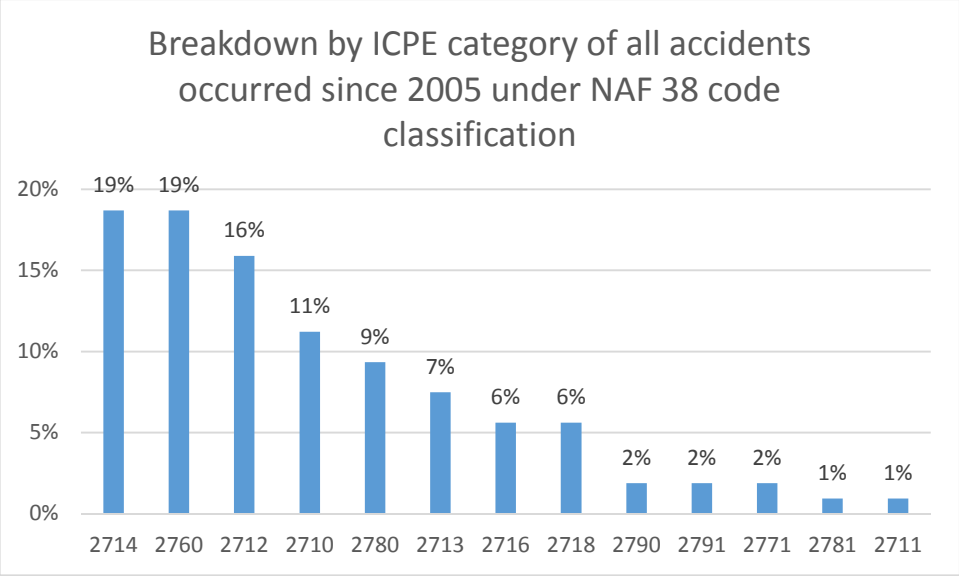
The following histogram depicts these various observations.



Accidents tied to malicious acts in the waste management sector (NAF code 38)

Fires are involved in 89% of all accidents reported subsequent to malicious acts. A **discharge of hazardous or polluting substances**, whether combined with fire or on its own, occurred in **59% of all cases**.

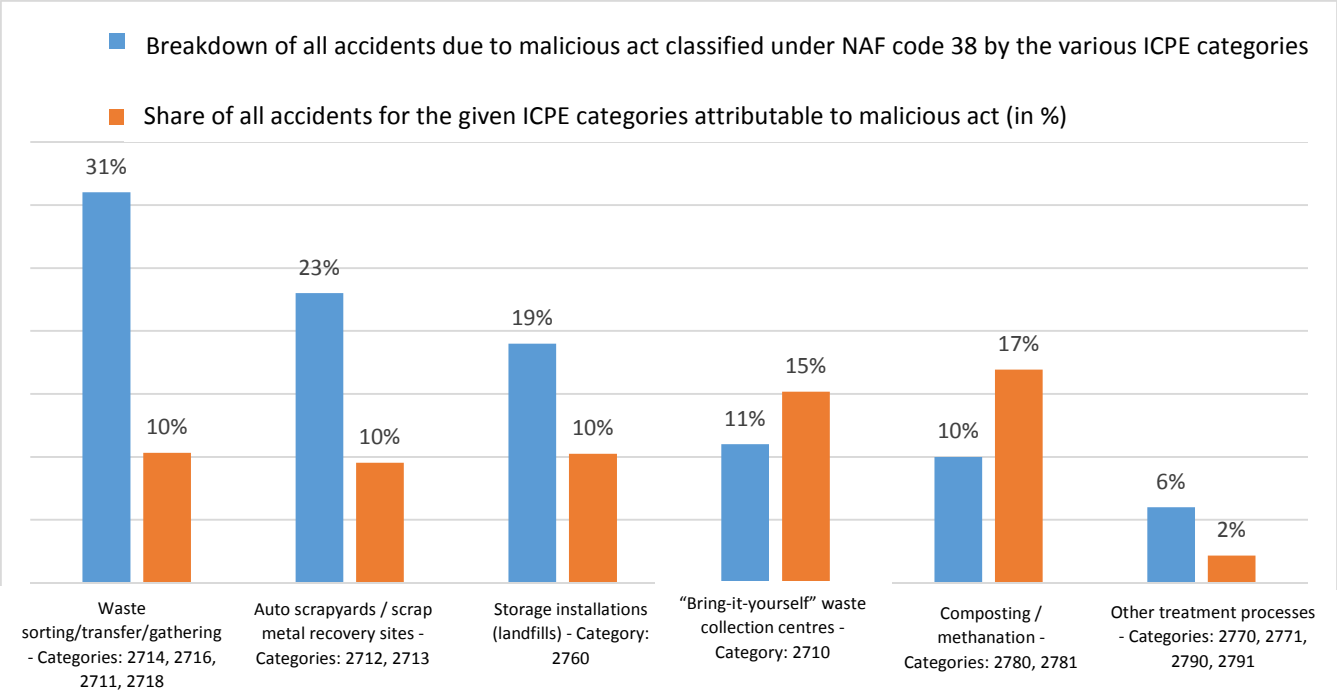
For a more detailed view of this fairly large sample (182 accidents), it is useful to examine the breakdown of events vs. classified facility (ICPE) category for sites where the accidents occurred. Out of the 107 accidents recorded at ICPE facilities assigned NAF code 38 since 2005, the following distribution is found.



By aggregating according to activity typology, the results are as follows:

Aggregated activity categories	Pertinent ICPE category codes	Number of accidents	Share of total accidents ascribable to malicious acts for NAF code 38 (%)
Waste sorting / transfer / gathering	2714, 2716, 2711, 2718	33	31%
Auto scrapyards / scrap metal recovery sites	2712, 2713	25	23%
Storage facilities (landfills)	2760	20	19%
“Bring-it-yourself” collection centres	2710	12	11%
Composting / methanation	2780, 2781	11	10%
Other types of treatment	2770, 2771, 2790, 2791	6	6%

The following histogram shows this distribution, in adding for each aggregation of activities the significance of accidents involving malicious acts with respect to all accidents recorded.



- **Sorting / transfer / gathering of both hazardous and non-hazardous waste (excluding scrap metal recovery sites applicable to category 2713)**

All waste sorting/transfer/gathering centres are concerned by malicious acts, regardless of the type of waste being managed. **For solid waste, the losses experienced pertain to material combustion**, whose origin typically remains unknown.

Let's note that sites containing scrap tyre stockpiles are targeted at a greater frequency. These accidents lead to the release of potentially toxic black smoke containing carbon particles and perhaps traces of benzene and chlorine (ARIA 3688, 11957, 17628, 23334). Fires that break out at plastics storage sites can also generate highly polluting smoke (ARIA 3861).

The storage / gathering of **liquid waste** with hazardous or polluting properties is often the target of malicious acts intended to express neighbouring residents' vehement opposition / protest. Such acts typically lead to **discharging these substances into the environment** and wind up causing an environmental pollution incident. Examples include:

- Deliberate spreading of oils in storage/warehousing facilities for used oils (ARIA 4146, 8960, 20311, 14007, 12871);
- Deliberate opening of valves on tanks containing methanol, xylene and ARIA-rated used solvents at a hazardous waste recovery centre (ARIA 27864).

- **Automobile scrapyards and metal waste sorting/transfer/gathering centres**

These sites are the target of malicious acts primarily motivated by the **theft of auto parts or scrap metal**. In many cases, vandals set fire to the site after committing their crime (ARIA 38989). Such fires cause the release of highly polluting black smoke.

- **Storage centres (landfills)**

These installations are a front-line arson target. The two most common reasons cited for such malicious acts are: **protest against the nuisances** created by the particular establishment, and attempted **theft** (e.g. igniting copper wire sheathing to steal the copper, ARIA 25169).

Other types of malicious malfeasance however have also been detected:

- Deliberate discharge of polluting substances
    - deliberate perforation of a hose used to supply diesel to the site's fleet, subsequent to the theft of a fuel oil tank (ARIA 3923);
    - vandalism at a leachate treatment plant causing pollution of the aquatic medium (ARIA 22537);
    - vandalism on a lift pump discharge line resulting in aquatic pollution (ARIA 35759);
- Illegal dumping of banned hazardous products, e.g. a stripping compound containing hydrochloric acid (ARIA 30185).

- **Waste collection centres ("bring-it-yourself" collection centres)**

These facilities are visited by **intruders looking for objects or products capable of being resold** (ARIA 30631, 35698). Here again, such intrusions often conclude by purposely setting fire (ARIA 35698, 45709). They almost always occur at night (ARIA 45286, 45281).

The harmful event might also entail **disposal of a banned object** simply as a means of discarding it, e.g. detonators (ARIA 39004, 70860), shells (ARIA 40043, 44325), warning flares (ARIA 40102), hot ash (ARIA 46279). In some instances, these discarded objects or products are the direct source of the loss event (ARIA 46279, 39004).

- **Composting / methanation**

Sites dedicated to the biological treatment of waste are specifically targeted by arsonists (ARIA 36919, 40349, 45879, 45940, 34221).

- **Other types of material treatment**

Waste treatment facilities affiliated with actual industrial plants (classified under the codes 2770, 2771, 2790 and 2791) are globally equipped with efficient means of protection and hence significantly less vulnerable than open-air sites, like waste storage depots or composting platforms (6 cases in all).

Accidents involving malicious acts in the sectors of manufacturing and selling goods (NAF codes 46, 45, 47, 52, 20, 25, 16, 10)

The accidents arising in these sectors subsequent to malicious acts closely resemble one another in terms of typical scenarios and motives.

Fires are involved in 83% of accidents triggered by malicious acts. Examples include:

- In the wholesaling sector (NAF 46): ARIA 4471, 11864, 38903
- In the sector of automobile and motorcycle sales and repairs (NAF 45): ARIA 19763, 21838, 33480. This category frequently involves the combustion of tyre stockpiles. The same toxic smoke danger is dealt with here as in the case of scrap tyre fires in facilities classified under NAF code 38.
- In the warehousing sector (NAF 52): The most frequently cited case is a blaze ignited in an abandoned warehouse or hangar (ARIA 7422, 11222, 14833, 18482). Outdoor storage of pallets and containers is also often targeted (ARIA 13479, 32248).
- In the chemical industry (NAF 20): ARIA 7485, 10584. These incidents tend to involve the burning of chemical products.
- In the metalwork sector (NAF 25): ARIA 6359, 14165, 31446

The motives giving rise to malicious acts are not always known. It would appear however that **theft is a very powerful one** behind intrusions (ARIA 4283, 4480, 24640, 31218, 24640, 39958).

- In the retailing sector (NAF 47): thefts mainly occur in the supplies, inventory or even in supermarket cold storage rooms, which happen to be the least well monitored zones and where merchandise is stored (ARIA 23355 10057 14230 16539 28023, 29033). Offenders also sometimes take advantage of delivery schedules, when the merchandise is still in bulk packaging on pallets (ARIA 23744).
  Even when left derelict or undergoing demolition, supermarkets remain in thieves' line of sight, mainly for the copper contained in old transformers (ARIA 19041, 19076, 35546, 39865). These acts of vandalism systematically allow PCB to pollute soil and water.
  Filling stations are the scenes of attempts to steal fuel, some of which may wind up polluting the environment (ARIA 5595).

- In the chemical industry (NAF 20): Some chemical substances featuring special properties attract wrongdoers (e.g. explosives ARIA 34096). Such thefts may be committed without any hazardous phenomenon taking place as a result of the intrusion (ARIA 25665, 34096).

- In the metal manufacturing sector (NAF 25): The motivation here would be to steal metals or chemical substances used in the metal manufacturing or treatment process (ARIA 23459). These installations also experience many vandalism incidents perpetrated on transformers (ARIA 5844, 18484, 25142, 33107, 40316, 40609, 41022).

Quite often, **intruders set fire to the installation after committing a theft** so as to eliminate all traces of their misdeeds (ARIA 39958, 17516). This tendency further increases the frequency of fire.

Thefts however can degenerate into environmental pollution by means of discharging hazardous or polluting substances:

- The illegal removal of transformers leads nearly systematically to environmental pollution (a Pyralene spill) ARIA 4283
- The opening of valves on hydrocarbon storage tanks in order to recover contents also causes

environmental pollution ARIA 4480.

Overall, for accidents subsequent to a malicious act occurring in a sector coded as NAF 46, 45, 47, 52, 20, 25, 10 or 16, **hazardous or polluting substances are discharged 42% of the time**. In 27% of cases, the discharge consists of smoke released from fires. In the other 15% of these discharges, physical pollution serves as the main objective behind the malicious deed and occurs independently of fire. The discharged substances may be:

- the materials produced by the company or introduced as an input during the manufacturing process (discharge of chemical products from chemical plants - ARIA 9341, 25704, 36767, 37129, 18335 or food processing plants - ARIA 40645, 13756);
- or hydrocarbons, whose pollution potential is well known: discharge of lubricating oils from garages (ARIA 15031, 12444, 35355), discharge of quenching oils and lubricants from metal factories (ARIA 12736, 20134), discharges of fuel oil / diesel in facilities across all sectors of activity (ARIA 30747, 40645, 30535, 31592, 20814, 32038).

Summary of the typological classification of malicious acts

➢ Wide-ranging motives

As a summary of the cases presented above, below is a recap of the primary motives identified during the perpetration of malicious acts. Some are more generic while others more specific to the type of targeted installations.

- Malicious acts **intended to express disapproval within the scope of issues surrounding local acceptance of the particular facility**
  - Such a situation is frequently encountered in the waste sector, where installations may generate nuisances for neighbouring residents (an eyesore, pungent smells, smoke releases, handling of substances considered noxious with the fear of contamination should an accident occur). Neighbours sometimes become exasperated by poorly managed sites creating repeat problems (aquatic pollution). Among the types of installations drawing the most ire, let's cite: used oil treatment plants (ARIA 4146, 8960), tyre recovery centres (ARIA 35408), and methanation plants (ARIA 37842).
  - Acceptance also proves to be a challenge in other sectors (e.g. a sawmill experiencing problems with the local community, victim of malicious acts ARIA 20814).

- Malicious acts perpetrated **to discard cumbersome or hazardous objects/products**
  - This concern is specific to waste management facilities serving as preferred disposal sites for individuals seeking to throw away objects or products of all sorts (cans of stripping agent, detonators, shells, radium lightning rods, etc.).
    Examples: ARIA 30185, ARIA 39004, 70860, 40043, 44325,41589, 46279

- Malicious acts for the purpose of **stealing materials or objects with resale value**
  - These thefts may occur in waste recovery facilities and concern in particular:
    - Metals (ARIA 25169, 31596 17628)
    - Any other product capable of being resold or recycled (cans of acid and cyanide, WEEE, auto parts), ARIA 30631, 45709, 38792, 38989;
  - They are however committed in installations that manufacture or store substances or finished products. Topping the list are:
    - Stolen metal (ARIA 23459), especially copper in transformers (ARIA 4283, 5844, 32478, 33740, 19041, 19076, 35546, 39865).
    - Stolen hydrocarbons (ARIA 4480, 10148), especially fuel from filling stations (ARIA 32038, 5595).
    - Stolen chemicals (ARIA 25665, 23459). Note that thefts of substances with explosive properties (aluminium powder, as a potential ingredient in explosives manufacturing - ARIA 24426, 31218; stolen nitromethane - ARIA 34096). These thefts raise suspicions of criminal intent.
    - Thefts of various staples in supermarket stocks, inventory and cold storage rooms: ARIA 23355 10057 14230 16539 28023, 29033.
    - Other examples concerning respectively the theft of precious woods, fertilisers and computer hardware: ARIA 24640, 38699, 27037.

- Malicious acts as a **demonstration towards resolving labour disputes in the company**. Stories of malicious acts committed by an employee in conflict with his/her employer, or a disgruntled laid off employee seeking revenge abound in all sectors. These acts can also stem from collective initiative (e.g. during a strike period):
  - Examples in waste management facilities: ARIA 20249, 21024, 21003, 36905
  - Examples in other sectors of activity: ARIA 31501, 34085, 43518, 17516, 32297, 18335,

36767, 37920, 40059.

- Malicious acts as a sign of "**solidarity" during a massive labour movement** (without any direct relation to the targeted industrial site). Let's cite for example an accident due to malicious acts that arose against the backdrop of widespread urban violence in Villiers-le-Bel in 2007 (ARIA 33924). Similar examples show that industrial sites may be attacked during clashes with police (e.g. following a demonstration: ARIA 35977, 30967).

- Other less frequent situations also deserve mention. In this category would be malicious acts based on **ideological grounds**. Isolated cases have been recorded, such as the attack in a company working with Kosher products (ARIA 35920). Such acts can also be intended to "**cover tracks**". This explained a fire set at an industrial caterer that was submitted to an investigation subsequent to a listeria epidemic. The authorities suspected a criminal act intended to destroy evidence (ARIA 17285).

- Let's not overlook the fact that some malicious acts are committed purely to **inflict harm**. These acts of vandalism or gratuitous violence may be the work of psychologically unstable individuals (ARIA 23756, 40050, 4118), or else children or adolescents (ARIA 17563, 41031, 24976, 35355 13209).

- On the other hand, accidents ascribed to malicious acts may also in reality be **accidental drifts** subsequent to an imprudent gesture by children/teens without necessarily the desire to cause harm (ARIA 38988, 20564, 35497, 32371, 43714). For example, a group of youth illegally entering a plant make a fire to keep warm and unintentionally set the place ablaze (ARIA 35551). Adults are also capable of instigating accidental drifts as a consequence of poor understanding of risks (ARIA 43353: a warehouse watchman seeking to "verify" whether or not plastic is flammable starts a fire).

- Lastly, let's note those cases where malicious acts carried out in industrial facilities serve a purpose of suicide or murder (e.g. by spraying and igniting fuel in filling stations, ARIA 40890, 41043).

➢ Simple, yet "efficient" methods

For closed installations (like a warehouse or supermarket), intrusions often rely on a battering-ram vehicle used to break down the doors of the establishment (ARIA 24577, 36122, 41592, 28662, 21441, 23997, 38133).

In the case of a deliberate discharge of substances to cause environmental pollution, the methods are almost always the same: opening of valves (ARIA 29857); spilling of a receptacle's contents, e.g. barrels (ARIA 36767, 37129, 18335), a car's gas tank (ARIA 31738); damaging of pipelines to create a leak (ARIA 9341, 25704).

The methods used are more varied for accidents involving fires or explosions.

In the waste management sector, the recurring methods are: directly igniting waste stockpiles often containing easily combustible substances (ARIA 3688), or bringing a car on-site, whether or not stolen, and then burning it (ARIA 14908, 33043).

Other techniques have been identified in all types of installations:

- attack from the outside by throwing a Molotov cocktail (ARIA 35920, 38432, 12160, 31684, 36116), fireworks rocket (ARIA 14230) or another type of fire bomb (ARIA 39232);
- attack by use of hazardous products or objects present on the site being visited. Examples include:
    - in supermarkets and filling stations: ignition of gas bottles (ARIA 38397, 41863, 45899);
    - at a chemical plant: opening of valves on ethylene glycol storage tanks and ignition of burning vapours (ARIA 3809);
- firing after sprinkling with gasoline (ARIA 14807, 14370, 34640, 20000).

A special case that warrants our attention pertains to malicious acts undermining an industrial process. Such an example (and one that has been repeated) in the ARIA base occurred at a metal surface treatment plant. Cyanide was introduced in excessive quantities into rinsing baths (ARIA 16025, 16040). This case has not been detailed, but it could be assumed that the objective sought was actually to undermine the treatment process implemented by the firm.

➢ Evidence of entry or helpful clues at the time of investigation

The kinds of recurrent proof uncovered during investigations can indicate the presence of a malicious act:

- Traces of intrusion:
    - Broken or forced doors, gates, windows or padlocks (ARIA 22433, 30630, 35698, 23459, 45709, 14165);
    - Holes in fences or gratings (ARIA 25297, 43466, 36919, 25169, 41008).

- Presence of multiple fire sources, eliminating the hypothesis of an accidental fire outbreak. This scenario is very frequent for fires in waste stockpiles (ARIA 7178, 12011, 12957, 13235, 15182, 15276, 20249, 23451, 34224).

- Occurrence, over a short period, of several similar fires in the vicinity or even at several sites belonging to the same industrial group (in installations specific to the waste sector: ARIA 7178, 45281, 21024; in other business sectors: ARIA 13045, 7303, 21630, 42631, 38675).

- Discovery of flammable elements or elements triggering pollution, like empty gasoline cans (ARIA 20000), open valves (ARIA 29857), dismantled fuel oil tank spray gun and hose (ARIA 32038).

- Disappearance of valuable objects.

- A situational context favouring intrusions, e.g. event triggered during a period of site closure (ARIA 23639), following departure of the watchman (ARIA 25297), and after a vocal demonstration by neighbours (ARIA 35408).

- Fire protection water supplies emptied beforehand (ARIA 20468).

Vulnerabilities revealed by malicious acts

A number of common site-related factors can be highlighted regarding the targets of malicious acts. Ill-intentioned individuals are in fact taking advantage of deficiencies in the level of site protection. The main deficiencies inventoried are as follows:

- **Insufficient maintenance of enclosures and access controls**

  The fences of many waste management sites are in a poor state of repair or missing altogether.

  Examples: ARIA 3688, 17563, 23451, 22441, 38556 24982

  In some instances, the fence is present but substandard operating practices prevent anti-intrusion systems from working properly. For example, placing devices along the fence might interfere with the anti-intrusion cell beam transmission (ARIA 28786).

  This type of problem is also encountered however in high-risk industrial installations. In July 2015, a child was able to penetrate into a lower-tier "Seveso" oil refinery in the Languedoc-Roussillon Region to chase down a wayward balloon He passed through a hole in the fence created by corrosion. This event, which had no adverse consequences, reveals a sometimes inadequate level of attention paid to maintaining fences and controlling access. This lackadaisical attitude relative to a site's anti-intrusion protection is also illustrated by accident ARIA 32129: video recording malfunctions lasting several days had been detected by the refinery operator but remained unresolved, leaving an opening for vandals.

  In addition, below are a few examples showing blatant defects in anti-intrusion protection, enabling unrestricted access to sites storing hazardous products:

  - At night, deliberate opening of valves on tanks of methanol, xylene and used solvents in a hazardous waste recovery firm, ARIA 27864;
  - Fire in a tank containing solvents of the type toluene, isobutyl acetate and ethylene glycol at a site neither enclosed nor monitored, ARIA 3809;
  - Intrusion into a room storing benzene and toluene-based products, ARIA 5518;
  - Theft of hazardous products, despite being stored in a locked container, inside a recycling centre, ARIA 30631;
  - Leak of a malicious origin on a cryogenic oxygen tank in a metalwork factory, ARIA 35058.

  Attention must also be paid to cases of "unregulated" or non-compliant sites, which often lack sufficient monitoring relative to the intrusion risk (ARIA 23334, 16366). This is the tell-tale sign of poor overall safety management.

- **Absence of site surveillance during idle periods**

  Intruders often opt to act at night or during periods of site closure or temporary shutdown. The absence of a watchman or other surveillance mode at these times is a common error in the waste management sector.

  Examples: 36739, 22441, 33433, 40278, 40349, 43972

  When wrongdoers confident of being able to act freely meet a human presence, they may resort to violence (ARIA 39958).

- **Unsecured closed sites**

Sites left derelict or abandoned following a business liquidation or shutdown are preferred targets for looters. Valuable products or goods are in fact sometimes held on-site even after operations have been completely halted. The lack of monitoring and anti-intrusion protection measures clears the path for malicious-minded individuals. This configuration is encountered across all business sectors.

Below are a few examples related to a lack of security during activity shutdown:

- Intrusion at the site of a former chemical plant still containing many hazardous product storage zones, yet devoid of a safety system, ARIA 37129;
- Explosion in a former joinery shop that had not been secured following closure (no chemical product disposal or access restrictions in place), ARIA 32371.

Other examples: ARIA 4754, 22433, 40543, 11957, 31596, 44620, 44373.

- **Vulnerable equipment without proper protection**

At times, site operators fail to protect their vulnerable equipment or materials. The first configuration to cite is that of outdoor storage. Whether in the waste sector or production/sales activities, these areas lacking any built protection are often targeted.

Examples: ARIA 13235, 15182, 20249, 25383, 30850, 31738,35060, 40704, 31731, 35242, 31414, 25192

The concern is identical for storage sites located at the property boundary, adjacent to enclosure walls capable of being penetrated without drawing attention.

Examples: ARIA 37218, 45879, 37869

On the whole, questions are raised over the geographic locations of certain sites, i.e. surrounded by empty countryside and regularly subjected to surveillance problems (ARIA 33043, 45940). Such is also the case for very extensive sites that are therefore challenging to monitor and entirely enclose (ARIA 36003, 36205).

Even in places that seem to be heavily frequented, e.g. supermarkets, some zones are plagued by inadequate monitoring. This is true of supply rooms and inventories, which are often targeted by thieves. Examples: ARIA 23355 10057 14230 16539 28023, 29033

- **Neglect of whistle blowers and experience feedback**

Many examples highlight an insufficient acknowledgment of lessons learnt from past events. Repeat accidents due to malicious acts occur at these sites, even though they likely could have been, at least partially, avoided.

- Absence of monitoring at a recovery site despite several alarming events (site degradation, thefts of scrap metal and pallets). The pallets had been left outside, ARIA 40704.
- Absence of corrective measures at an automobile scrapyard despite fence height non-compliance being cited several years prior, ARIA 45512.
- Absence of heightened surveillance at the unloading dock of a waste recycling centre: disposal of ordnance at a site already known for discarding grenades, ARIA 40043.
- Failure to install a fence in spite of several malicious events carried out inside a waste recovery firm, ARIA 17563.
- Many other cases of sites experiencing repeat malicious incidents: ARIA 16366, 17563, 31798, 40739, 41206, 44216, 4414, 44216, 33480

A few examples of corrective or preventive measures addressing malicious acts

Comment: The following proposals are in no way meant to be exhaustive. They are to be taken as leads for strategizing based on the main set of deficiencies noted at sites victimised by malicious acts. These recommendations are not always applicable in their entirety; they obviously depend on the site layout and the range of products being handled.

- Installation and reinforcement of fences (replacement of gratings by metal cladding, a concrete shell, addition of barbed wire, etc.) and regular verification of their structural integrity (ARIA 43471, ARIA 18884, 44945).
- Securing of sites that are closed or derelict: shuttered, boarded-up entrances (ARIA 44373).
- Reinforcement of control procedures: site access, closure of building and site ingress / egress (ARIA 35292).
- Introduction or enhancement of instrumented surveillance systems: anti-intrusion alarm, remote / video monitoring, motion or heat detection systems (ARIA 45709).
- Set-up or consolidation of a guard service (increased frequency of rounds; transition to a canine-assisted watchman).
- Securing of sensitive storage sites and equipment.
- Removal of sensitive equipment (e.g. electrical installations) in order to more easily provide for protection; special procedures for maintaining isolated zones whenever a plant encompasses a large floor area (ARIA 34508, 24981).
- Reorganisation of storage sites and, if possible, elimination of open-air storage cells, construction of fences / roofs around high-risk cells (ARIA 26857, 39860).
- Awareness-building in order to avoid intrusions or acts without harmful intent, e.g. information to recycling centre users on the risks associated with dumping banned objects (ARIA 44325, 46279).
- Consolidation of the safety function, e.g. creating and filling the post of Head of Safety (ARIA 3809).
- Enactment of measures to prevent aggression to the natural environment in the event of an on-site malicious act, e.g. closure of the site's confinement basin valve over the weekend to avoid any environmental pollution subsequent to an unauthorized product flow (ARIA 29857).

Conclusion

Industrial sites are tempting targets for ill-intentioned individuals. Given the often substantial consequences associated with these malicious acts, the risks incurred by such a threat must not be taken lightly.

Beyond "conventional" malicious attacks, whose aim is to steal materials or goods or else to express disapproval (problem with neighbours, vengeance against a former employer), **new forms of attacks** are always developing.

In the highly charged geopolitical context shaping the beginning of this new century, industrial facilities may become the target of extremist organisations (see the event that occurred on 26th June 2015 at a chemical products plant in Saint-Quentin-Fallavier, Isère Department). Flyovers of industrial sites and nuclear power plants by drones will expand.

In light of these new threats, site operators must be extra vigilant and draw the most lessons possible from past events.