Roma, 25 January 2018

WATER SERVICES MANAGEMENT

SECURITY MANAGEMENT
DETECTION AND RESPONSE TO EXTERNAL AGGRESSIONS

Renato
Drusiani

UTILITALIA

WHO IS UTILITALIA

imprese acqua ambiente energia

UTILITALIA is the Italian National Association of Companies operating in the public services of Water, Environment , Energy, representing them at national and international institutions.

Served population by UTILITALIA Members

Water Services (drinkwater and wastewater)	*76 %*
Environmental Services (solid wastes)	*65 %*
Gas Services (natural gas distribution)	*35 %*
Electricity Services (producion and distribution)	*20 %*

UTILITALIA represents over 500 members with about 90,000 employees.

In the field of Water Services UTILITALIA is the Italian Member of:

Eureau (Water European Association)

EurEau

IWA (International Water Association)

IWA the International water association

UTILITALIA offices
Piazza Cola di Rienzo 80/A
00192 Rome

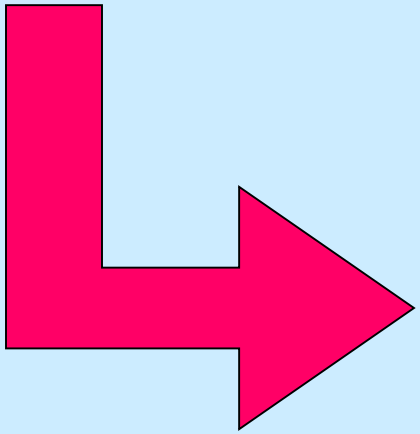
website:
www.utilitalia.it

Infrastruxcture risks and exposure

Origins:

- Natural hazards (flood, earthquake,…)
- Technological hazards
- People-generated unintentional hazard
- People-generated intentional hazard

Normally included in the emergence planning



By:

- Criminal - insane
- Terrorist
- Military operation

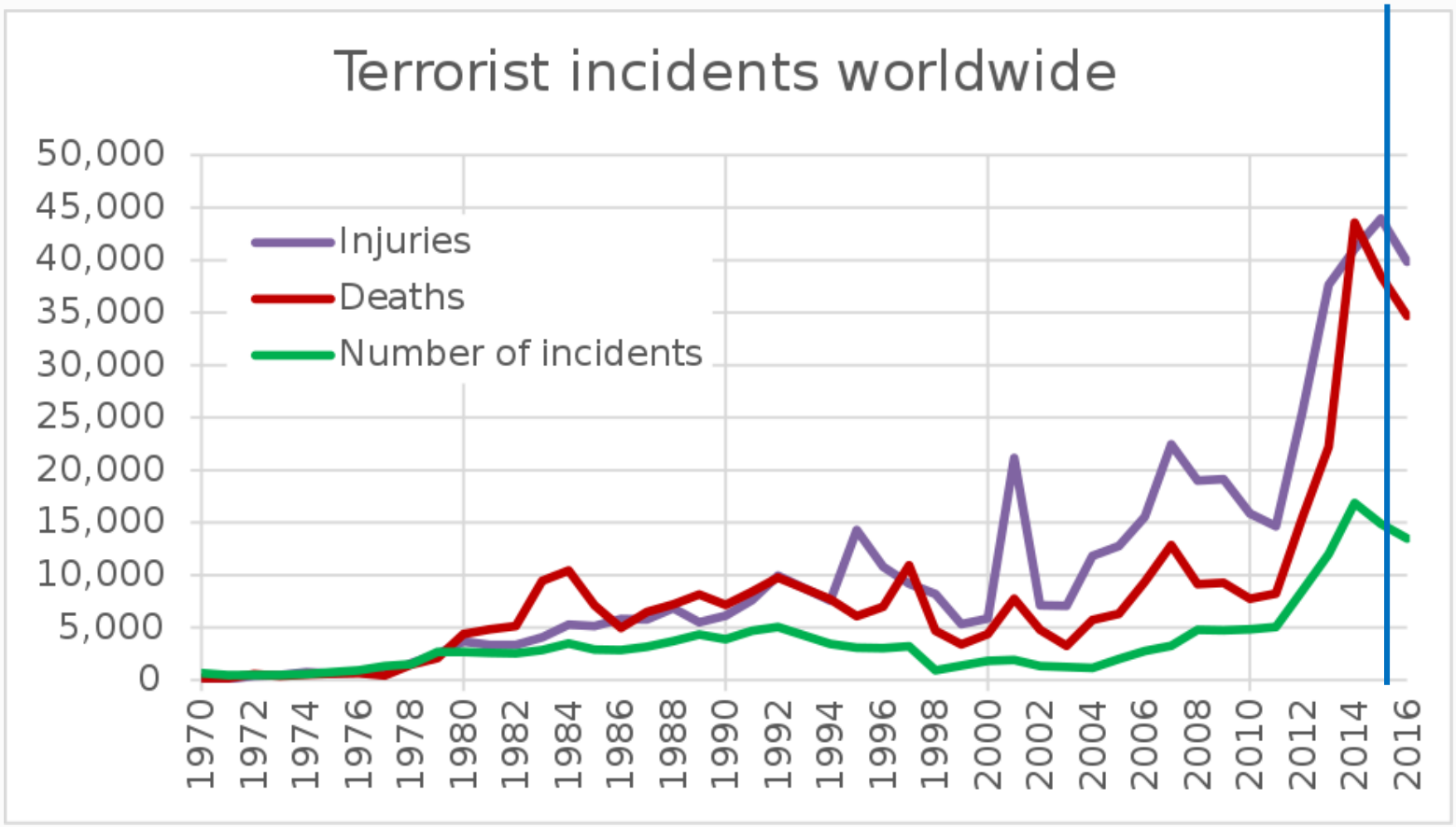
External attack

Possible targets

- Telecommunications Systems
- Electrical Power
- Oil & Gas
- Transportation
- Banking & Finance
- Water Systems
- Government Building
- Symbolic monument
- ……

Global Terrorism Database (GTD)

The *Global Terrorism Database* (*GTD*) is a database including information on terrorist events around the world from 1970 through today. The *GTD* includes systematic data on domestic as well as international terrorist incidents



Targets of terrorist attacks worldwide, 2015

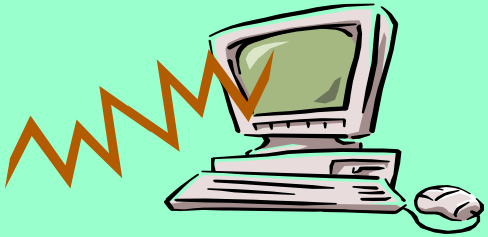
Target Type	Number of Targets
Private Citizens & Property	4514
Police	2159
Business	1149
Government (General)	1136
Military	715
Terrorists/Non-State Militia	447
Religious Figures/Institutions	394
Transportation	381
Educational Institution	297
Utilities	255
Violent Political Party	161
Government (Diplomatic)	148
Journalists & Media	146
Other	145
NGO	53
Telecommunication	46
Airports & Airlines	23
Food or Water Supply	17
Tourists	7
Maritime	6
Abortion Related	5
Total	**12204**

Public services
86 attacks

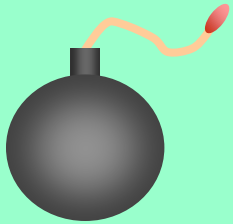
External attack in Water Systems

Possible ways

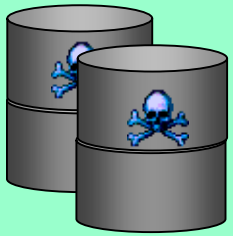
Cyber attack



Explosive/Sabotage

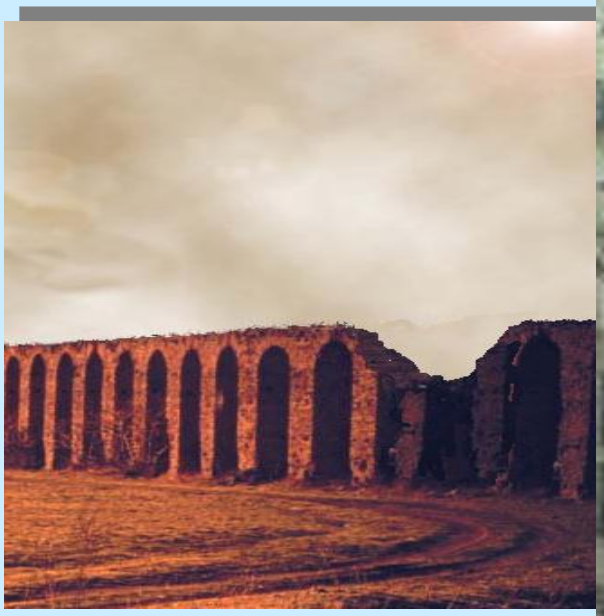


Contamination

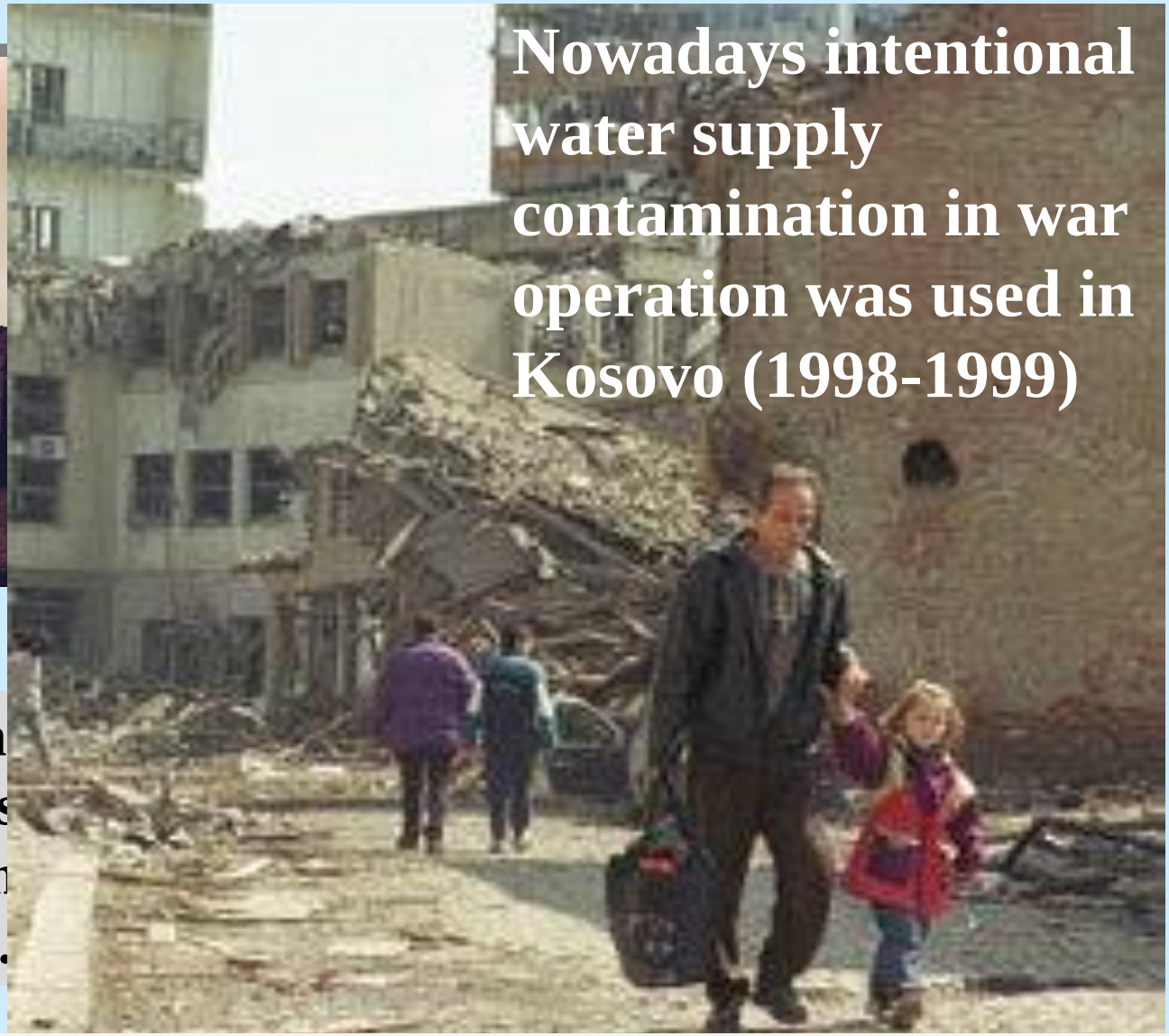


- **Chemical**
- **Biological**
- **Radiological**

History of attack against water supply



Water contamination in military operations was made by Assirian Romans, Greeks, …..



Nowadays intentional water supply contamination in war operation was used in Kosovo (1998-1999)

Protocol on victime of war (Geneve 1949) prohibited attack against water supply (irrigation and civile uses)

WATER CONTAMINATION
Italian Legislation - Penal Code

Art. 438 - Epidemy
Whoever causes an epidemy by pathogenic germs is sentenced to the life imprisonment.

Art. 439 – Water or Food poisoning
Whoever poison water or food before the consumption is sentenced to imprisonment not less than 15 years. If this fact provoques the death of more people it is life imprisonment.

INTENTIONAL DAMAGE TO WATER SYSTEMS
Italian Legislation - Penal Code

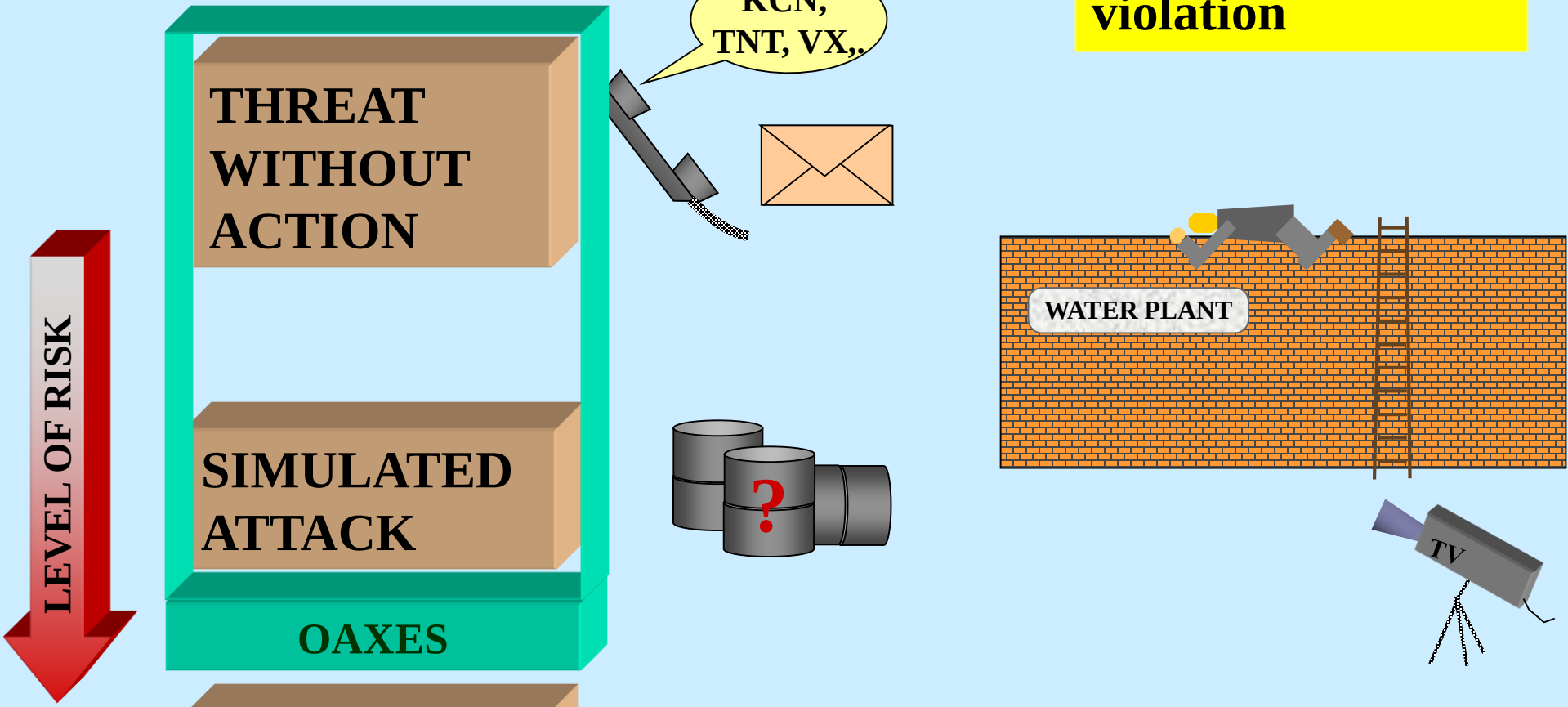
Art. 427 C.P. - Damage followed by flooding, landslide or avalanche

Anyone who breaks, deteriorates in whole or in part, barriers, embankments, dams or other works designed to defend against water, avalanches or landslides, or to collect or conduct the water, for the sole purpose of damage, is punished, if from the fact comes the danger of a flood or a landslide, or the fall of an avalanche, with imprisonment from one to five years ....

DIFFERENT WAYS OF THREAT

Conventional way

Explicit boundary violation



IMPORTANCE OF INFORMATION AT THE BEGINNING

Nowadays anxiety and fear are considered a merchandise we can be selled by mass-media to the population/readers.

This is particulary true if our health can be involved in presence of invisiblee and unexpected events like water contamination.

We can’t forgotten that the great part of events concerning water contamination terrorism are the oaxes.

Not only the real acts but also the simple spread of fear into the population (amplified by mass-media) can be a terrorist target.

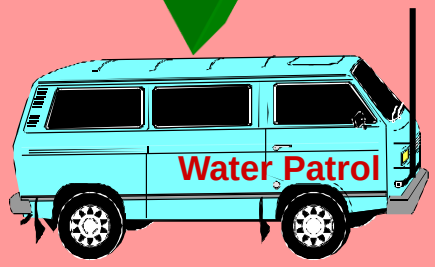
COMUNICATION PROCESS AT THE BEGINNING

Menace arrival

KCN,
VR, VX,..

FAR
DISTANCE
OPERATIONS

First field
tests



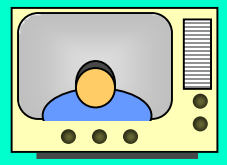
INFORMATION TO
THE AUTORITIES

CRISIS
MANAGEMENT

CRISIS
ROOM

END OF
INTERN
ALLARM

DECISIONS
TO TAKE



"INTERNAL"
INFORMATION

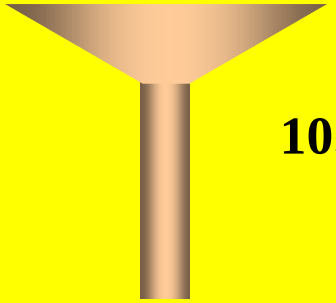
EXTERNAL
INFORMATION

CONTAMINATION

Different agents and different risks

		Accessibility	Use and storage	Monitoring	Effects
C	Chemicals	●●●	●●●	●●	● – ●●
B	Bacteria	●●	●●	●	●●●
	Virus	●	●	●	●●●
	Toxins	●	●●●	●	●●
	Spores	●	●●●	●	●●
R	Radioactive	●	●●	●●	●●●

Performances of contaminants



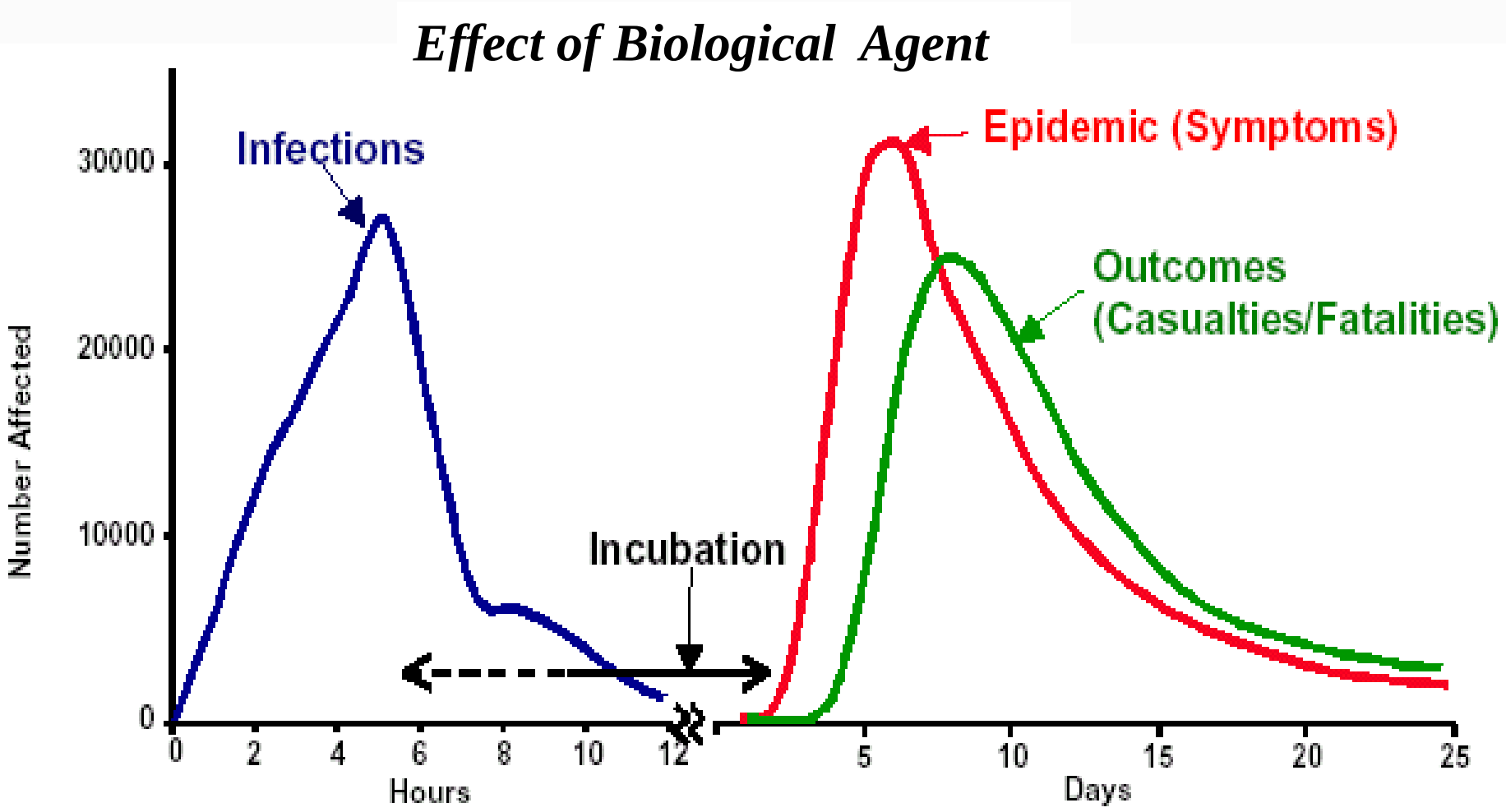
10.000 mc

AGENT USED	*Concentration in mg/litro to be dangerous with 0,5 litri/day*	
Arsenic	**100**	**1.000 Kg** 
Cyanide	**25**	**250 Kg** 
Botulinum toxin	**0,14**	**1,4 Kg** 
Salmonella typhi	**10.000 bact.**	**10 - 50 g** 

Time to outcomes of different agents

C	**Nerve agents**	**Seconds to minutes**
	Blood agents	**Minutes**

B	**Toxin**	**1 - 5 days**
	Bacter.Virus	**2 - 20 days**



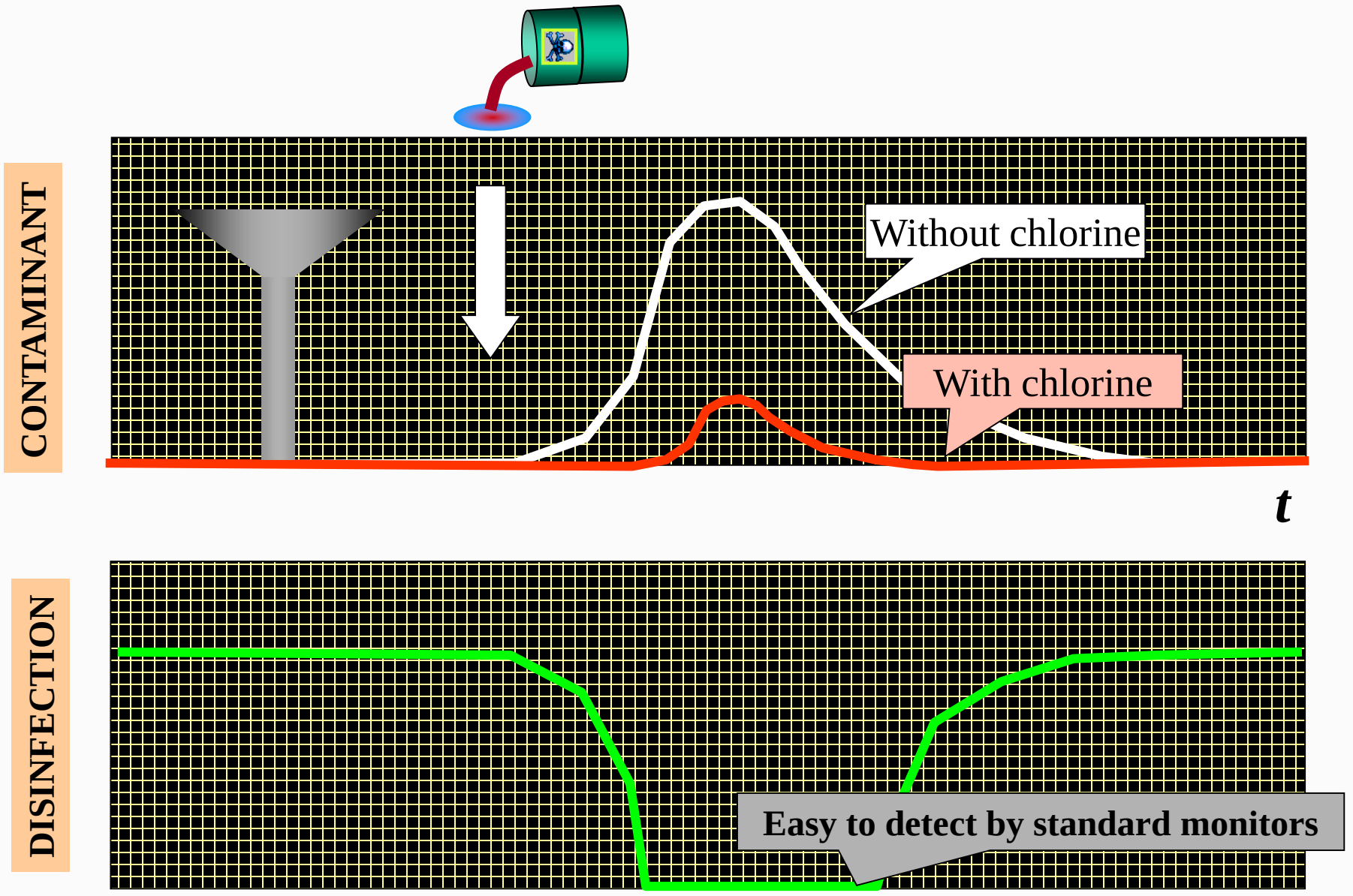
The Dilemma of Biological Agents: Pathogens

AGENT	TYPE	WEAPON-IZED	WATER-THREAT	STABLE IN WATER	INFECTIOUS DOSE	CHLORINE TOLERANCE
Anthrax	B	Yes	Yes	2 yrs spore	6,000	Spores resistant
Brucellosis	B	Yes	Probable	20-72 days	10,000	Unknown
C. *Perfringens*	B	Probable	Probable	Common in sewage	~500,000	Resistant
Tularemia	B	Yes	Yes	< 90 days	25	Inactivated, 1 ppm, 5 min
Shigellosis	B	Unknown	Yes	2-3 days	10,000	Inactivated, 0.05 ppm, 10min
Cholera	B	Unknown	Yes	"Survives well"	1,000	"Easily killed"
Salmonella	B	Unknown	Yes	8 days, fresh water	10,000	Inactivated
Plague	B	Probable	Yes	16 days	500	Unknown
Q Fever	R	Yes	Possible	Unknown	25	Unknown
Variola	V	Possible	Possible	Unknown	10	Unknown
Hepatitis A	V	Unknown	Yes	Unknown	30	Inactivated, 0.4 ppm, 30 min
Crypto-sporidiosis	P	Unknown	Yes	Stable days or more	130	Oocysts resistant

The Dilemma of Biological Agents: Toxins

AGENT	WEAPON-IZED	WATER THREAT	STABLE IN WATER	ESTIMATED EFFECTIVE DOSE	CHLORINE TOLERANCE
Botulinum Toxin	Yes	Yes	Stable	0.07 mg	Inactivated, 6 ppm, 20 min
T-2 mycotoxin	Probable	Yes	Stable	None given	Resistant
Aflatoxin	Yes	Yes	Probably stable	2 mg	Probably tolerant
Ricin	Yes	Yes	Unknown	None given	Resistant at 10 ppm
Staph Enterotoxins	Probable	Yes	Probably stable	4 μg	Unknown
Microcystins	Possible	Yes	Probably stable	1 mg	Resistant at 100 ppm
Anatoxin A	Unknown	Probable	Inactivated in days	None given	Unknown
Tetrodotoxin	Possible	Yes	Unknown	1 mg	Inactivated, 50 ppm
Saxitoxin	Possible	Yes	Stable	0.3 mg	Resistant at 10 ppm

DISINFECTION EFFECT IN WATER



Terrorist threats against drink water years 1999 - 2000

Agent: poison **Type of Event:** hoax
A rumor that the city's water supply in Istanbul, Turkey, had been contaminated with an unknown poison reached the media.

Agent: unidentified chemical **Type of Event:** plot
On 19 June, the newspaper *Yidyout Ahranout* reported that members of Hamas, the Islamic Opposition Movement, had plans to poison water Supplies in Israel with "chemical substances."

Agent: cyanide **Type of Event:** use of agent
On 18 December, seven students at a law school in Springfield, Massachusetts, became ill after drinking water from a cooler that had been contaminated with potassium cyanide.

Agent: poison **Type of Event:** hoax
During the night of 31 December, individuals drove through the streets of Al Kosheh, Egypt, with a megaphone, warning that Christians had poisoned the village's tap water in an effort to kill Muslims. The event was part of an escalating dispute between Muslims and Coptic Christians in the village.

Type of Event: plot **Agent:** unknown poison
On January 23, it was reported that Chechen rebels planned to poison unknown water sources in Chechnya, Russia, in order to harm Russian Federal Forces.

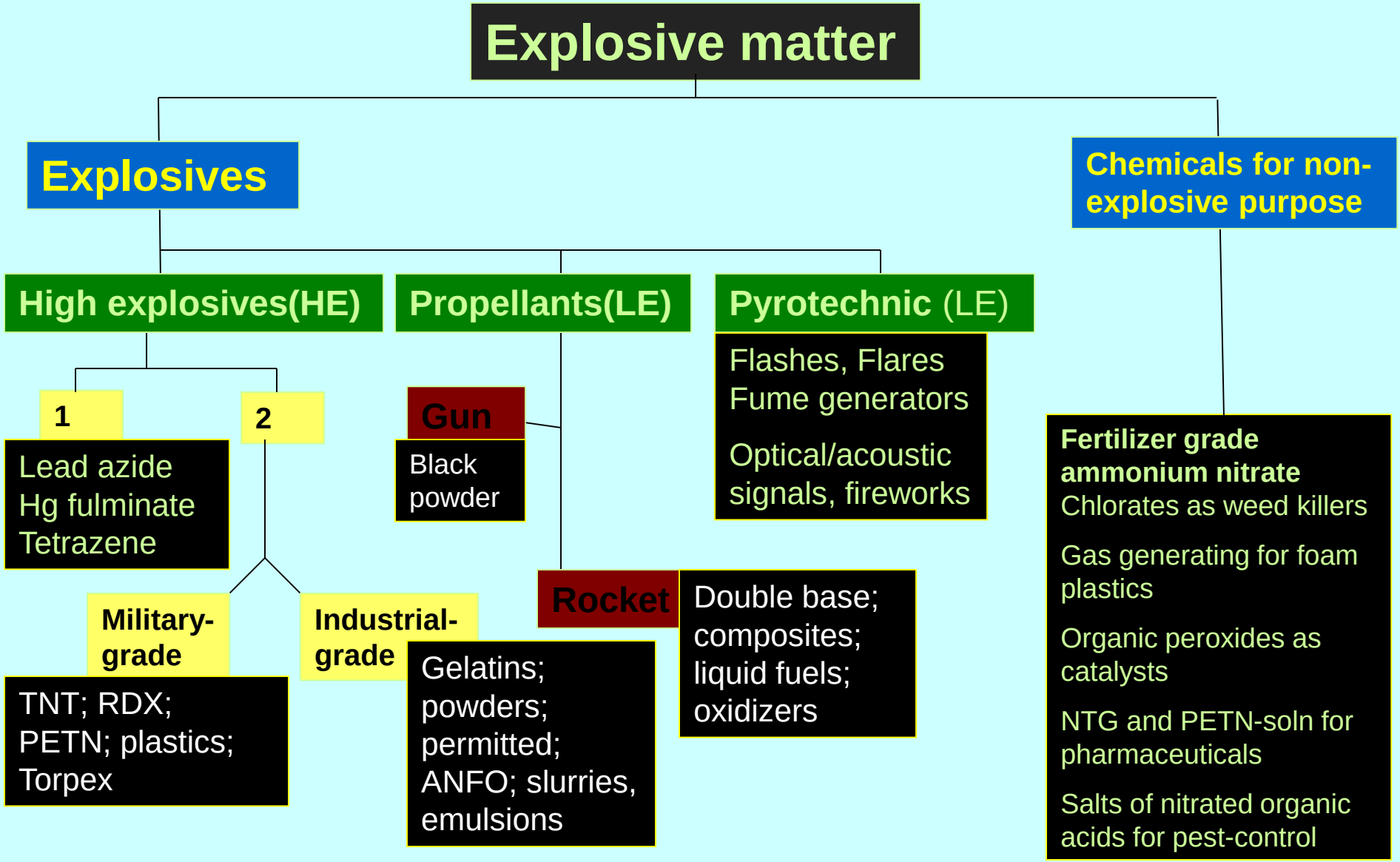
Type of Event: use of agent **Agent:** insecticide
In May 2000, the Anatolia news agency reported that a man was arrested for attempting to poison the water supply of the village of Kurusaray, Turkey, with insecticide.

Type of Event: use of agent **Agent:** arsenic
On May 18, students at a university in Quebec City, Canada, were poisoned with arsenic by drinking coffee from a vending machine on the campus. Police discovered a total of 150 milliliters of arsenic in the bottom of the reservoir tank.

Type of Event: use of agent **Agent:** sewer water
In June 2000, Palestinian news sources reported that Israeli settlers from the Efrat settlement had deliberately released sewer water into Palestinian agricultural fields in the village of Khadder in the West Bank.

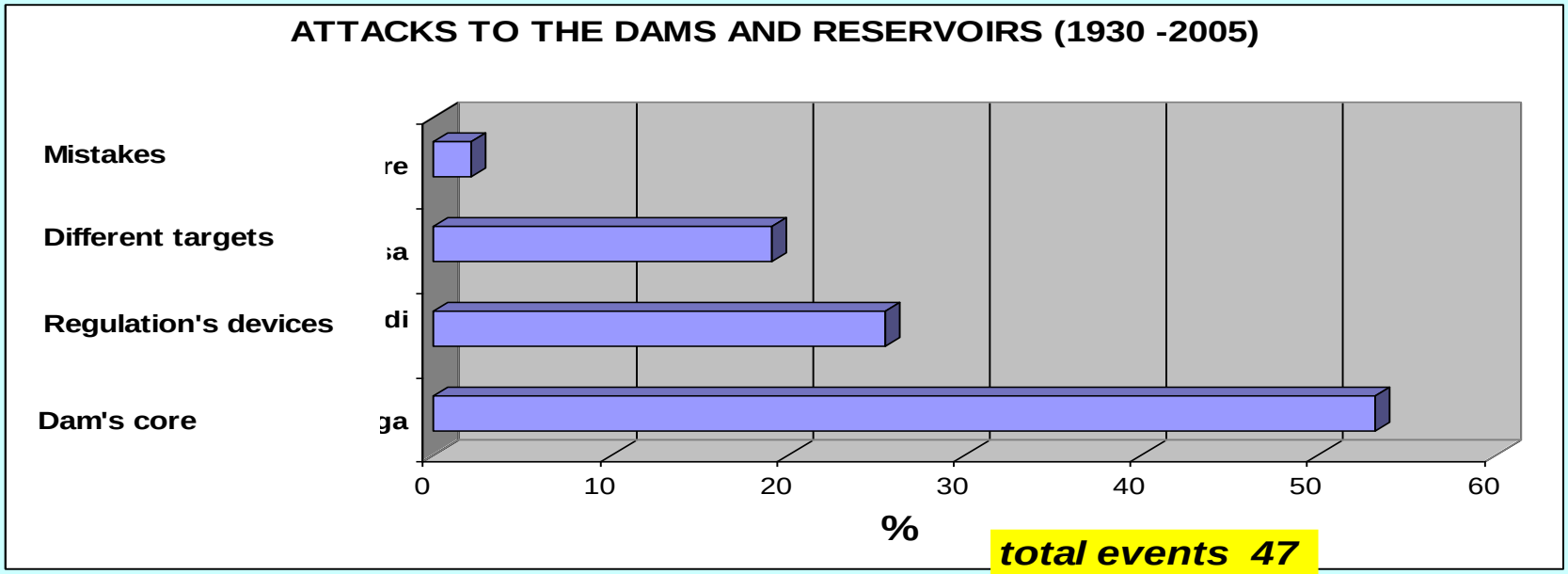
Type of Event: use of agent **Agent**: kerosene and turpentine
On September 15, a day after residents in a condominium block in Singapore had complained of a strange odor in their water supply, it was discovered that the water tank had been deliberately poisoned with kerosene and turpentine

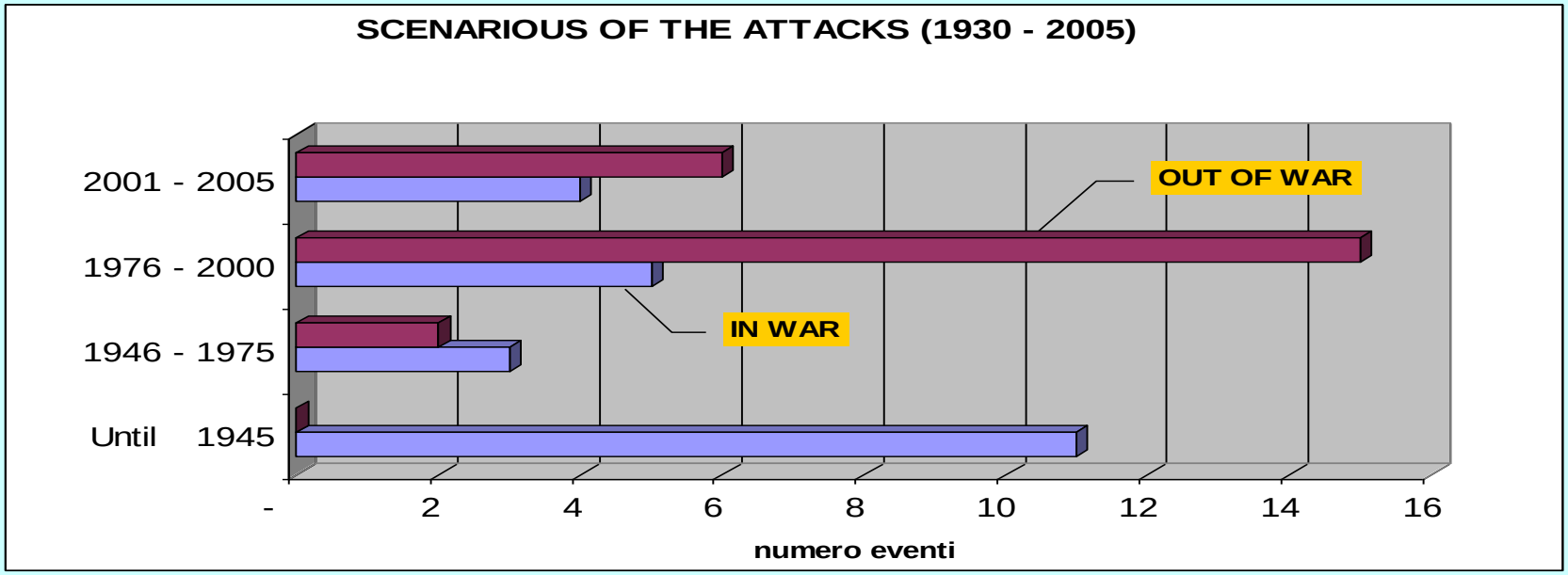
EXPLOSIVES



From *Explosives*, R. Meyer – 5th Edition

Attacks to the dams





Most dangerous attack to a dam
- Second World War -

Mohne Dam

Eder Dam

Sorpe Dam

SFOR Informer Archives


SLOVENIA
HUNGARY
CROATIA
ROM
Vojvodina
Republika Srpska
BOSNIA
AND
HERZEGOVINA
Federation of Bosnia
and Herzegovina
Republika
Srpska
Serbia
Montenegro
CROATIA
Adriatic
Sea
ITALY
Zagreb
Sarajevo
Belgrade
Split
Sokolac
Podromanija
Romanija
Pale
Praca
Jahorina
Mesići
Višegrad
Rogatica
Ustiprača
Goražde
Zagor
Rudo
Čajniče
Dobro Polje
Drina
Foča
Kalinovik
Dragočava
Drniš
Siverić
Vuković
Maovice
Otavice
Gradac
Kričke
Čikola
Ružić
Umljanović
Planjane
Kljake
Otišić
Dabar
Peručko jezero
Potravlje
Zelovo
Hrvace
Pribude
Milešina
Ogorje
Postinje
Muć
Neorić
Kladnice
Brštanovo
Gizdavac
Lećevica
Radošić
Konjsko
Prgomet
Labin
Bristivica
Klis
Dugopolje
Sinj
Ljubitovica
Ljubostinje
Nevest
Unešić
Zagora
Sitno

Peruca Dam

Drina River

Attacks to the other water infrastructures

IRAK

Acqueduct of Bagdad 17 august 2003

A Rocked Propelled Grenade (RPG) damaged a 1.200 mm water pipe
300.000 people had a water loss for several days

Access and area control

CYBER-TERRORISM

The risks of Cyber-attacks

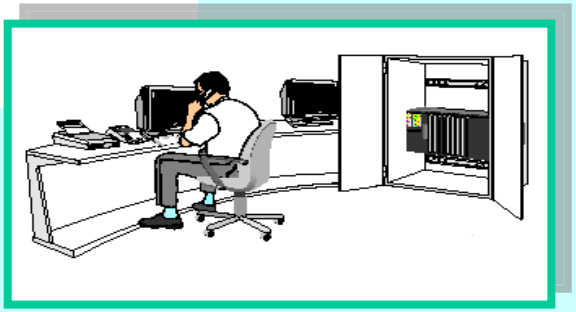
Email spamming

Transmission of Virus or Worms

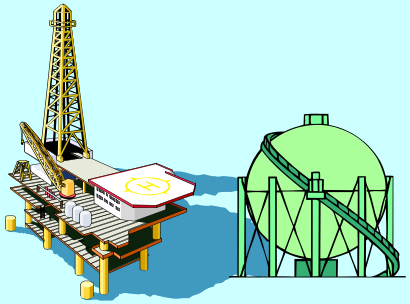
Transmission of Troy (informatic spions)

Far modifying of WEB sites

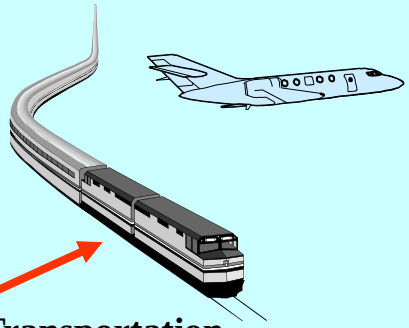
SCADA Intrusion



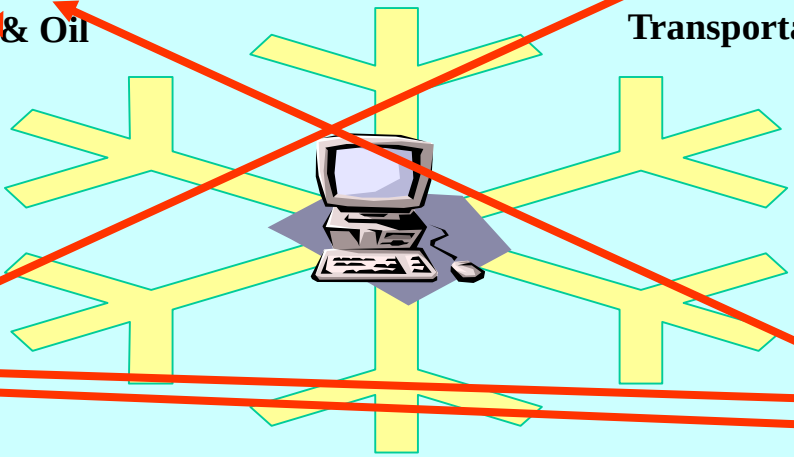
Interdipendence between public utilities

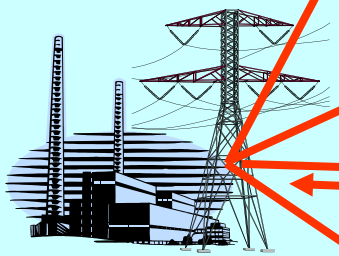


Gas & Oil

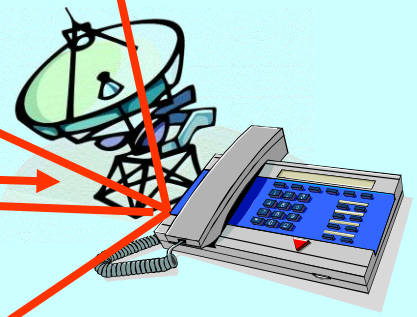


Transportation



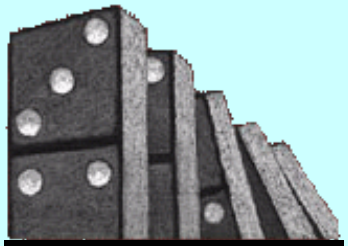


Electric Power



Telecommunications

Water & Sewer



DOMINO'S EFFECT

A MALFUNCTION IN A SERVICE DEPENDING BY AN HACKER'S ATTACK CAN PROVOKE NEGATIVE EFFECTS IN OTHER SERVICES

Example of Cyber-Terrorism in Water SCADA

In Queensland (Australia), the 23 april 2000 police arrested Vitek Boden electronic technician dismissed by a telemetry company.

During two months he caused several environmental damages opening in random ways the gates of waste water pipes. He used an home-made apparatus with the same radio frequencies of Maroochy Shire Wastewater SCADA.

Cyber-Terrorism : counter-mesure

Antivirus (and antiworm) especially for networks that can be connected to the Internet

Updating of operating systems

Firewall protection systems

IDS systems (Intrusion Detection Systems) with 24-hour monitoring

Use of cryptography on transmitted data

Use of strong passwords and their modification over time

Strong authentication to access the consoles (smart-card, biometrics, ...)

Physical protection of transmission channels

Additional safety procedures on critical maneuvers

Activation of backup systems and disaster recovery plans

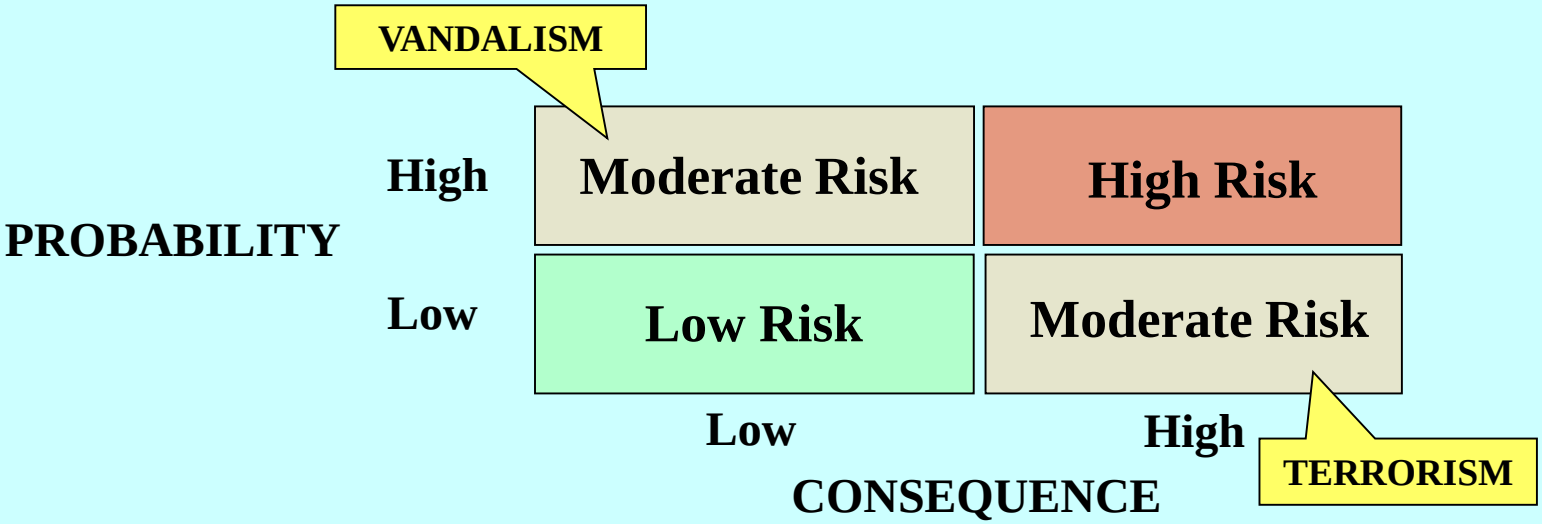
Termination disconnection not strictly functional to process control

QUANTITATIVE ANALYSIS OF THE RISK: THE EMERGENGY PLANNING

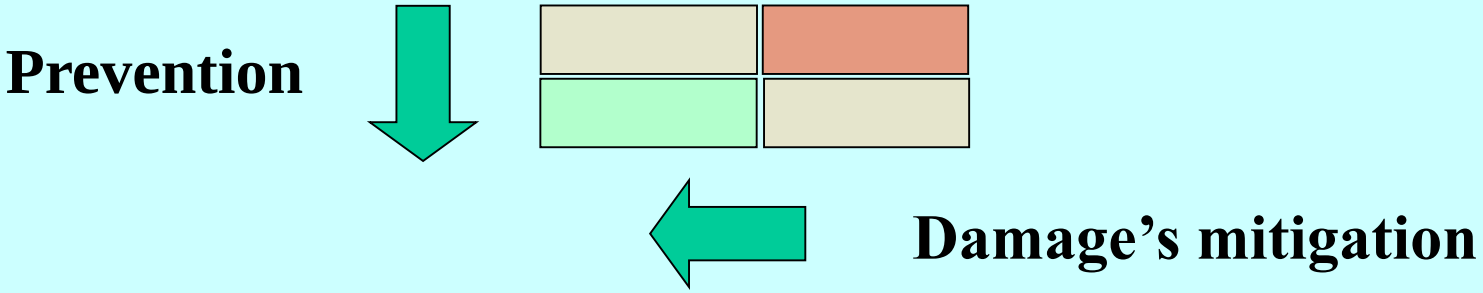
Why do an Emergency Planning?

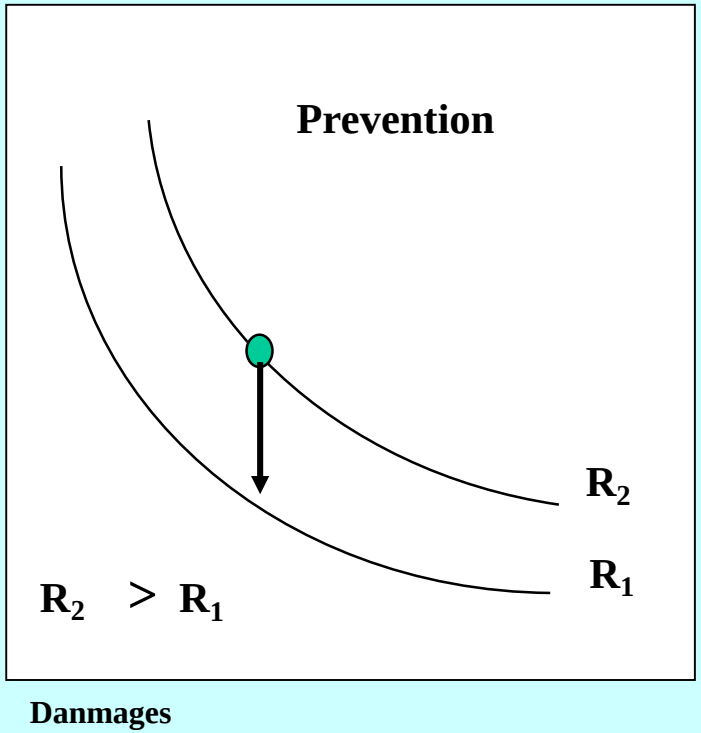
- It's our responsibility as managers of public service
- The health and the safety of citizens depend by our technical preparation and organization
- Because none of us have a crystal ball

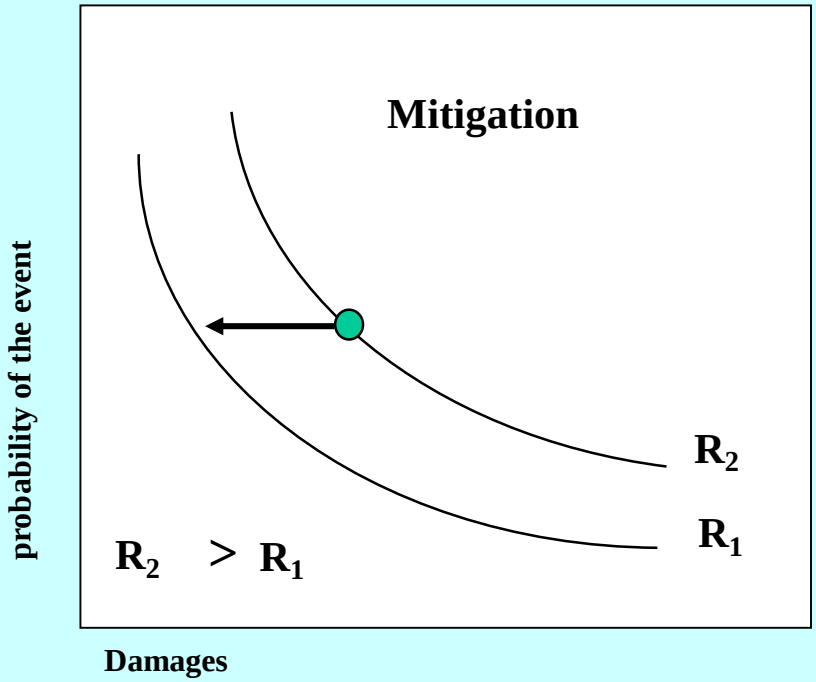
RISK = PROBABILITY x CONSEQUENCE



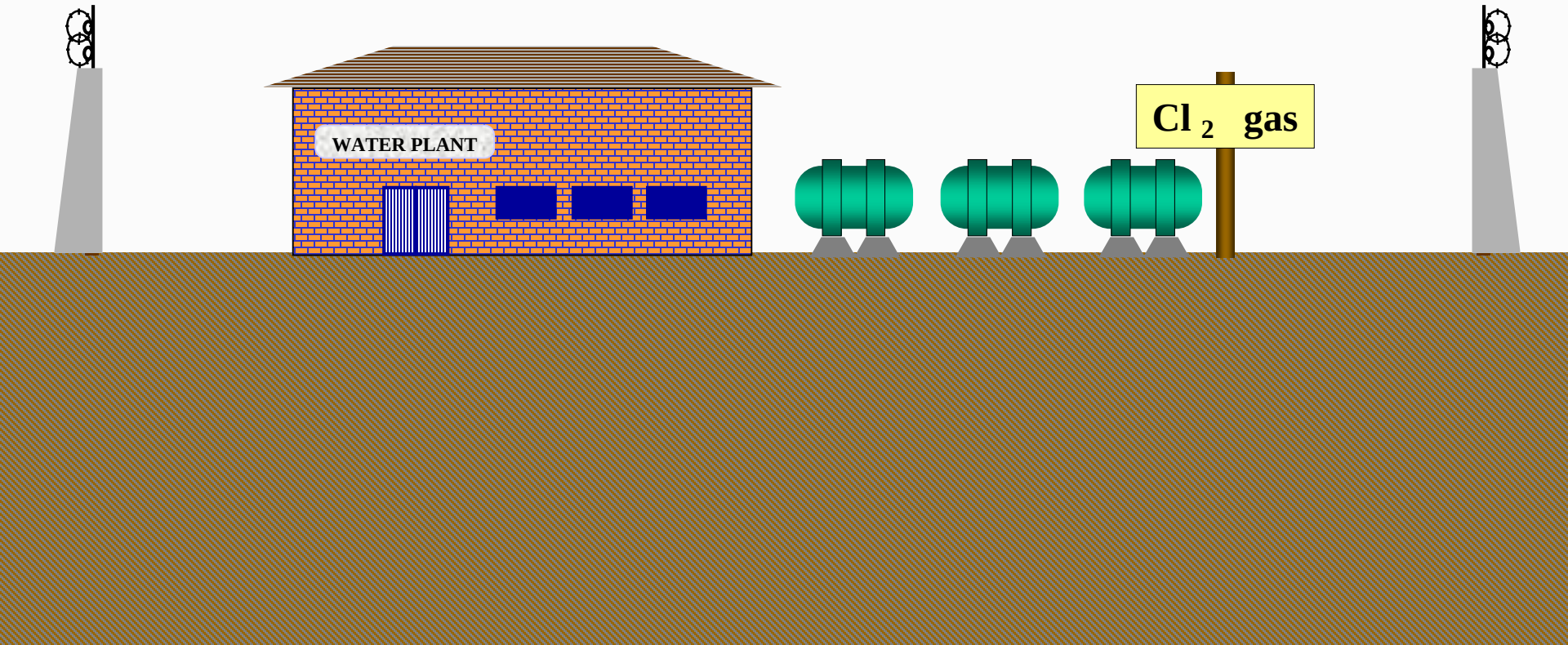
STRATEGIES OF RISK REDUCING




Prevention
probability of the event
R_2
R_1
$R_2 > R_1$
Danmages

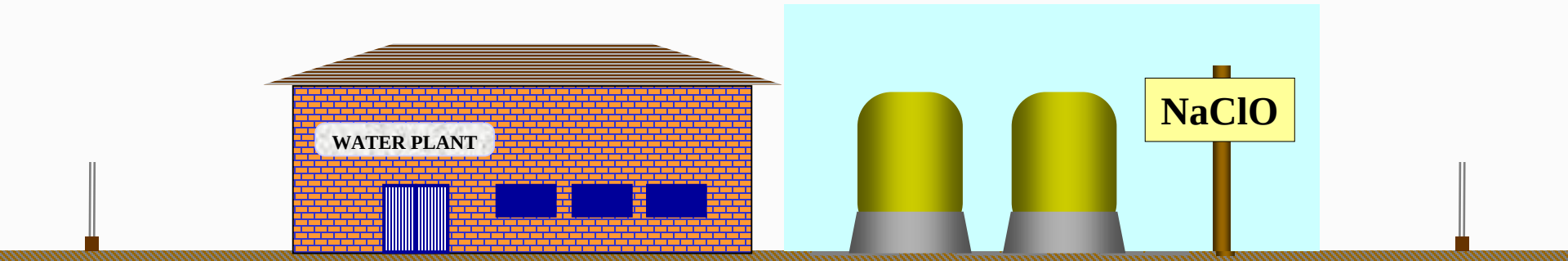

Mitigation
probability of the event
R_2
R_1
$R_2 > R_1$
Damages

Prevention strategy: an example



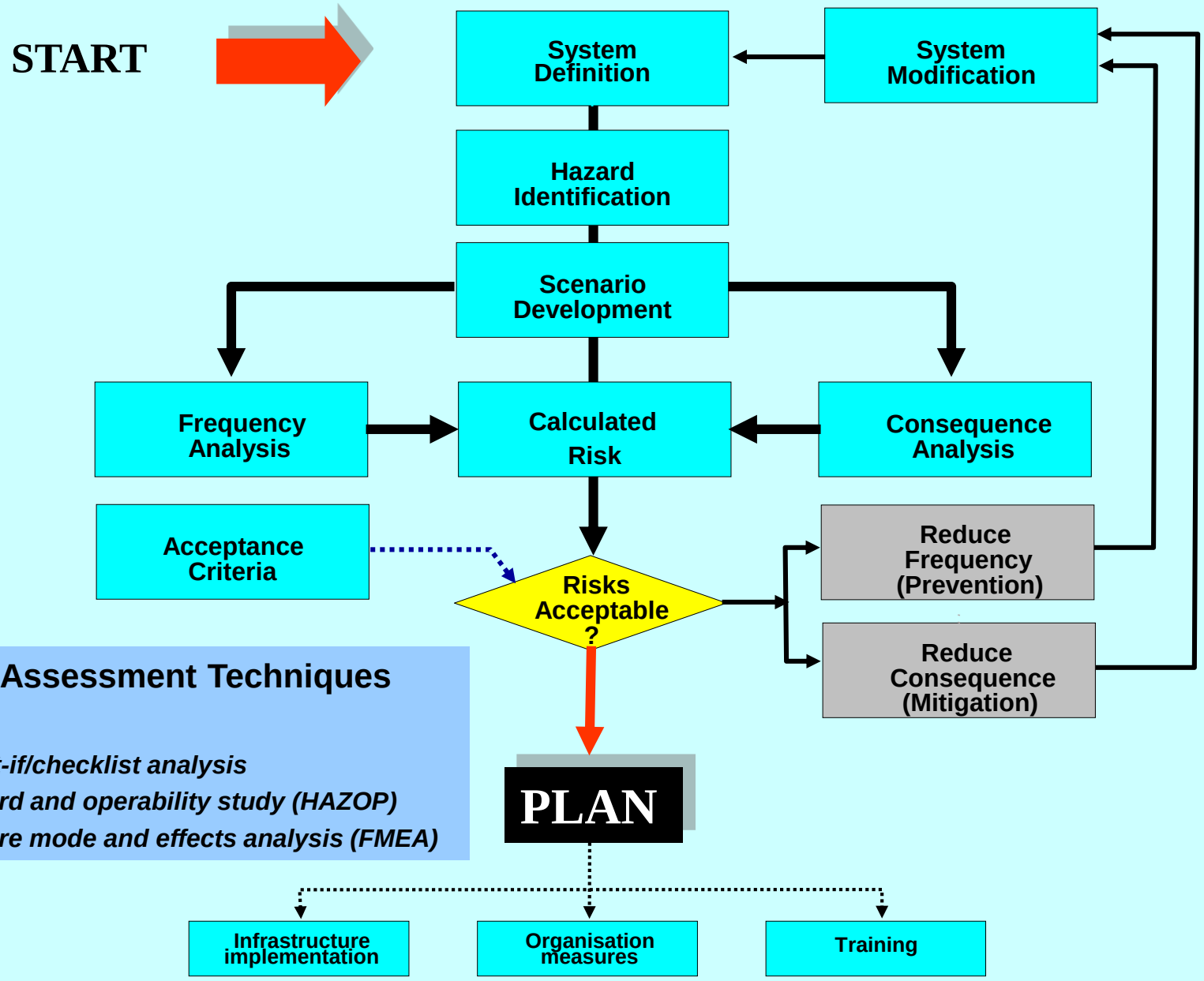

Accident Management
Status: NOT COMPLETE
Accident Summary
Health unknown
Damage unknown
Dynamic Model Control
Manual reset
10.00
Manual reset
700.00
UNITS
N
W
E
S
Time: 14 : 44
EXIT
Model Descriptors
Substance Chlorine
Mass 2000.0 kg
Wind Speed 0.5 m/s
Air Temperature 10.0 C

Mitigation strategy: an example



In USA after 11 september disinfection plants changed from gas chlorine to NaClO or UV

Risk Assessment Process



Risk Assessment Techniques

- *What-if/checklist analysis*
- *Hazard and operability study (HAZOP)*
- *Failure mode and effects analysis (FMEA)*

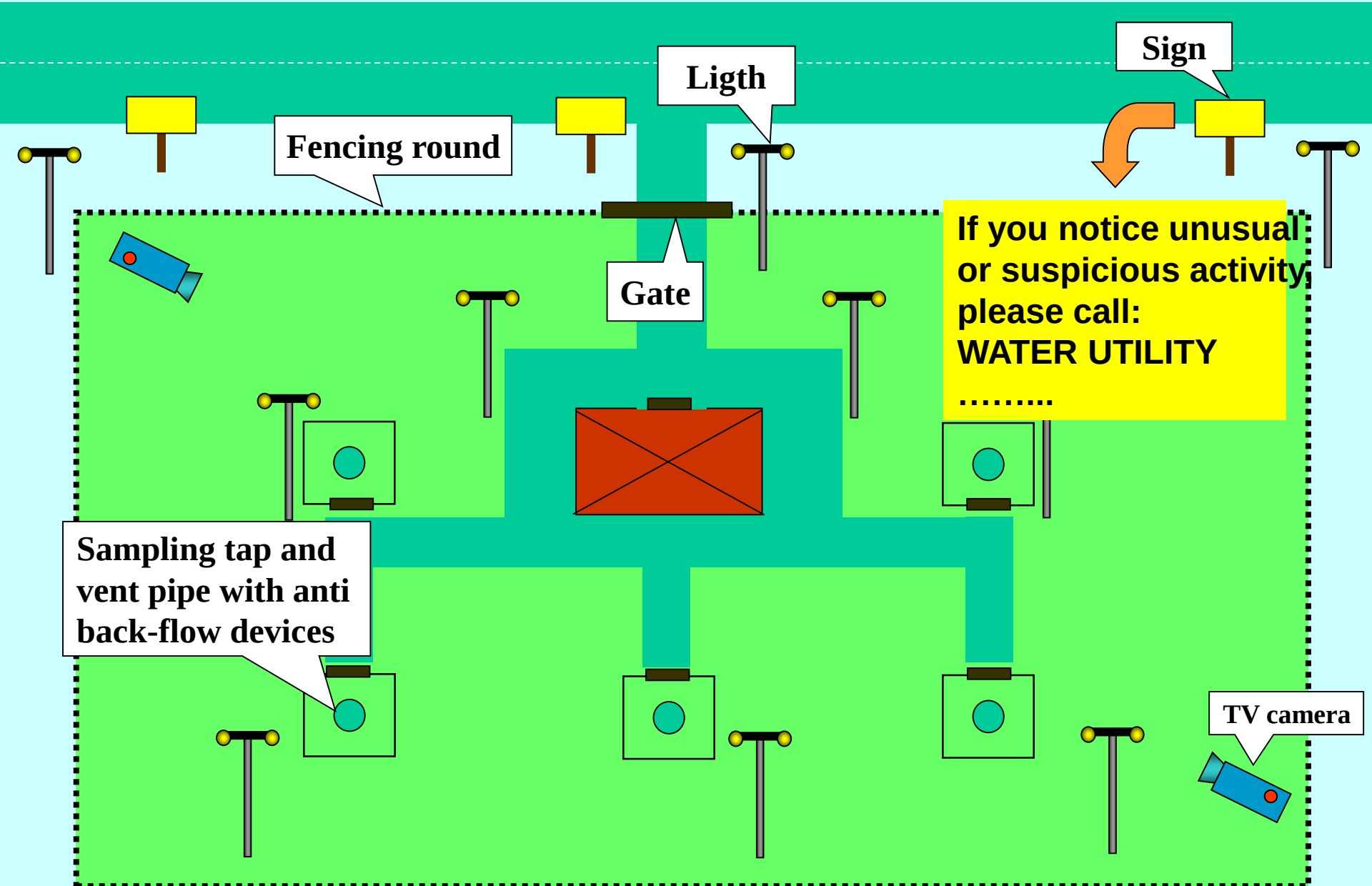
Check list

Information/Storage/Computers/Controls/Maps

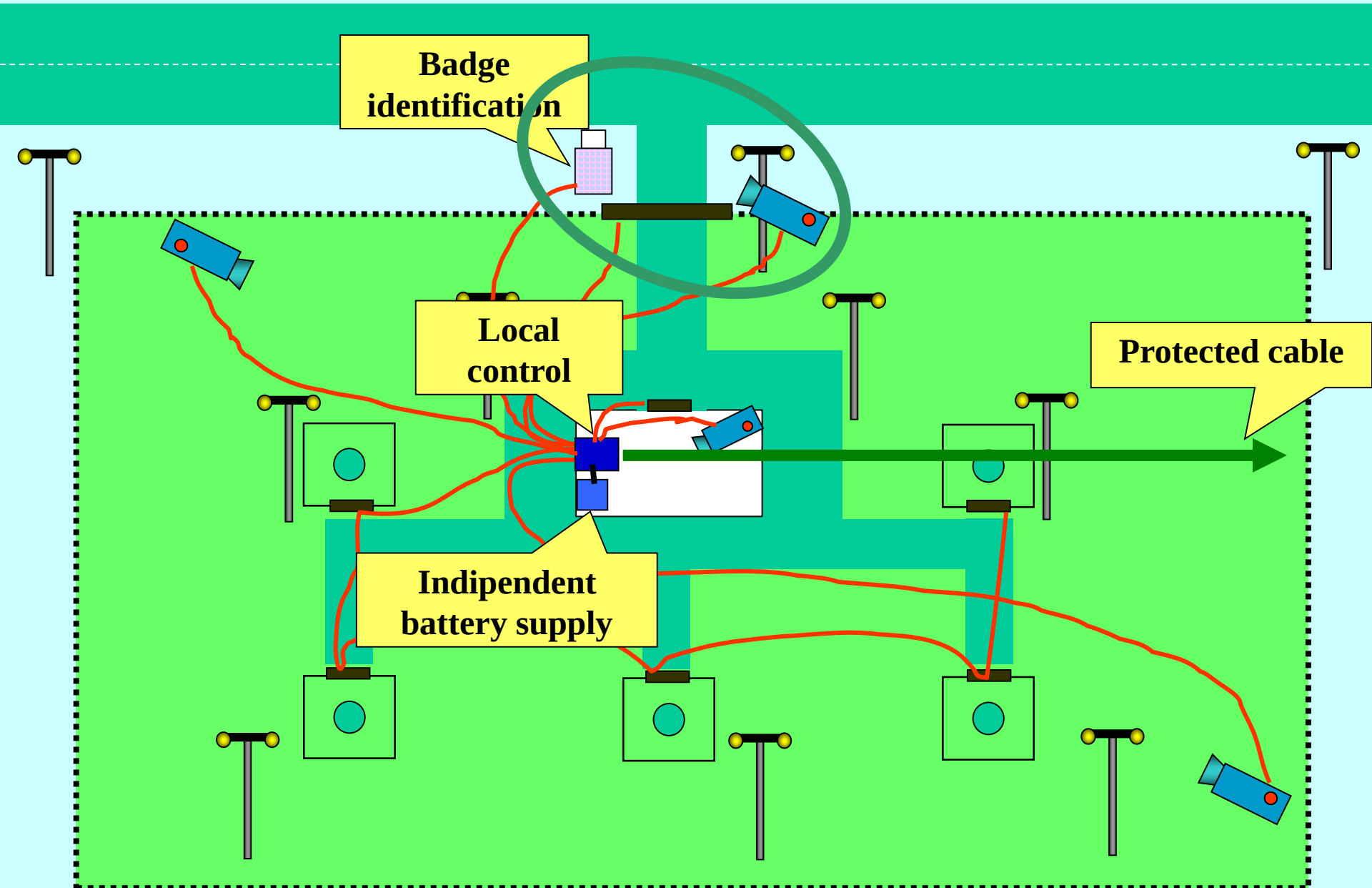
Security of the system, including computerized controls like a Supervisory Control and Data Acquisition (SCADA) system, goes beyond the physical aspects of operation. It also includes records and critical information that could be used by someone planning to disrupt or contaminate your water system.

QUESTION	ANSWER	COMMENT	ACTION NEEDED/TAKEN
36. Is computer access "password protected?" Is virus protection installed and software upgraded regularly and are your virus definitions updated at least daily? Do you have Internet firewall software installed on your computer? Do you have a plan to back up your computers?	Yes ☐ No ☐	All computer access should be password protected. Passwords should be changed every 90 days and (as needed) following employee turnover. When possible, each individual should have a unique password that they do not share with others. If you have Internet access, a firewall protection program should be installed on your side of the computer and reviewed and updated periodically. Also consider contacting a virus protection company and subscribing to a virus update program to protect your records. Backing up computers regularly will help prevent the loss of data in the event that your computer is damaged or breaks. Backup copies of computer data should be made routinely and stored at a secure off-site location.	
37. Is there information on the Web that can be used to disrupt your system or contaminate your water?	Yes ☐ No ☐	Posting detailed information about your water system on a Web site may make the system more vulnerable to attack. Web sites should be examined to determine whether they contain critical information that should be removed. You should do a Web search (using a search engine such as Google, Yahoo!, or Lycos) using key words related to your water supply to find any published data on the Web that is easily accessible by someone who may want to damage your water supply.	
38. Are maps, records, and other information stored in a secure location?	Yes ☐ No ☐	Records, maps, and other information should be stored in a secure location when not in use. Access should be limited to authorized personnel only. You should make back-up copies of all data and sensitive documents. These should be stored in a secure off-site location on a regular basis.	
39. Are copies of records, maps, and other sensitive information labeled confidential, and are all copies controlled and returned to the water system?	Yes ☐ No ☐	Sensitive documents (e.g., schematics, maps, and plans and specifications) distributed for construction projects or other uses should be recorded and recovered after use. You should discuss measures to safeguard your documents with bidders for new projects.	

Basic wellfield security measures



Basic wellfield security measures



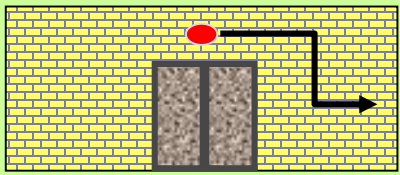
Planning of different activities

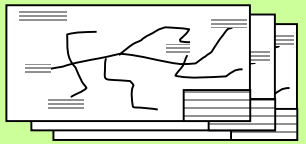
BEFORE

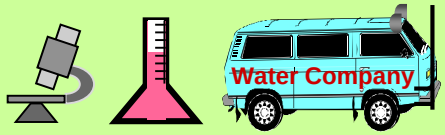
- Using suitable technologies against vandals
- Reinforcing anti-intrusions systems
- Protects the critical informations
- Increase control of water quality
- Rule of communication in critical situation

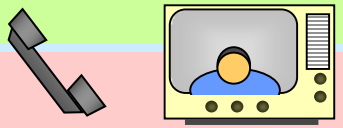
AFTER

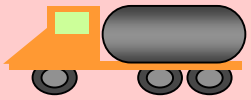
- Emergency water supply plan
- Decontamination and recovery plan

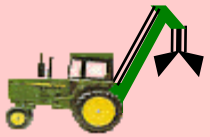












Distribution of drinking water in emergency conditions

Simple and easy rules for medium-little aqueducts

(by EPA – New England)

… maximize use of backflow prevention devices …

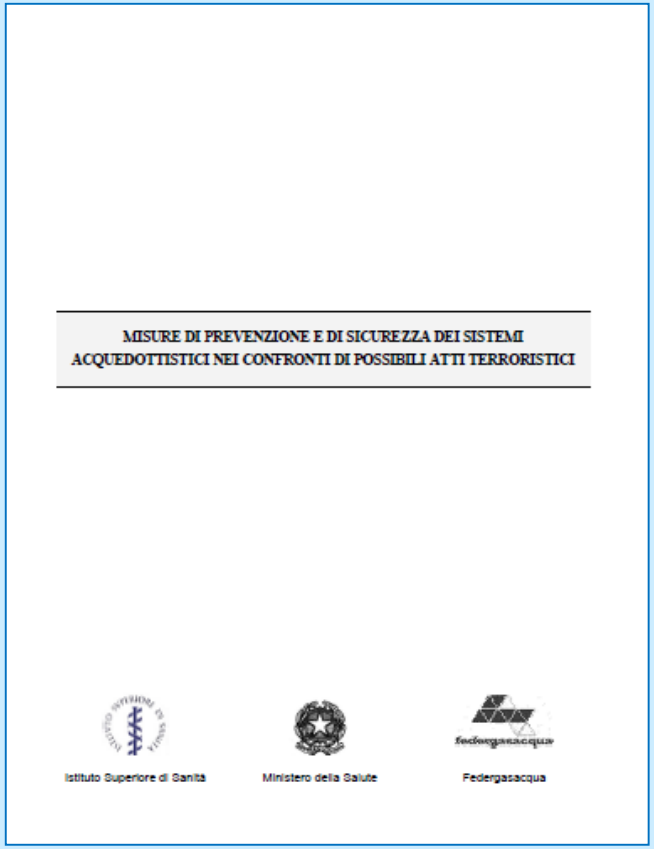
TOP TEN LIST

10. **Prepare** (or update) an emergency response plan. Make sure all employees help to create it and receive training on the plan;
9. **Post** updated emergency 24-hour numbers at your facilities in highly visible areas (pumphouse door, vehicles, office) and give them to key personnel and local response officials;
8. **Get to know** your local police and ask them to add your facilities to their routine rounds. Practice emergency response procedures with local police, emergency response and public health officials;
7. **Fence and lock** your drinking water facilities and vulnerable areas (e.g. wellhead, hydrants, manholes, pumphouse, and storage tanks);
6. **Lock all** entry gates and doors and set alarms to indicate illegal entry. Do not leave keys in equipment or vehicles at any time;
5. **Install good lighting** around your pumphouse, treatment facility and parking lot;
4. **Identify** existing and alternate water supplies and maximize use of backflow prevention devices and interconnections;
3. **Use** your Source Water Assessment information to work with any businesses and homeowners that are listed as potential sources of contamination and lessen their threat to your source;
2. **Lock** monitoring wells to prevent vandals or terrorists from pouring contaminants directly into ground water near your source. Prevent pouring or siphoning contaminants through vent pipes by moving them inside the pumphouse or treatment plant, or if that isn't possible, fencing or screening them; and
1. **In case of an emergency**, first call "911," then follow your emergency response plan.

Work made in Italy

In the 2005 it was created a working group composed by:
- **Ministery of Health**
- **Central Institute of Health**
- **Utilities**

This collaboration has produced guidelines contained in a manual containing:
- **Risk analysis**
- **Prevention techniques**
- **Water monitoring**
- **Agents and countermeasures**
- **Emergency managing**
- **Information's protection about aqueduct**



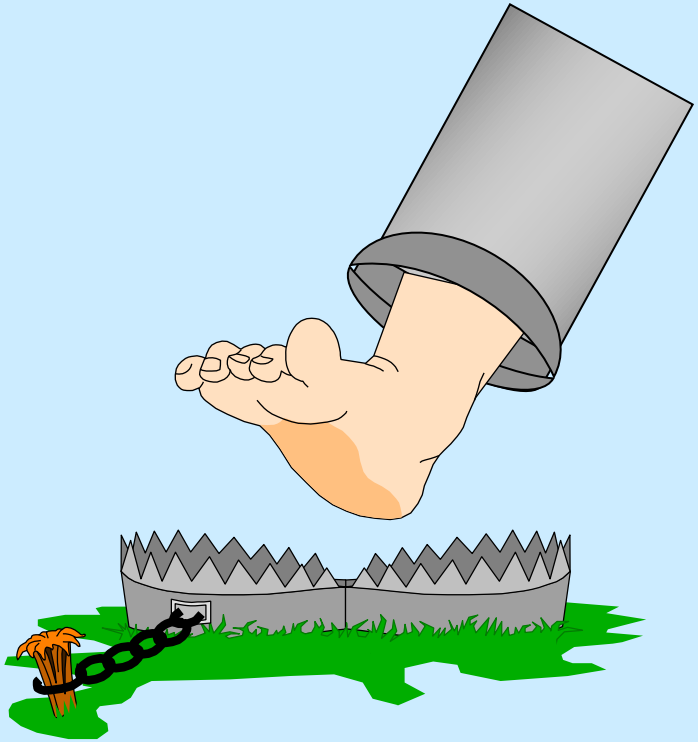
Work made in Italy

Protocol of collaboration with the Civil Protection (organ of the Council of Ministers) to face any important emergency concerning the water services and others services.

Signed 24 maggio 2016

The better paths to true Disaster

- It can’t happen here
- We don’t have time to plan
- We’re too busy
- We have a plan in a drawer
- It’s not our job
- We didn’t think of it
- Let sleeping dogs lie



Roma, 25 January 2018

WATER SERVICES MANAGEMENT

SECURITY MANAGEMENT
DETECTION AND RESPONSE TO EXTERNAL AGGRESSIONS

Renato
Drusiani

UTILITALIA