DAMSE

EC funded project
JLS/2006/EPCIP/001

DAMSE

"A European Methodology for the Security Assessment of dams"

DAMSE Methodology

"Universidad Politécnica de Valencia"

Dr. Manuel G. de Membrillera Ortuño

DAMSE WORKSHOP – Valencia February 26th, 2008

Outline of presentation

1. **Background**
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

Objectives of DAMSE (reminder):

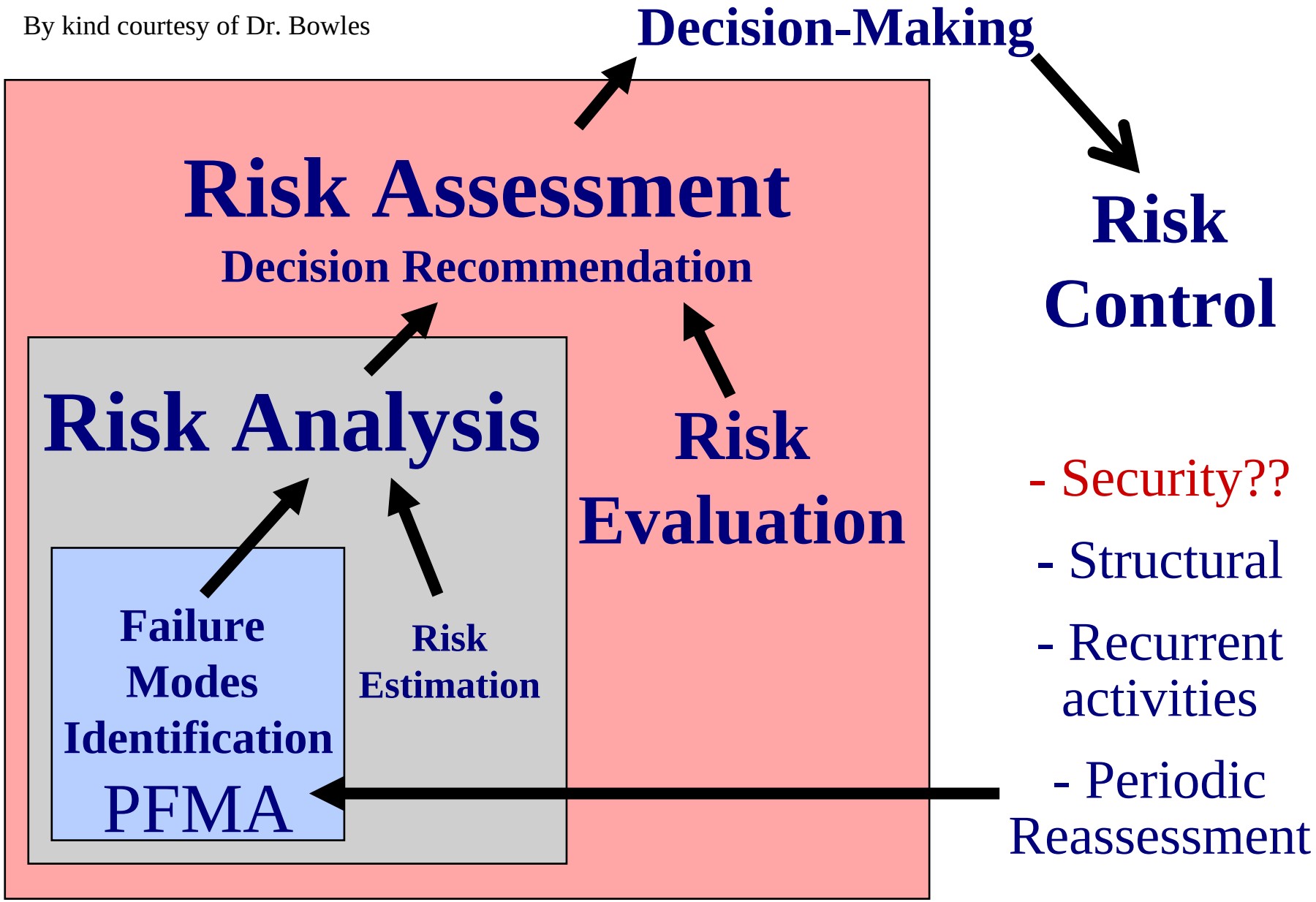
The project is aimed at the development and validation of a methodology for the ***security assessment*** of dams against threats such as: ***terrorist attacks, sabotage*** and ***malevolent intrusions***.

*(*to be proposed as a common framework for the effective protection of dams at EU level)

Acknowledgement of Expert Panel contribution

Dam Safety Risk Management

By kind courtesy of Dr. Bowles



- **The objective will be to identify, understand and qualitatively estimate the risks associated with a spectrum of adversarial attack scenarios on dams**
- **The goal of the methodology is to provide dam owners and stakeholders with a systematic basis for security management decision making**

In the context of dam security, the question is "how do we get started?"

- We will take on the mindset of adversaries
- We will focus on particular undesired events that will be the "loss of mission" events
- We will adopt a deductive way of thinking, beginning with these undesired events

- In addition, we will bear in mind the risk equation:

RISK is a function of:

(LIKELIHOOD OF ATTACK) ,

(1 – SYSTEM EFFECTIVENESS), and

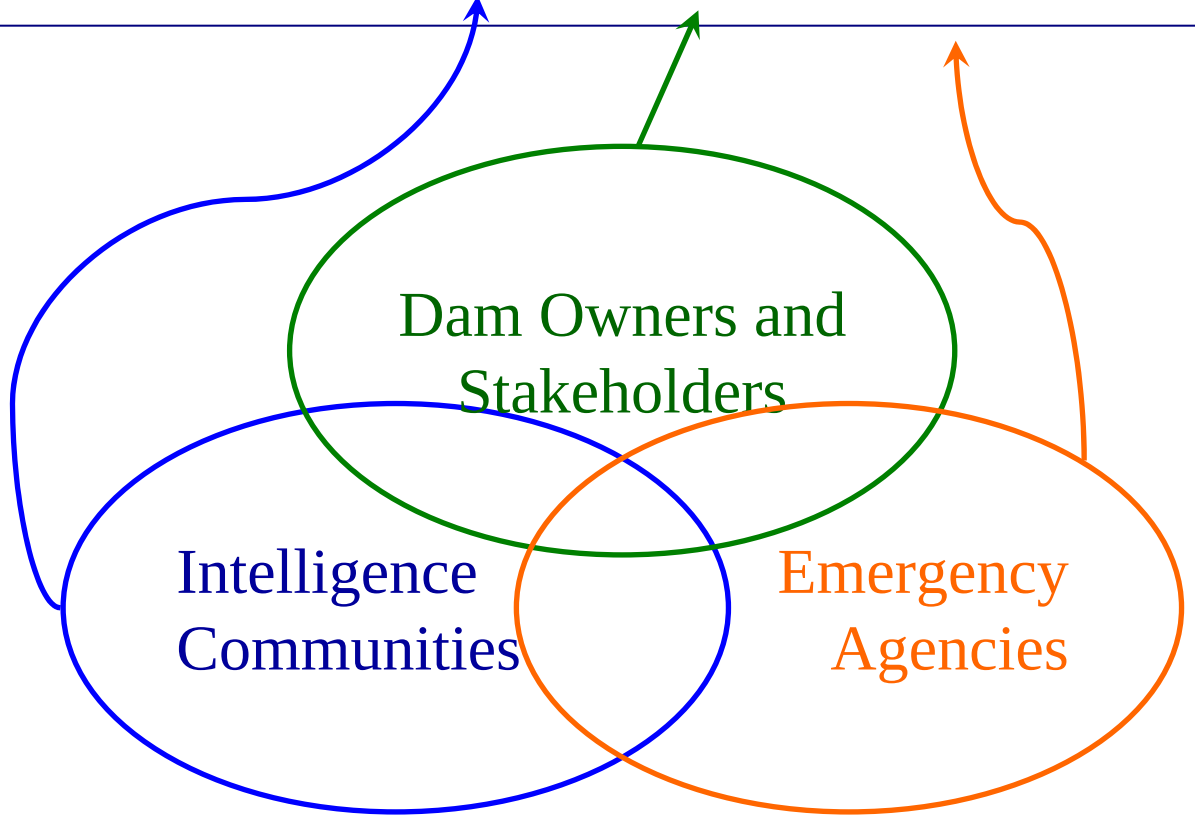
(CONSEQUENCES)

- The methodology will therefore address the **factors** of the equation

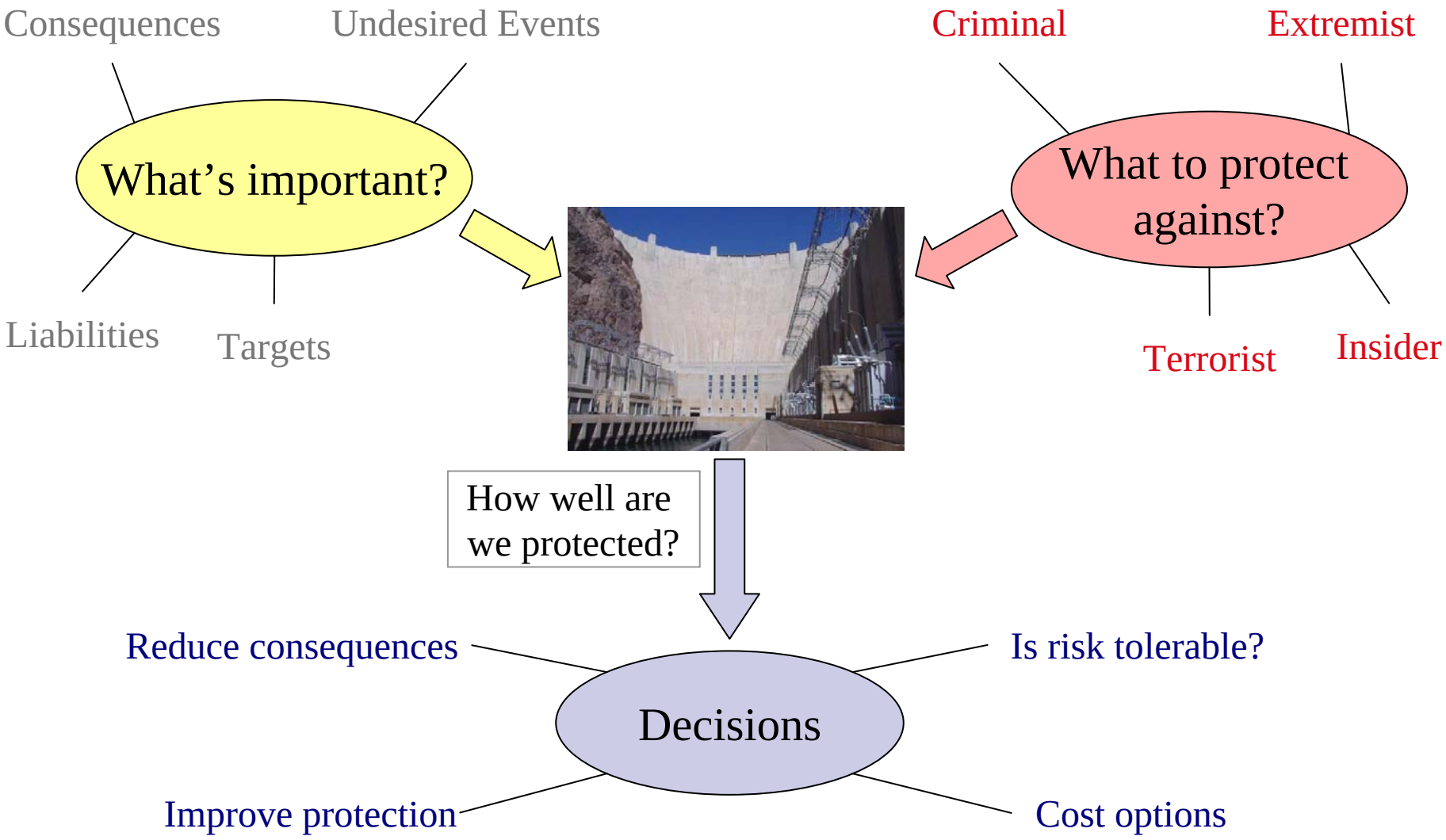
$$R = R\,[P_A, (1 - P_E), C]$$

- The methodology will therefore address the **factors** of the equation

$$R = R\,[P_A,\ (1 - P_E),\ C]$$

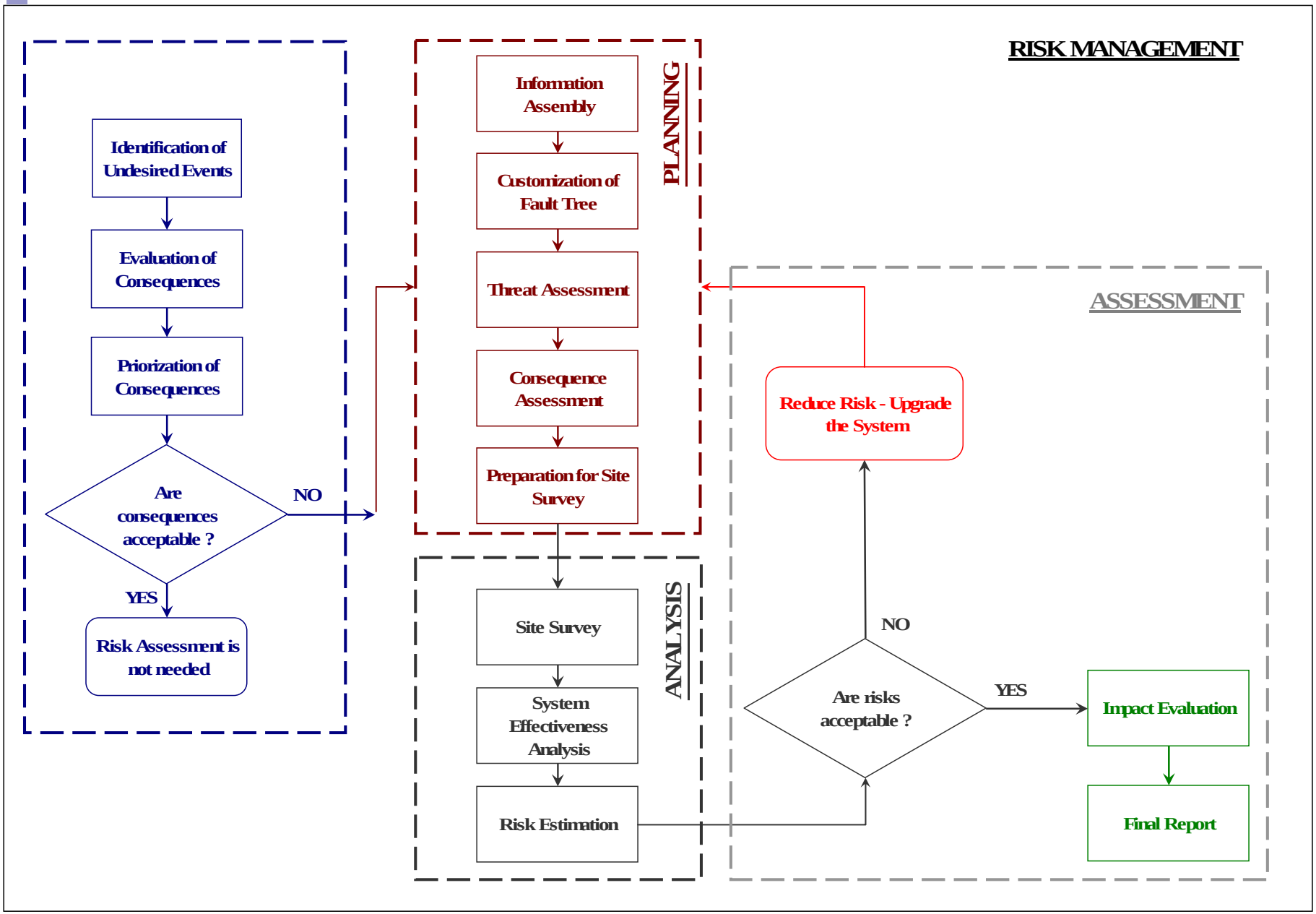


Qualitative Security Risk Assessment



(Adapted from Biringer et al, 2007)

Qualitative Security Risk Assessment



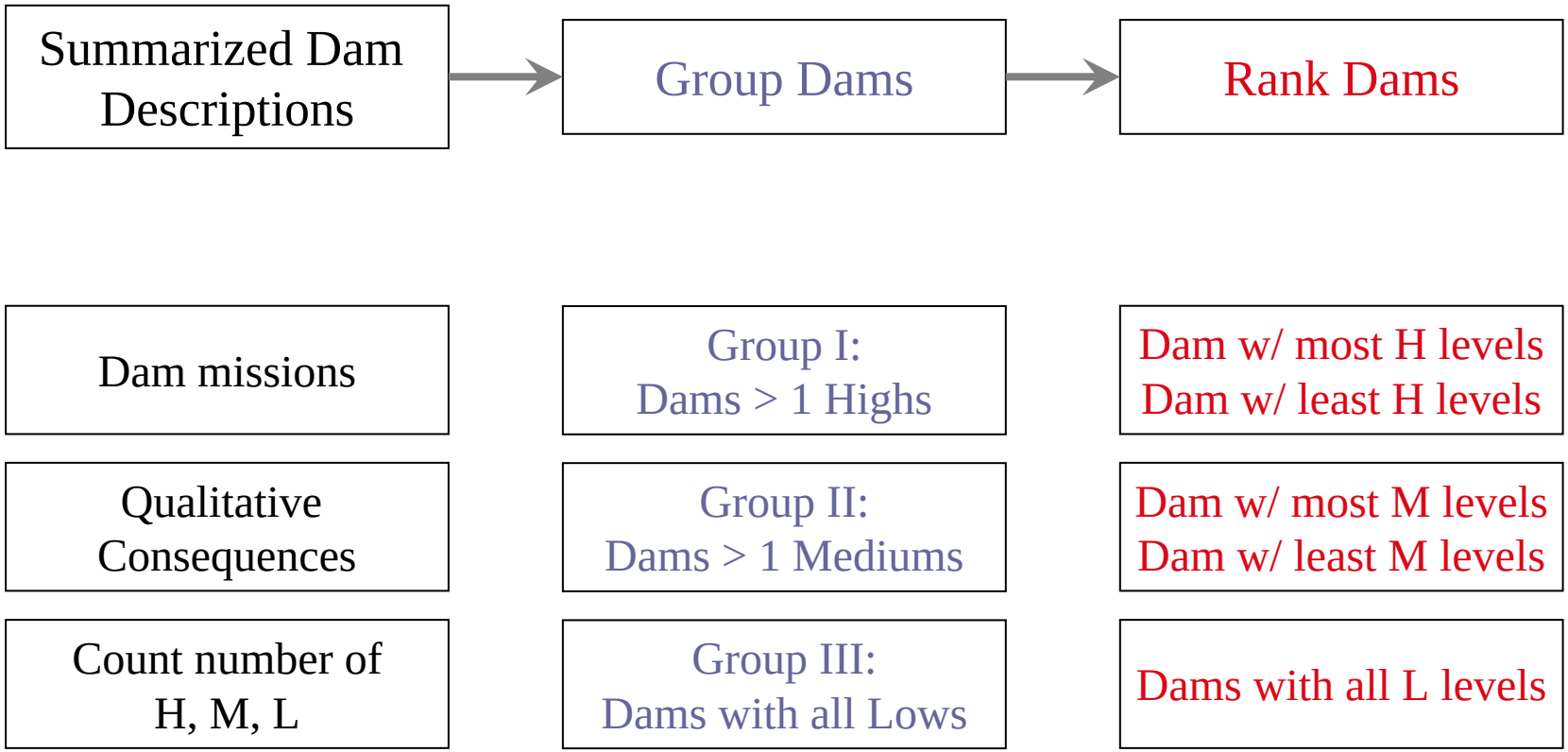
Outline of presentation

1. Background
2. **Screening analysis**
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

2. Screening Analysis

- It is an optional step before an investment is made in a complete security risk assessment
- Decision makers need an efficient process to select which dams warrant a full risk assessment first
- To provide the needed differentiation for screening, the consequence impact is proposed as the key parameter, although other risk factors can be considered
- In any case, the final responsibility for selection lies with the decision makers

2. Screening Analysis



Summary Table

DAMSE Preliminary Screening Procedure

Dam description					Dam missions loss		Consequences Assessment					
Name	Location	Type	Year of const.	Storage Capacity			Public Safety	Economic	Environmental	Total Score	Ranking	Full Security
dam1	**loc1**	**typ1**	**year1**	**cap1**	**x**	Loss of Reservoir	8	8	8	**24**	**H**	**YES**
						Loss of Hydroelectric		n/a		**0**	**n/a**	**NO**
					x	Loss of Water Supply		4	2	**6**	**L**	**NO**
					x	Loss of recreation, tourism		2		**2**	**L**	**NO**
						Loss of Navigation		n/a		**0**	**n/a**	**NO**
						Tot. Score	**8**	**14**	**10**	**32**	**M**	**YES**
Evaluator:	**Name_Lastname**	Evaluation date:	**day/month/year**									
dam2	**loc2**	**typ2**	**year2**	**cap2**	**x**	Loss of Reservoir	10	10	10	**30**	**H**	**YES**
					x	Loss of Hydroelectric		10		**10**	**M**	**YES**
						Loss of Water Supply		n/a	n/a	**0**	**n/a**	**NO**
						Loss of recreation, tourism		n/a		**0**	**n/a**	**NO**
						Loss of Navigation		n/a		**0**	**n/a**	**NO**
						Tot. Score	**10**	**20**	**10**	**40**	**M**	**YES**
Evaluator:	**Name_Lastname**	Date:	**day/month/year**									

Consequences Basic Table

Table 1 - Consequence values					
	Very High Score = 10	**High S = 8**	**Medium S = 6**	**Low S = 4**	**Very Low S = 2**
Public Safety	Population at risk is very high (**PAR>1000 people**)	Population at risk is high **(PAR = 100-1000)**	Population at risk is medium **(PAR = 10-100)**	Population at risk is low **(PAR = 1 - 10)**	There is no population at risk (except incidentaly)
Economic	National to multi-region disruption of essential facilities and access. Economic Impact: **Massive losses (>€1B)**	Multi-regional disruption of essential facilities and access. Economic Impact: **Multi-regional losses, (€100M to €1B) major public and private facilities**	Regional disruption of essential facilities and access.Economic Impact: **Regional losses, (€10M to €100M).**	Local to regional disruption of essential facilities and access. Economic Impact: **Local to regional (< €10M).**	No disruption of essential facilities and access. Economic Impact: **Minimal and confined to facility only**
Environmental	Massive environmental mitigation cost or impossible to mitigate.	Very large environmental cost mitigation and multi year recovery	Large environmental mitigation cost and 1 to 2 years to recover	Medium environmental mitigation cost and less than 1 year to recover	Minor environmental mitigation cost

Ranking criteria:

End users must give clear justification for score assignment

Ordering criteria for full security assessment (see example):

1st level - among single mission loss: select consequences H or M

2nd level - (If after level 1 conseq. are still comparable) among multiple mission loss: select consequences H or M

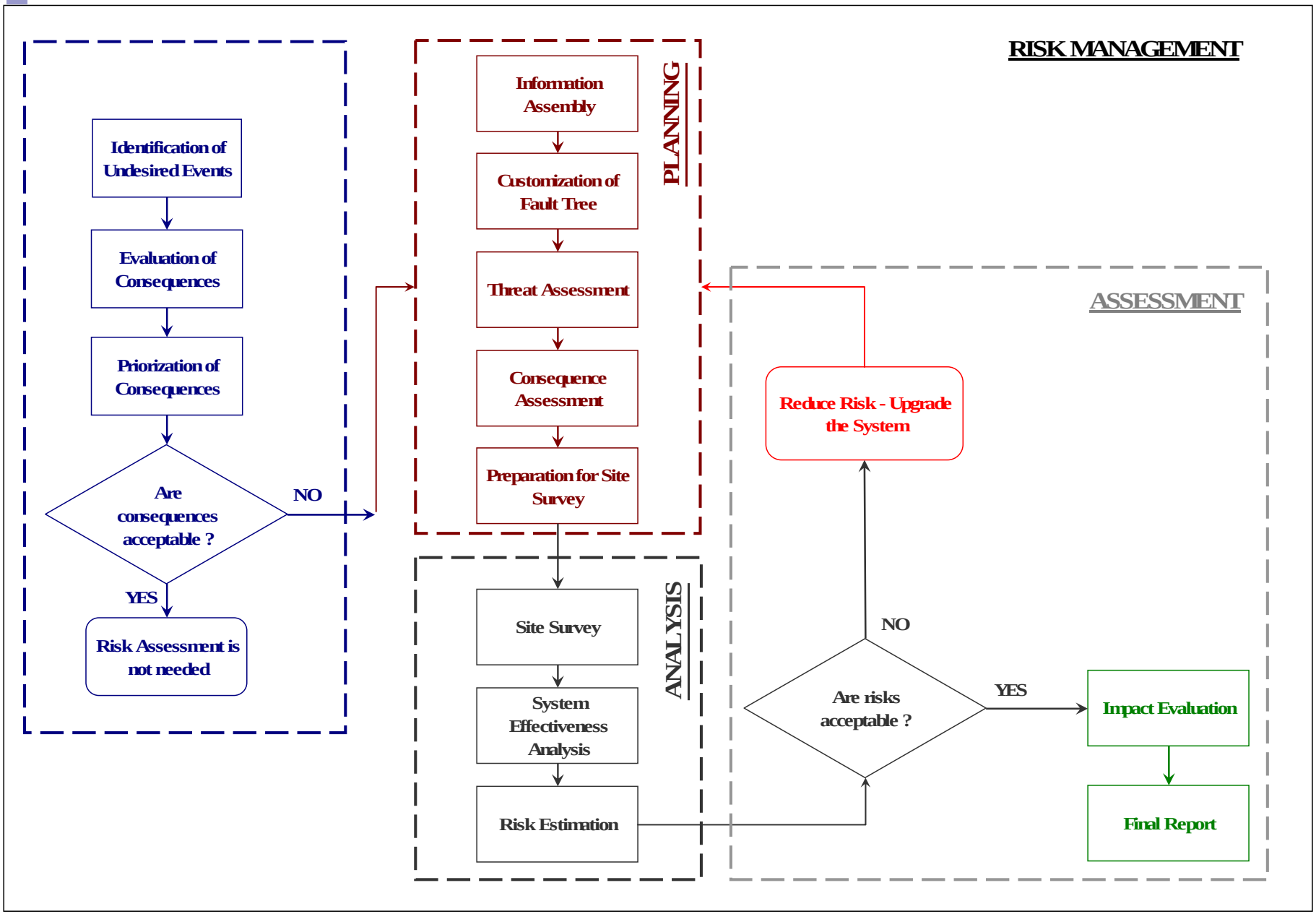
Consequence classification			
Single mission loss	2 <= S < 10	10 <= S <= 20	20 < S <= 30
Multiple mission loss	4 <= S < 26	26 <= S <= 53	53 < S <= 80
Category	**Low (L)**	**Medium (M)**	**High (H)**

3rd level - (If after level 2 conseq. are still comparable): select highest total

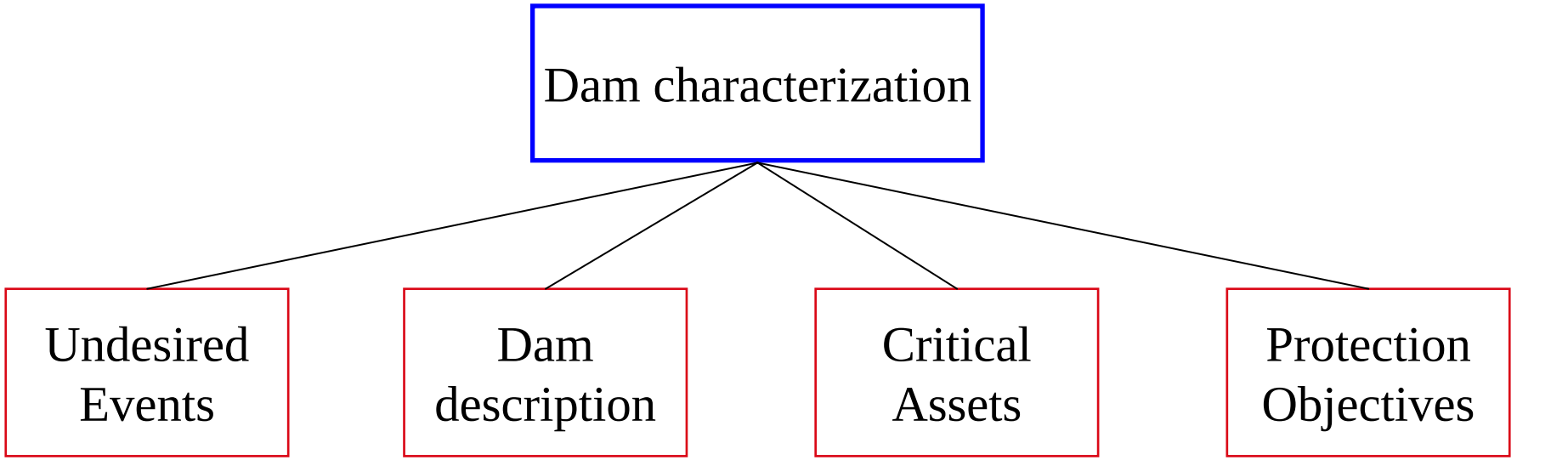
Outline of presentation

1. Background
2. Screening analysis
3. **Planning**
   - ***3.1. Facility characterization***
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

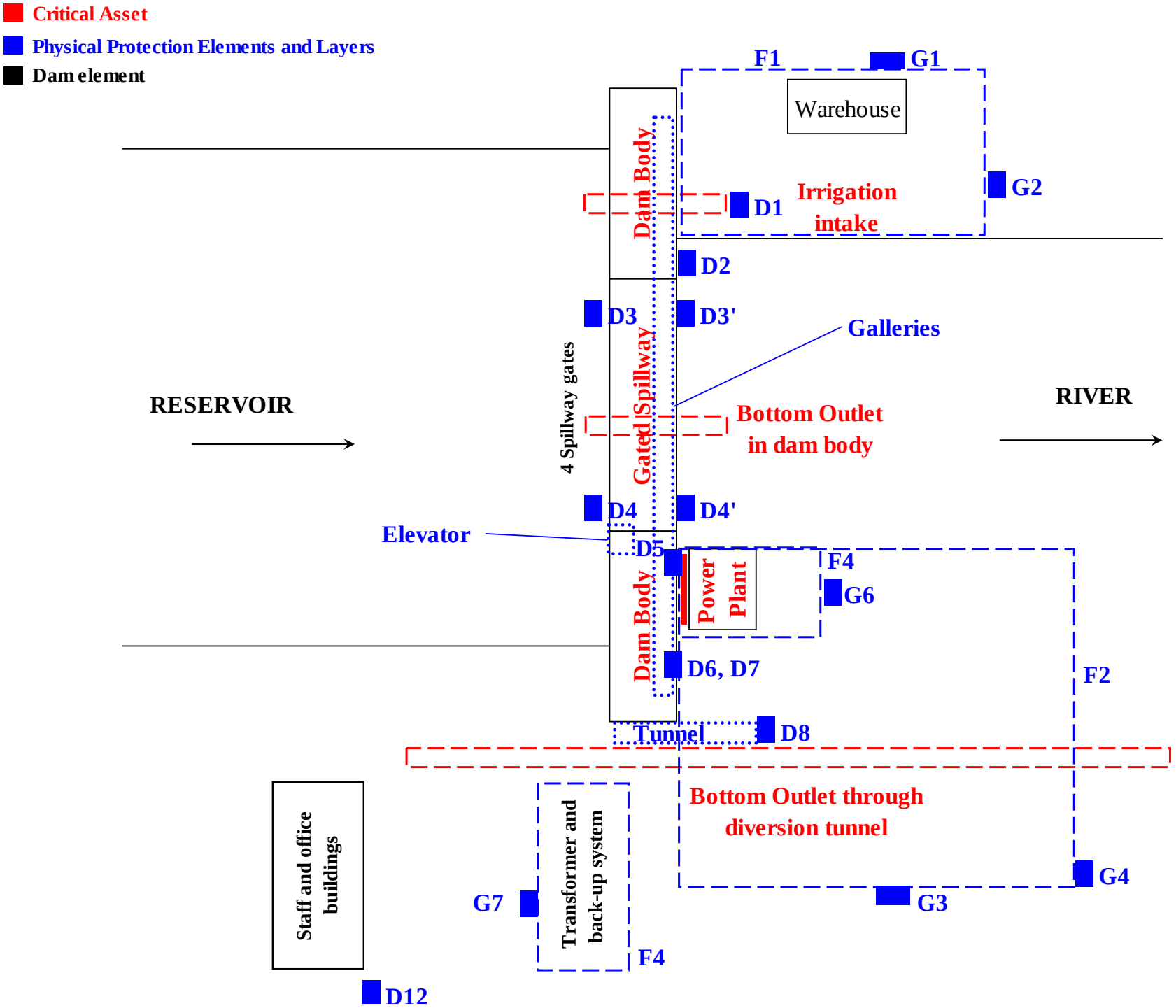
Qualitative Security Risk Assessment



3.1. Dam characterization



Undesired Events	Dam description	Critical Assets	Protection Objectives
•Disruption of operation •Theft of assets •Crimes against people •Destruction •Compromise of the information •Loss of public confidence	•Physical details •Dam operation rules •Security protection systems •Safety protection systems •Workforce description •Restrictions, require-ments, limitations	• Identified by means of Fault Trees	• Preventing disruption of normal operation •Or Compromise of the structural integrity •Or health and safety of occupants •Or disabling utilities •Or disabling emergen-cy systems


Critical Asset
Physical Protection Elements and Layers
Dam element
F1
G1
Warehouse
Dam Body
D1
Irrigation intake
G2
D2
D3
D3'
Galleries
4 Spillway gates
Gated Spillway
RESERVOIR
RIVER
Bottom Outlet in dam body
D4
D4'
Elevator
D5
F4
Power Plant
G6
Dam Body
D6, D7
F2
Tunnel
D8
Bottom Outlet through diversion tunnel
G4
G3
Staff and office buildings
Transformer and back-up system
G7
F4
D12

Outline of presentation

1. Background
2. Screening analysis
3. **Planning**
   - *3.1. Facility characterization*
   - ***3.2. Customization of Fault Tree***
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

Fault Tree Analysis

- Used to describe the causes of an undesired top event
- It's a graphical construct that shows the logical interaction among the elements of a system whose failure, individually or in combination, could contribute to the occurrence of a defined undesired event
- Structured rendering of process steps and barriers against failure
- Deductive way of thinking

Value of the Customized Fault Tree

- The value of this customized fault tree lays on:
  - Complete picture of security events at a dam
  - Identifies critical assets to each mission
  - Shows what needs to be protected:
  - Helps to document critical assets

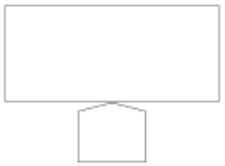
FTA: some important symbols

PRIMARY EVENT SYMBOLS

BASIC EVENT - A basic initiating fault requiring no further development

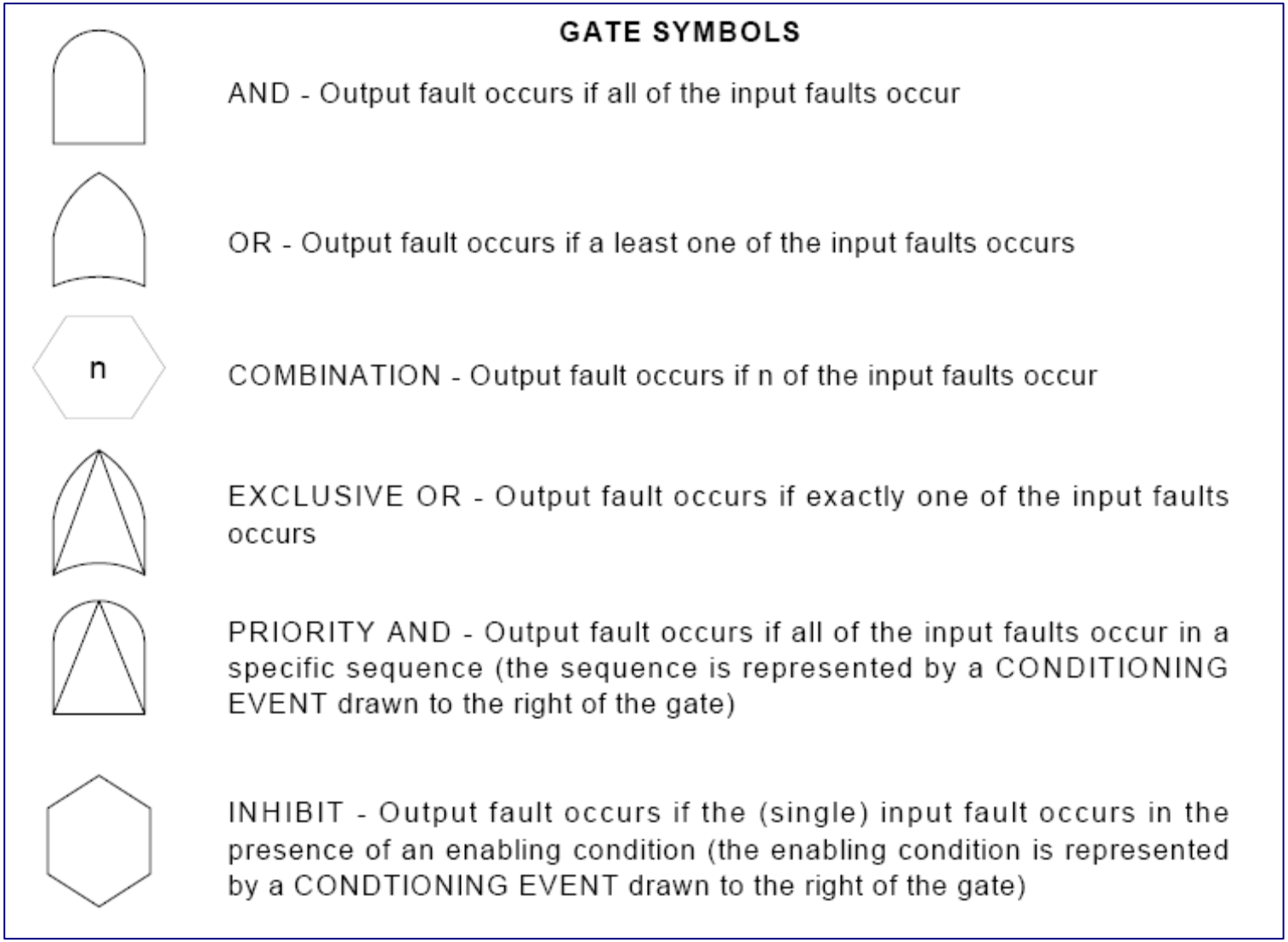
CONDITIONING EVENT - Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT - An event which is not further developed either because it is of insufficient consequence or because information is unavailable

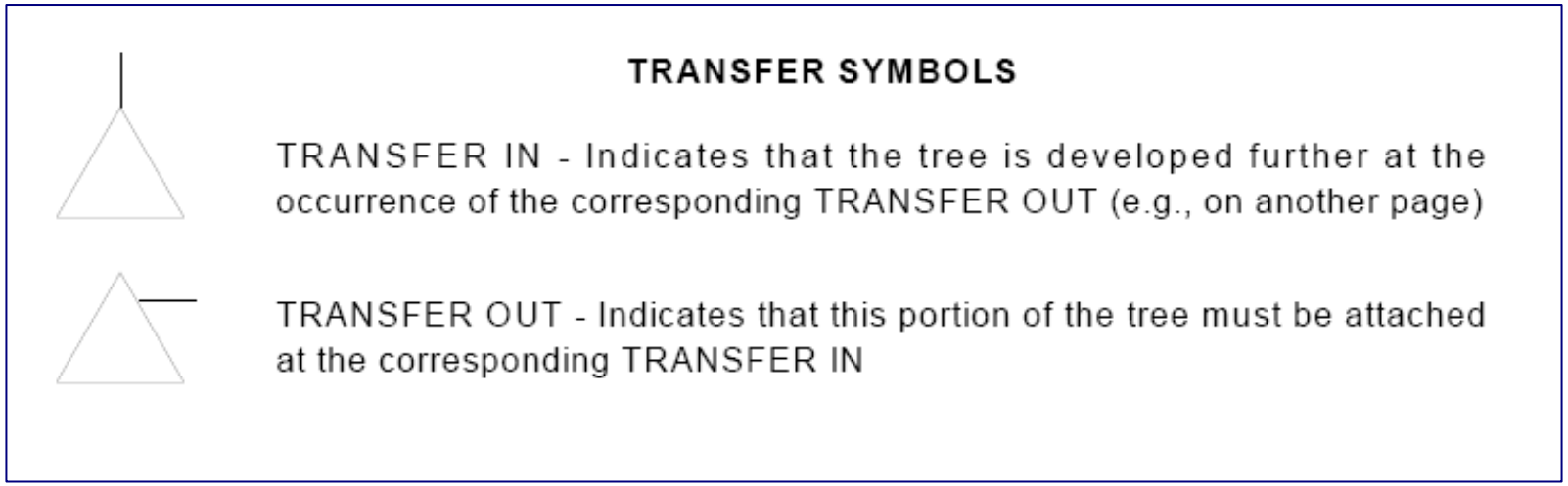


HOUSE EVENT - An event which is normally expected to occur

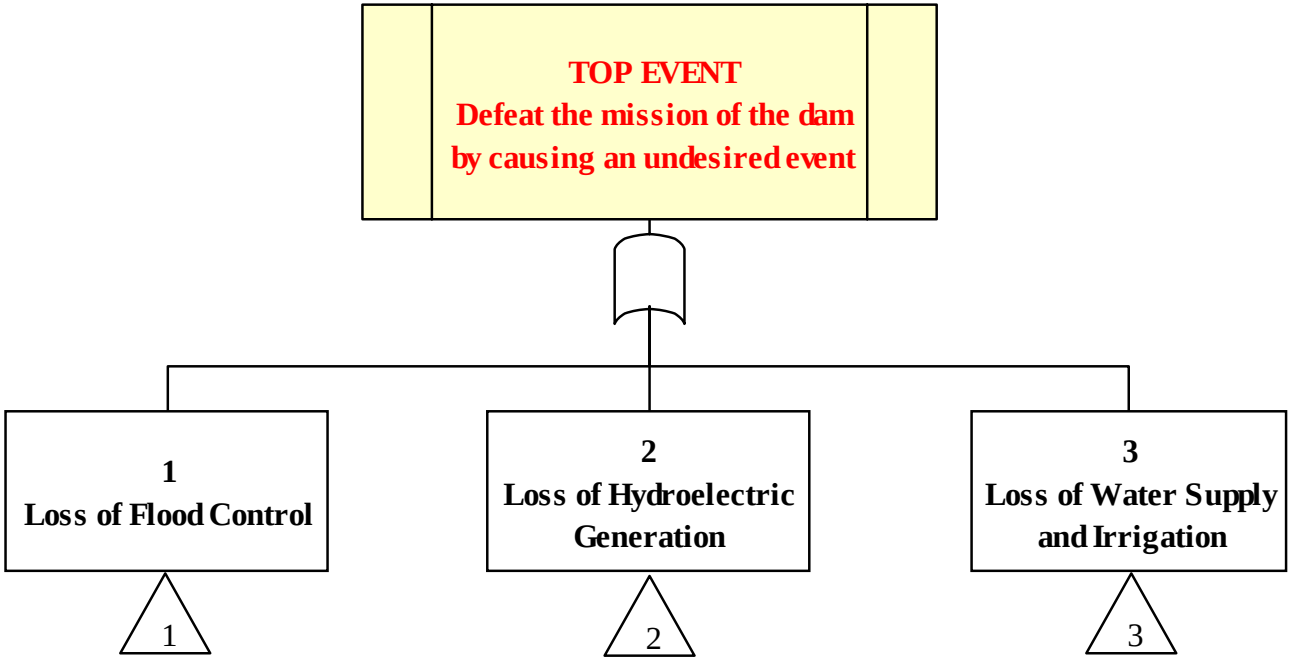
FTA: some important symbols



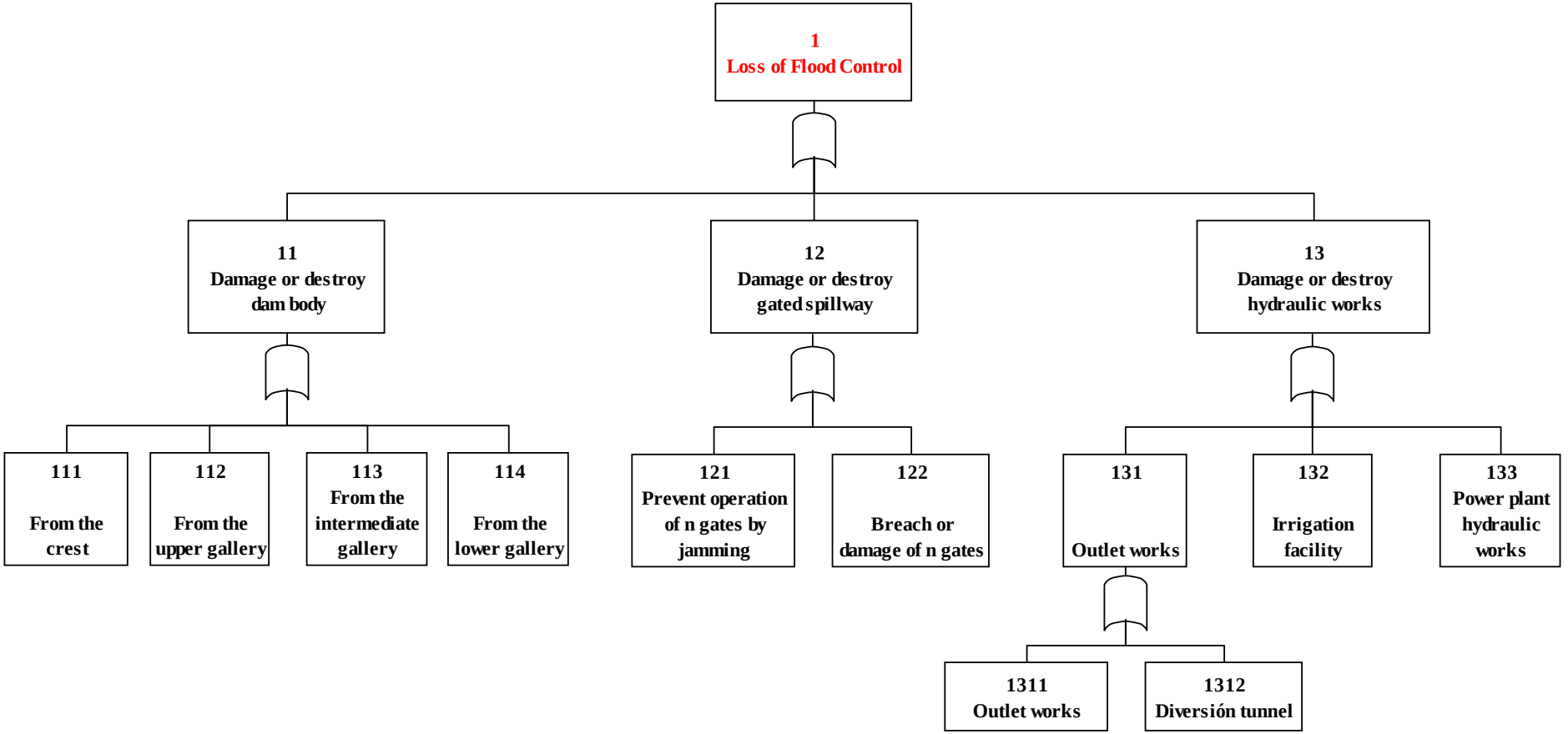
FTA: some important symbols



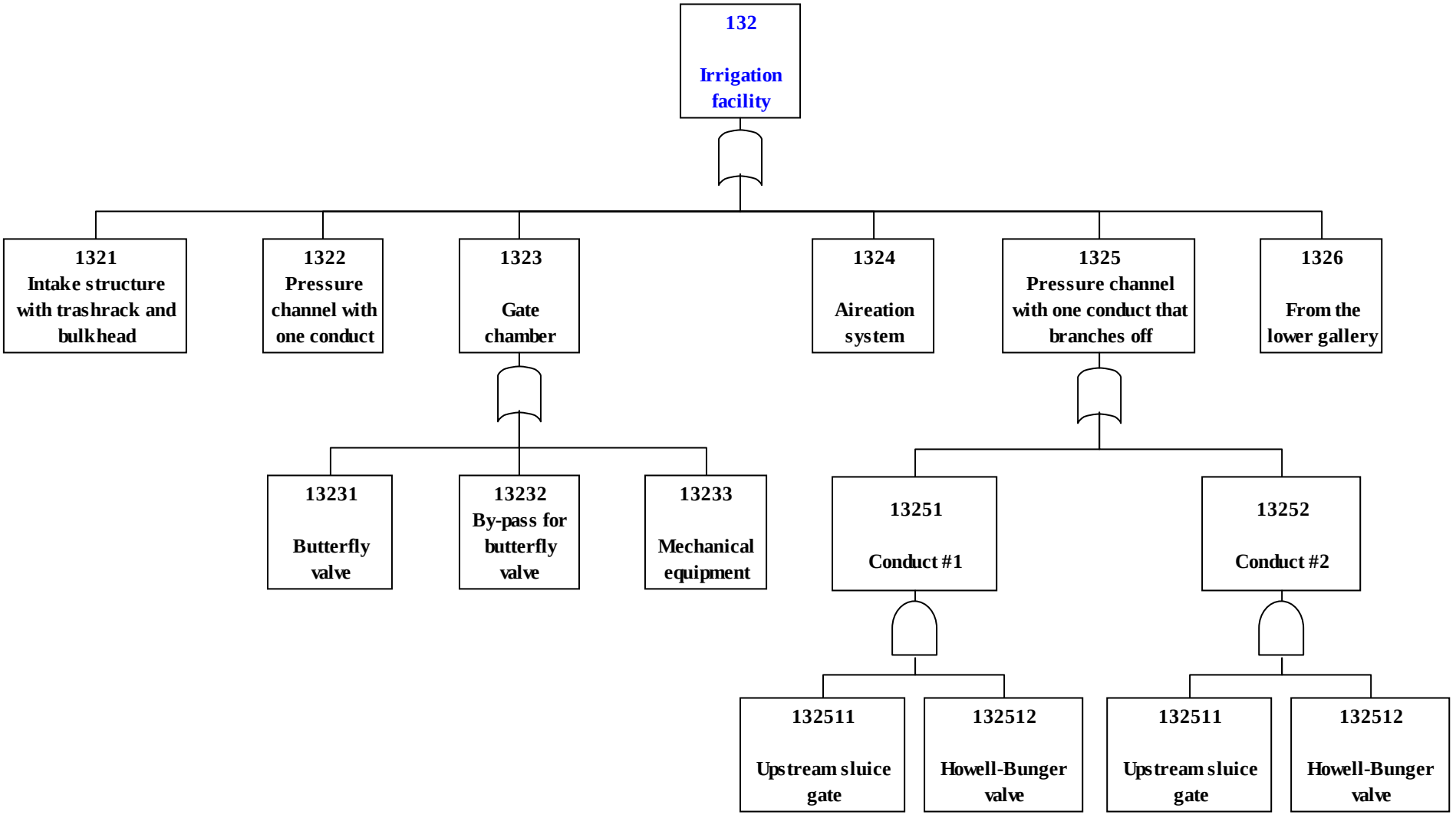
3.2. Customization of Fault Tree



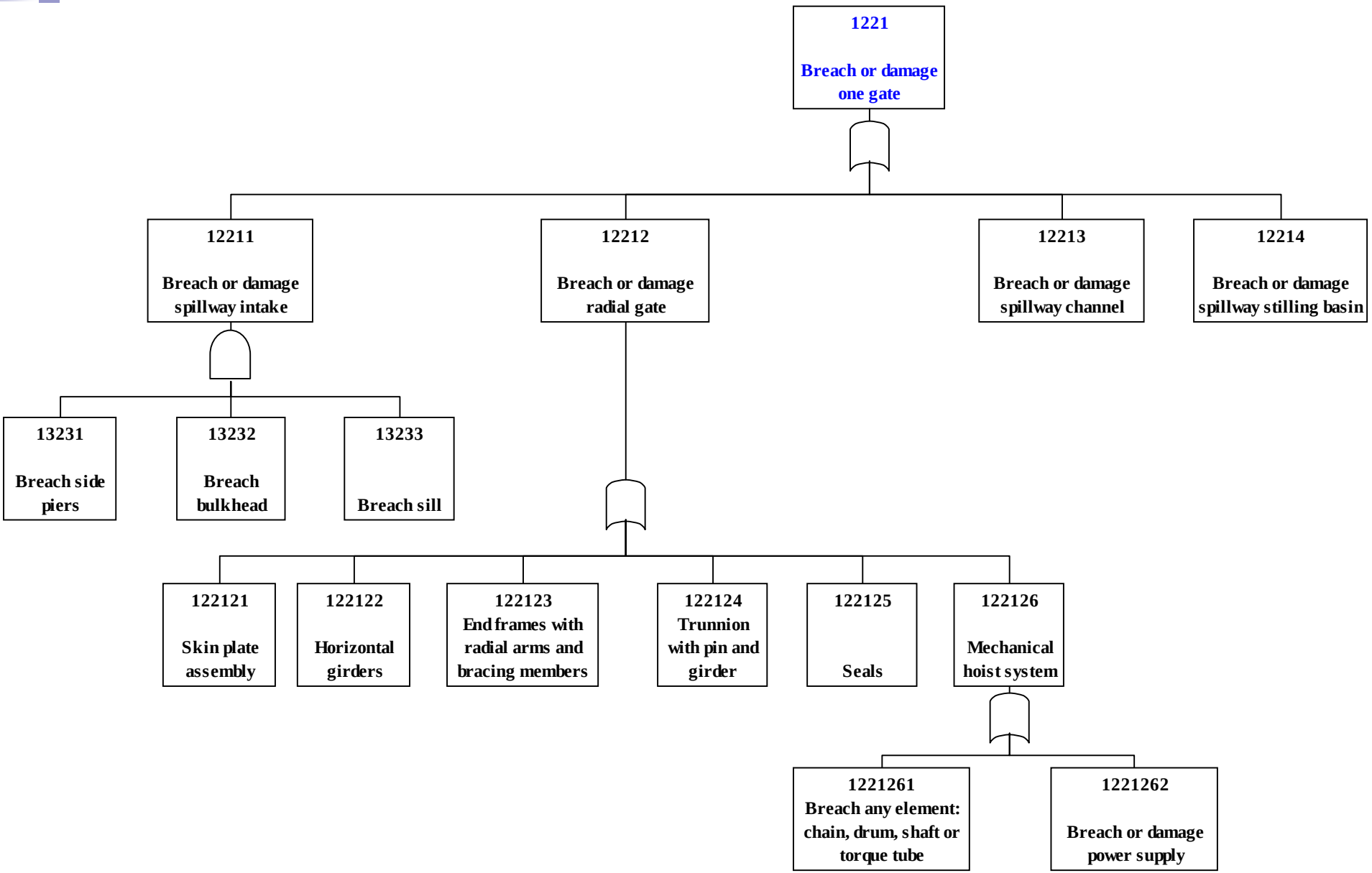
3.2. Customization of Fault Tree



3.2. Customization of Fault Tree



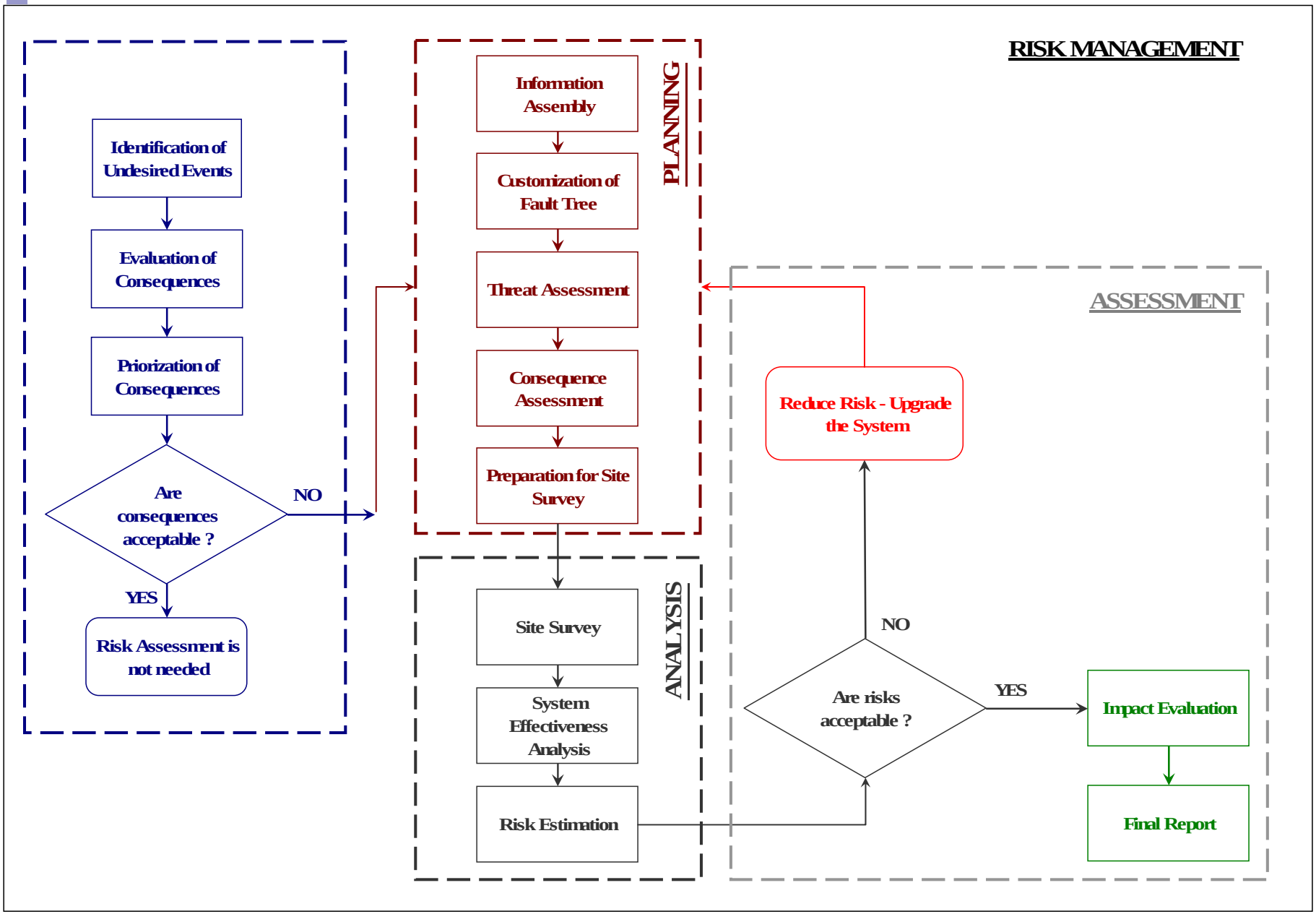
3.2. Customization of Fault Tree



Outline of presentation

1. Background
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - ***3.3. Threat assessment***
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

Qualitative Security Risk Assessment



3.3. Threat Assessment

- Threat description, carried out before any vulnerability analysis, and including possible adversaries, tactics, and capabilities
- Likelihood of attack, estimated per undesired event and per adversary group, taking into account statistics of past events and site-specific perceptions

3.3. Threat Assessment

- Types of adversaries:
  - Outsiders:
    - Terrorists
    - Criminals
    - Extremists
    - Vandals
    - Foreign intelligence personnel
    - Psychotics (people suffering from mental disorder)
  - **Insiders**

3.3. Threat Assessment

Adversary Capability	Adversary History	Relative Attractiveness of Asset to Adversary
•Access to region •Material resources •Technical skills •Planning skills •Financial resources	•Historic interest •Historic attacks •Current interest •Current surveillance •Documented threats	•Desired level of consequence •Ideology •Ease of attack

Source: Biringer et al, 2007

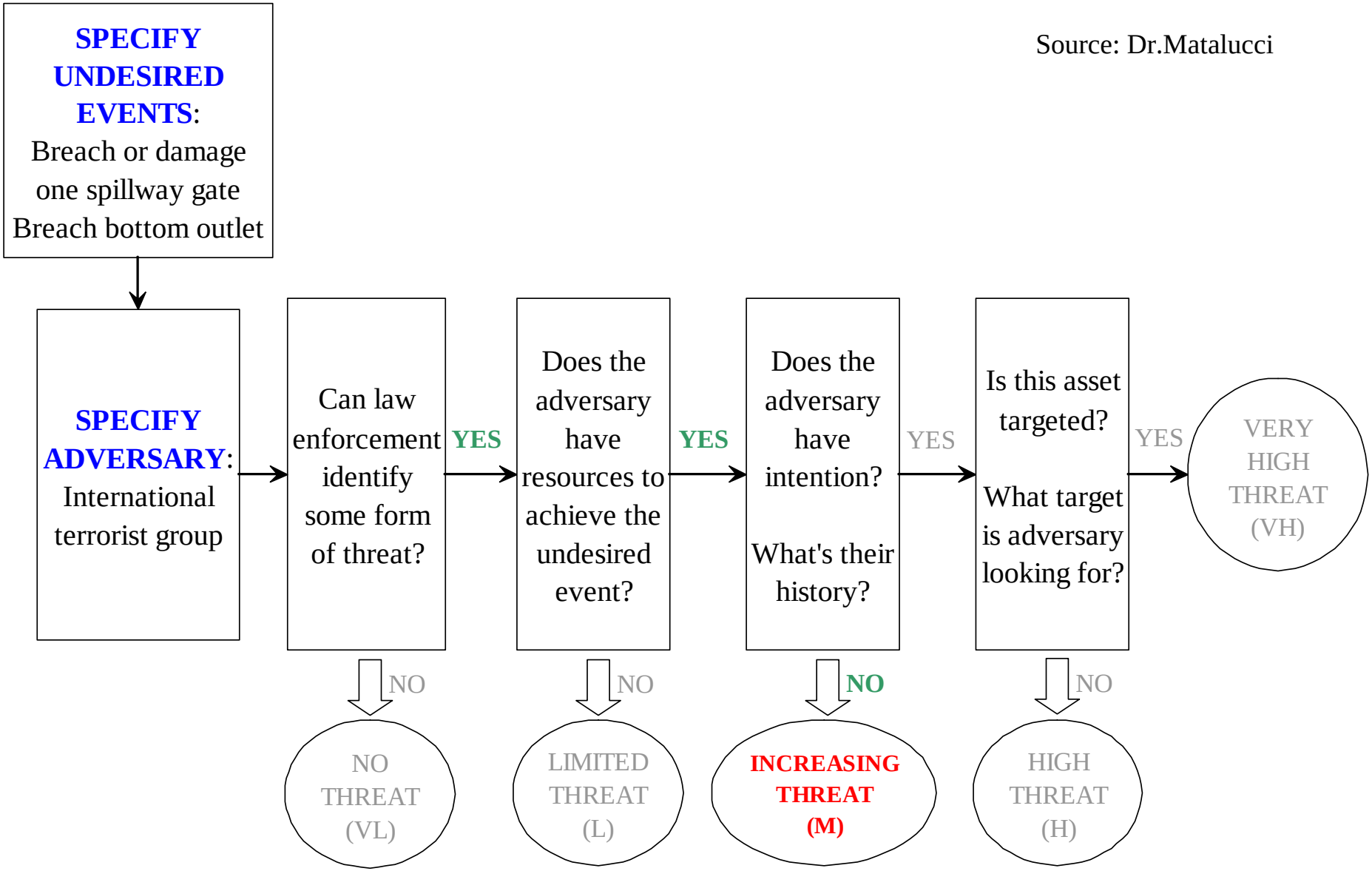
3.3. Threat Assessment

- This description of possible adversarial threats can be carried out:
  - **Based on present information**
  - **Based on "WHAT IF" scenarios**

- Since dam security is dynamic, it's important to **update** the threat assessment

3.3. Threat Assessment

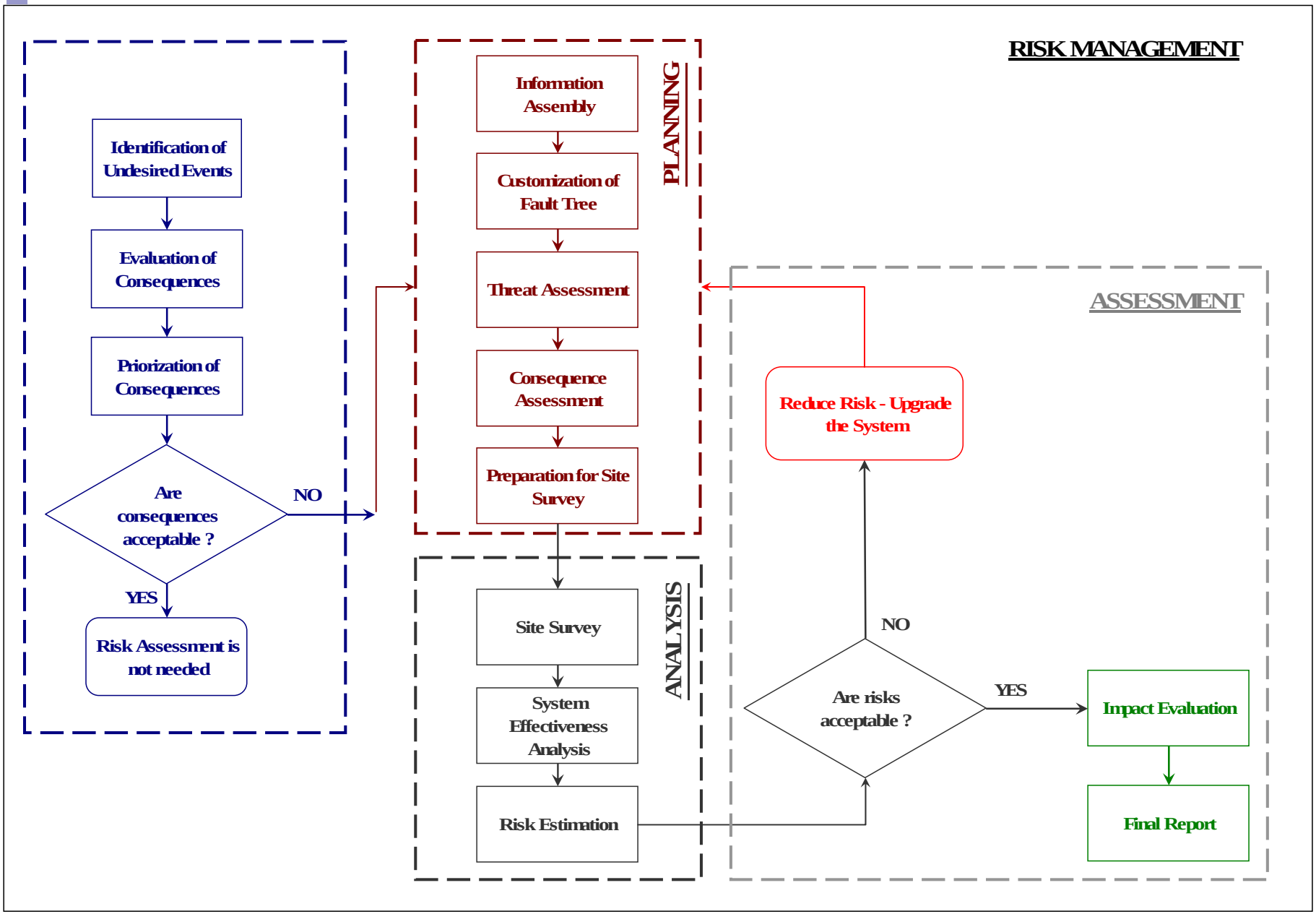
Source: Dr.Matalucci



Outline of presentation

1. Background
2. Screening analysis
3. **Planning**
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - ***3.4. Consequences assessment***
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

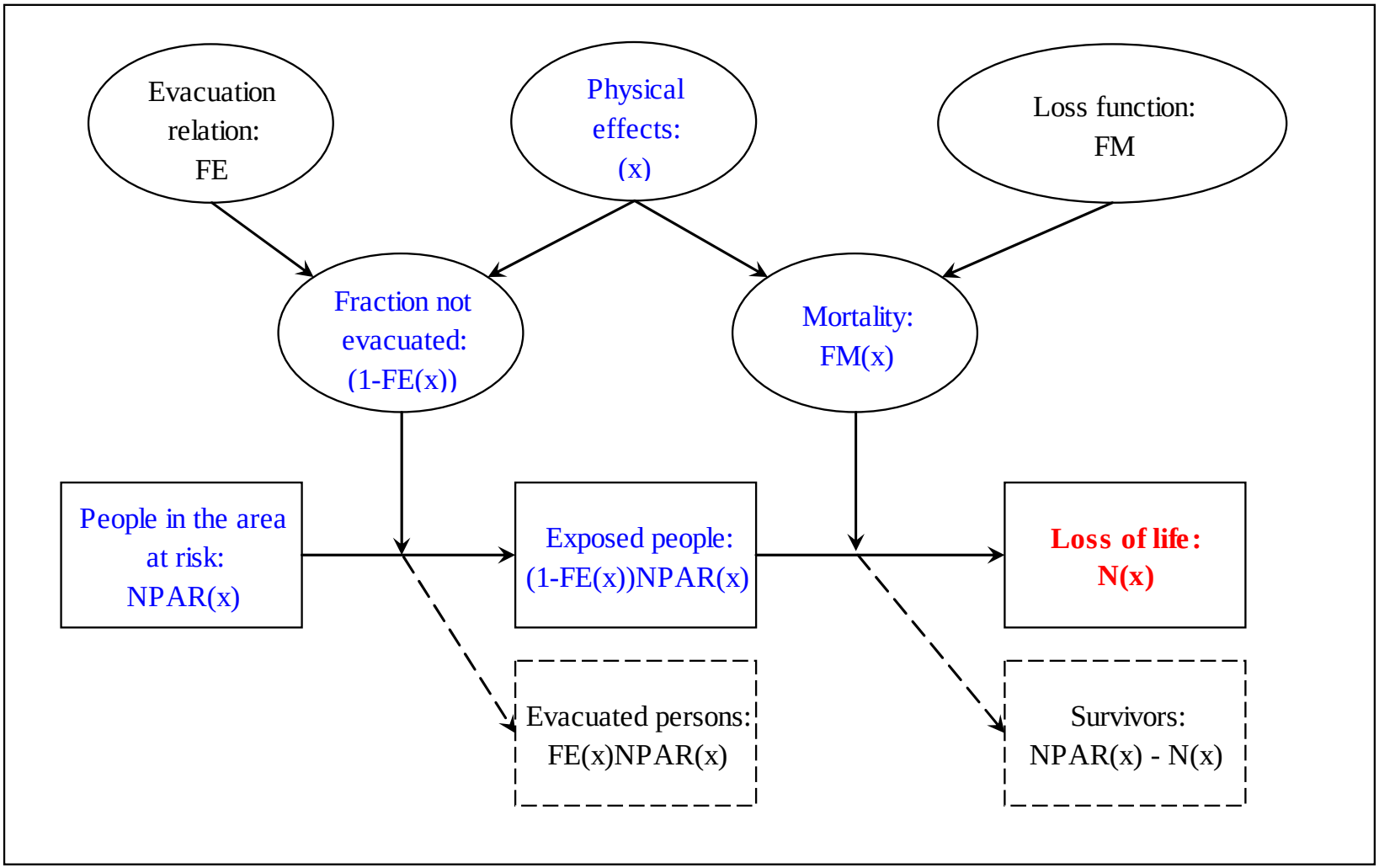
Qualitative Security Risk Assessment



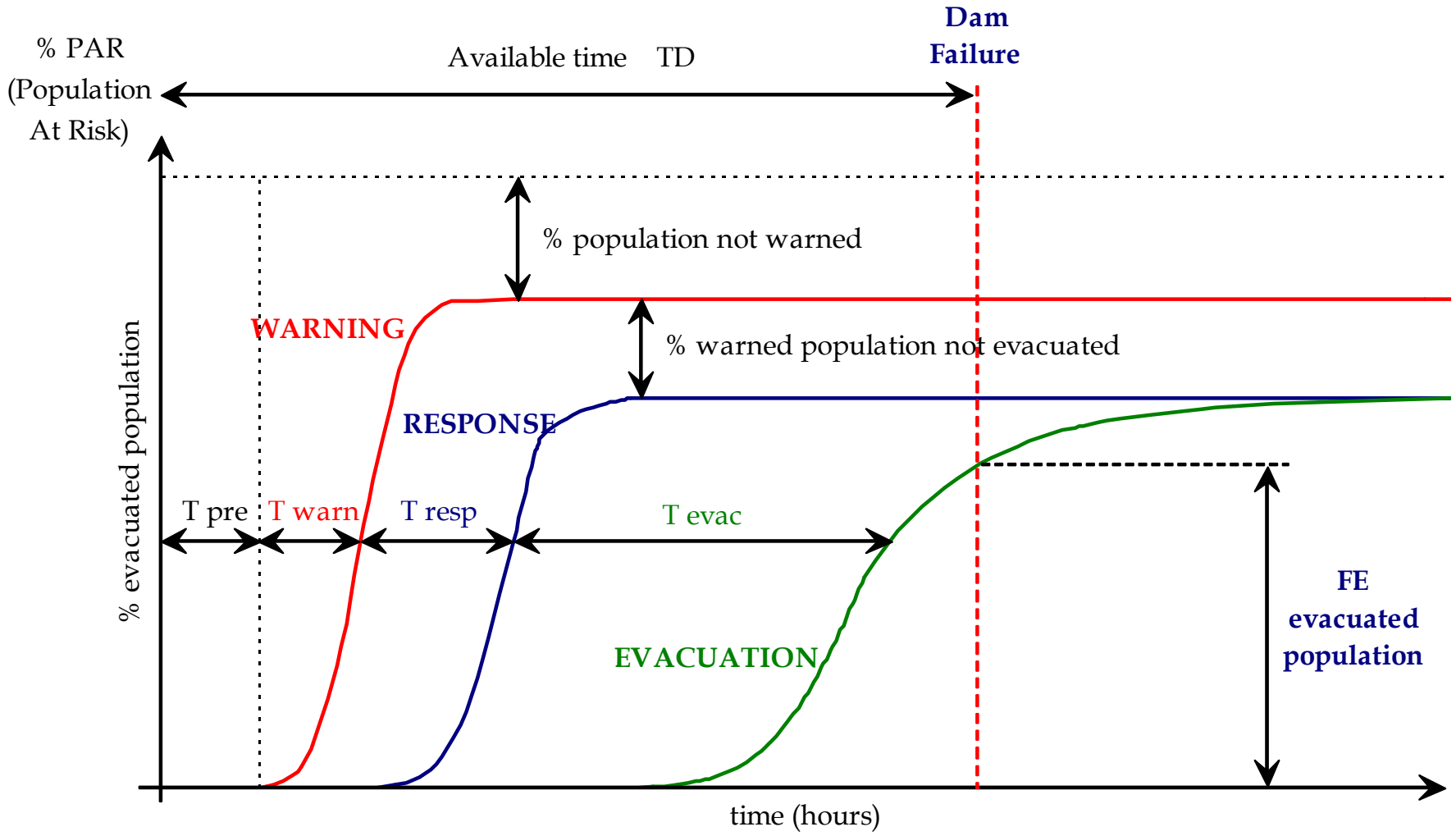
3.4. Consequence Assessment

Table 1 - Consequence values					
	Very High Score = 10	**High S = 8**	**Medium S = 6**	**Low S = 4**	**Very Low S = 2**
Public Safety	Population at risk is very high (**PAR>1000 people**)	Population at risk is high **(PAR = 100-1000)**	Population at risk is medium **(PAR = 10-100)**	Population at risk is low **(PAR = 1 - 10)**	There is no population at risk (except incidentaly)
Economic	National to multi-region disruption of essential facilities and access. Economic Impact: **Massive losses (>€1B)**	Multi-regional disruption of essential facilities and access. Economic Impact: **Multi-regional losses, (€100M to €1B) major public and private facilities**	Regional disruption of essential facilities and access.Economic Impact: **Regional losses, (€10M to €100M).**	Local to regional disruption of essential facilities and access. Economic Impact: **Local to regional (< €10M).**	No disruption of essential facilities and access. Economic Impact: **Minimal and confined to facility only**
Environmental	Massive environmental mitigation cost or impossible to mitigate.	Very large environmental cost mitigation and multi year recovery	Large environmental mitigation cost and 1 to 2 years to recover	Medium environmental mitigation cost and less than 1 year to recover	Minor environmental mitigation cost

3.4. Consequence Assessment



3.4. Consequence Assessment



Outline of presentation

1. Background
2. Screening analysis
3. **Planning**
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - ***3.5. Preparation for site survey***
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

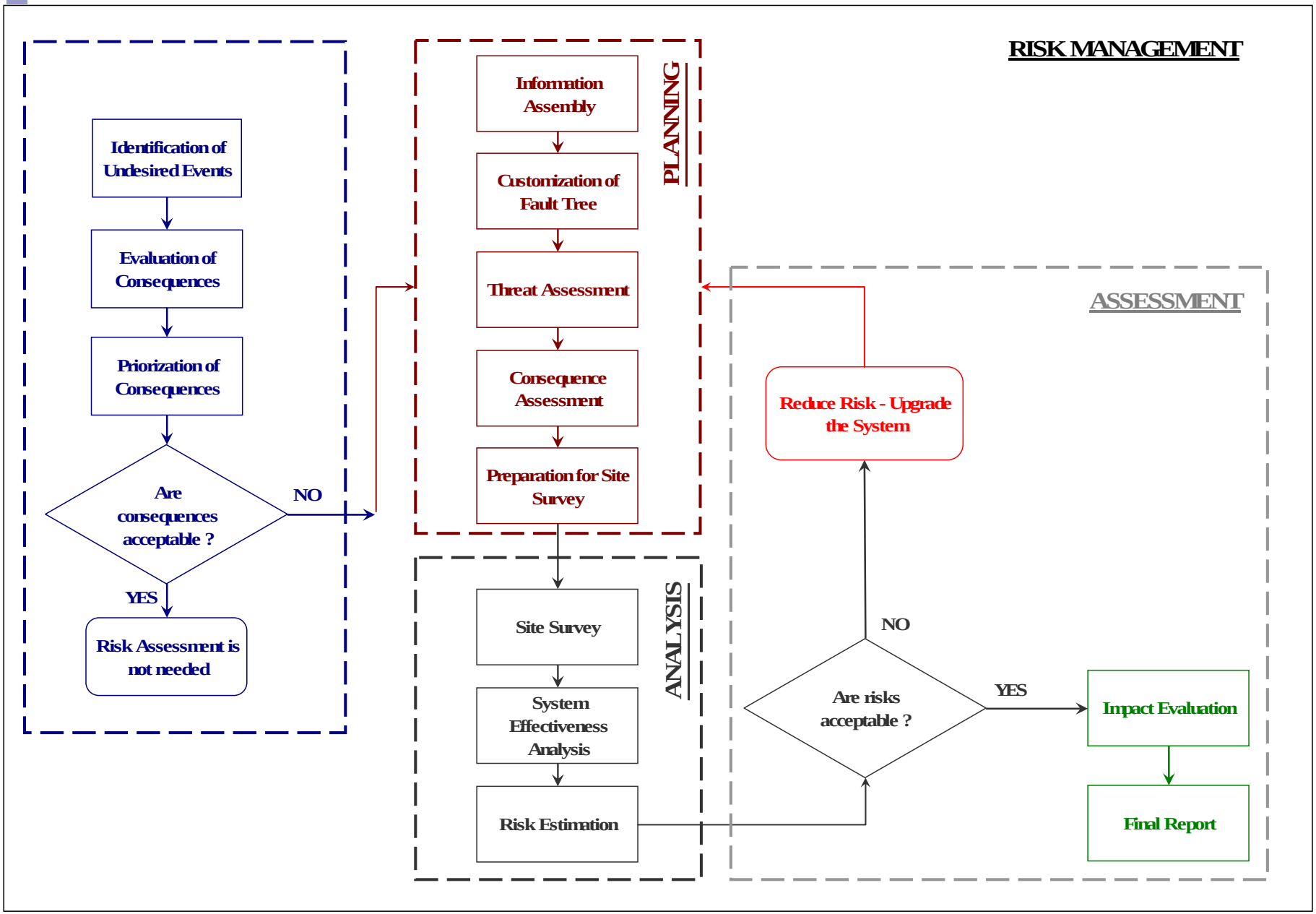
3.5. Preparation for site survey

- Prior to the surveys, check-sheets and worksheets are handed out
  - List of potential critical assets
  - List of dam missions
  - List of security systems: protection layers and elements between areas of the dam and its appurtenances
  - Emergency planning and procedures
  - Site layout showing targets and layers of protection

Outline of presentation

1. Background
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. **Analysis**
   - ***4.1. Site survey***
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. Risk management

Qualitative Security Risk Assessment



4.1. Site survey

- With the help of end-users and carried out by a team
- Collection of information not available before
- Completion and validation of:
  - Check-sheets and worksheets
  - System layout
- By means of observation and interviews
- It allows the system effectiveness analysis

4.1. Site Survey

1	Dam name/Nombre de la Presa	DAM 1
2	Location/Localización	
3	Type/Tipo	
4	Date built/Fecha de contrucción	
5	Purpose/Función	Retaining water, flood prevention/Almacenamiento y control de avenidas
6	Height (m)/Altura	
7	Crest Length (m)/Longitud de Coronación	
8	Storage (hm^3)/Capacidad	
9	Capacity of spillway (m^3/s)/Capacidad del Aliviadero	
10	Freeboard (m)/Resguardo	Storage is limited to 1/3 from September to December/Se limita la capacidad de almacenamiento a 1/3 entre Septiembre y Diciembre

WORKSHEET#1. DAM DATA

4.1. Site Survey

--- LEGEND OF LABELS AND SYMBOLS ---LEYENDAS Y SIMBOLOS

CA1, CA2…: Critical Assets/Puntos Criticos

- CA-1 Main spillway/Aliviadero principal
- CA-2 Dam body/Cuerpo de presa
- CA-3 Intermediate Gated spillway/Desagüe intermedio
- CA-4 Outlet works/ Desagüe de fondo
- CA-5 Dam office building/Casa de administración
- CA-6 Diversion tunnel/Tunel de desvío
- CA-7 Intake tower/Torre de toma
- CA-8 Pump station/Estación de bombeo
- CA-9 Regulation pool/Estanque de regulación
- CA-10 Recreation facility/Zonas de recreo

G1, G2… : Galleries/Galerías

C1, C2… : Chambers/Cámaras

E1, E2… : Elevators
- E1 Elevator to g 18.2
- E2 Elevator to well 2
- E3 Elevator to well 2

P1, P2… : Power supplies/Alimentación eléctrica
- P1 Voltage transformer 1
- P2 Voltage transformer 2
- P3 Voltage transformer 3

D1, D2… : Doors or gates/Puertas
- D1 Tous Road
- D2 Navarrés Road
- D3 Antella Road
- D4 Dam office building
- D5 Access to gallery D-4.1
- D6 Acces to well P2
- D7 Acces to well P3
- D8 Acces to well P4
- D9 Acces to spillway aireation conduit
- D10 First access intake towers
- D11 Access to intake valve tower
- D12 Exit from intake valve tower
- D13 Access to intake tower
- D14 Access to outlet works gallery
- D15 Access to reservoir from right abutment
- D16 Access to galleries from right abutment
- D17 Access to galleries from left side of spillway
- D18 Access to gated/ intermediate spillway
- D19 Access to gated/ intermediate spillway stilling basin
- D20 Access to voltage transformer 2
- D21 Access to voltage transformer 3
- D22 Access to regulating pool
- D23 Access to jucar-turia channel
- D24 Access to outlet works through Gallery G 14-1
- D25 First access to water surge building
- D26 Second access to water surge building
- D27 Access to pump station building
- D28 Access to Murteral Creek
- D29 Access to voltage transformer 2
- D30 Access to reservoir from left abutment
- D31 Access to voltage transformer 2 building
- D32 Access to crest from left abutment
- D33 Access to Dam Toe
- D34 Access to Gallery G-4-1
- D35 Access to voltage transformer 3 building
- D36 Access to bridge over the Jucar River
- D37 Internal Door before the jucar bridge

A1, A2… : Other assets/Otros elementos

F1, F2…: Fence or other physical barrier/Valla u otra Barrera Fisica

R1, R2… : Road/Carretera
- R1 Road from Tous
- R2 Road from Navarrés
- R3 Road from Antella
- R4 Road to access intermediate spillway intake
- R5 Road through the crest
- R6 Road to dam toe
- R7 Road to regulation pool
- R8 Road to recreational area (point view)
- R9 Road to acces reservoir from left abutment

S1, S2… : Security systems such as tv cameras or movement sensors
- S1 Camera at D1
- S2 Camera at D2
- S3 Camera at D3

WORKSHEET#2. SYSTEM LAYOUT

DAM MISSION LOSSES PERDIDAS DE MISION DE LA PRESA	INVOLVED CRITICAL ASSETS PUNTOS CRÍTICOS INVOLUCRADOS
Loss of Flood Control or Retaining Capacity Pérdida de capacidad y/o de control de avenidas	CA-1 Main spillway/Aliviadero principal CA-2 Dam body/Cuerpo de presa CA-3 Intermediate Gated spillway/Desagüe intermedio CA-4 Outlet works/ Desagüe de fondo CA-5 Dam office building/Casa de administración
Loss of Water supply and Irrigation Pérdida del abastecimiento y el riego	CA-2 Dam body/Cuerpo de presa CA-3 Intermediate Gated spillway/Desagüe intermedio CA-4 Outlet works/ Desagüe de fondo CA-5 Dam office building/Casa de administración CA-6 Diversion tunnel/Tunel de desvío CA-7 Intake tower/Torre de toma CA-8 Pump station/Estación de bombeo CA-9 Regulation pool/Estanque de regulación
Loss of Recreation and Tourism Pérdida de la zonas de Recreación y Turismo	CA-2 Dam body/Cuerpo de presa CA-3 Intermediate Gated spillway/Desagüe intermedio CA-4 Outlet works/ Desagüe de fondo CA-5 Dam office building/Casa de administración CA-6 Diversion tunnel/Túnel de desvío CA-7 Intake tower/Torre de toma CA-8 Pump station/Estación de bombeo CA-9 Regulation pool/Estanque de regulación CA-10 Recreation facility/Zonas de recreo

WORKSHEET#3. DAM MISSION LOSSES AND CRITICAL ASSETS

Name/ Nombre:	Intermediate Gated spillway	**Label/ Etiqueta:**	CA3	**Location/ Localización:**	Inside the dam/ Dentro de la presa

Physical description: Descripción Fisica	intake structure (trashracked)/Toma pressure channel/Conducción a presión gate chamber/Cámara de compuertas sluice gate/compuerta tajadera by-pass/by-pass radial gate/compuerta radial mechanical equipment/equipamiento electromecánico aireation system/sistema de aireación open channel/canal de descarga stilling basin/cuenco amortiguador						
Function: Función	Collect water from the upstream side of a dam to the downstream side/Conducir el agua desde aguas arriba hasta aguas abajo						
Condition: Condición	⊗ Good/Buena		Average/Regular		Bad/mala		
How often is this asset visited? Con que frecuencia se visita?	All the time/en todo momento	Couple of times per day/2 veces al día	⊗ Once per day/Una vez al día	Couple of times per week/2 veces por semana	Once per week/1 vez por semana	Randomly/ Aleatoriamente	Rarely/ Ocasionalmente
Who visits the asset? Quien lo visita?	Dam Operator once per day and dam officer and maintenance company once or twice per week/Un operador al menos una vez al día y un official de presa o personal de la empresa de mantenimiento una vez a la semana						
Comments, notes, sketches Comentarios, notas, esquemas…:	WORKSHEET#4. DETAILED DESCRIPTION OF CRITICAL ASSETS						

4.1. Site Survey

Name Nombre	Label Etiqueta	Location Localización	Type Tipo (material)	Lock type Tipo de cerradura	Other comments Otros comentarios
Door Puerta	D1	R1	Iron/Metal	Conventional /Convencional	Can be opened remotely/Puede operarse remotamente. There is also a camera (S1)/Tiene una cámara (S1). Vehicles/Paso de vehículos.
Door Puerta	D2	R2	Iron/Metal	Conventional /Convencional	Can be opened remotely/Puede operarse remotamente. There is also a camera (S2)/Tiene una cámara (S2). Vehicles/Paso de vehículos.
Door Puerta	D3	R3	Iron/Metal	Conventional /Convencional	Can be opened remotely/Puede operarse remotamente. There is also a camera (S3)/Tiene una cámara (S3). Vehicles/Paso de vehículos.
Door Puerta	D4	Dam office building/Edificio de control de la presa	Iron/Metal	Reinforced /Blindada	
Door Puerta	D5	Access to gallery D-4.1. /Acceso a gallería D-4.1	Iron/Metal	Conventional /Convencional	
Door Puerta	D6	Acces to well P2/Acceso a pozo P2	Iron/Metal	Conventional /Convencional	
Door Puerta	D7	Acces to well P3/Acceso a pozo P3	Iron/Metal	Conventional /Convencional	
Door	D8	Acces to well P4/Acceso a pozo P4	Iron/Metal	Conventional /Convencional	
Door	D9	Acces to spillway aireation conduit. Acceso a la aireación del aliviadero	Iron/Metal	Conventional /Convencional	

WORKSHEET#5:
LOCATION AND DESCRIPTION OF PHYSICAL BARRIERS

4.1. Site Survey

Element /Elemento	**Location** /Localización	**Label** /Etiqueta	**Condition & Maintenance** /Condición y Mantenimiento			**Operation mode** Modo de trabajo			**Who * + What** Quién + qué
Camera /Cámara	Door 1 /Puerta 1	S1	**Excellent** Excelente	Good Buena	Poor Mala	**24/7**	Often A menudo	Seldom Poco	Dam officer/vehicles Oficial de presa/vehículos
Camera /Cámara	Door 2 /Puerta 2	S2	**Excellent** Excelente	Good Buena	Poor Mala	**24/7**	Often A menudo	Seldom Poco	Dam officer/vehicles Oficial de presa/vehículos
Camera /Cámara	Door 3 /Puerta 3	S3	**Excellent** Excelente	Good Buena	Poor Mala	**24/7**	Often A menudo	Seldom Poco	Dam officer/vehicles Oficial de presa/vehículos

*: Who receives the output of the system? For example, in case of a tv camera, who watches the cameras, in case of an intrusion alarm, who receives the alarms…Quién recibe la información del sistema de seguridad? Por ejemplo, en caso de una camara de television, quién la ve, en caso de una alarma anti-intrusismo, quién la recibe

WORKSHEET#6. LOCATION AND DESCRIPTION OF SECURITY SYSTEMS

4.1. Site Survey

Past security incidents (attacks, sabotages, vandalism…). /Incidentes	Boats through the reservoir getting to closed to the dam/Botes que se acercan a la presa Hunters/Cazadores Pedestrians entering in the dam area/Peatones que entran en el area de la presa
Communication systems. /Sistemas de comunicación	Telephone/Teléfono Internal wireless telephone/Teléfono inalámbrico Mobile Phone/Teléfono móvil
Distance and time from the nearest response force (police, army or similar) to the dam. /Distancia y tiempo hasta el puesto de fuerzas del estado más cercano	20 minutes/20 Minutos
Are there operative communication protocols between the dam and the nearest response force?/Hay protocolos de comunicación operatives entre la presa y la fuerza del orden más cercana?	No
Do the response forces have action protocols in case of an attack event? Tienen las fuerzas del orden protocolos de actuación en la eventualidad de un ataque?	No
Potential response forces on the site (armed officers on the site). Hay fuerzas de orden en la presa	No
Type of security surveillance provided by technical personnel on the site on the site. Qué tipo de seguridad aporta el personal propio de la presa	Permanent personnel at dam control office building Maintenance supervisor team during day time /Personal de presa permanente y supervisión durante el día
Emergency Action Plan (Is it operative? Are there alarms in the downstream populations? Are there protocols with Civil Protection to evacuate people?). Plan de Emergencia (está operativo?) Hay alarmas para avisar a la población de aguas abajo? Hay protocolos de evacuación con protección civil?	Emergency action plan is not implemented. /El plan de emergencia no está operativo, no está implementado.

WORKSHEET#7.

MISCELLANEUS INFORMATION

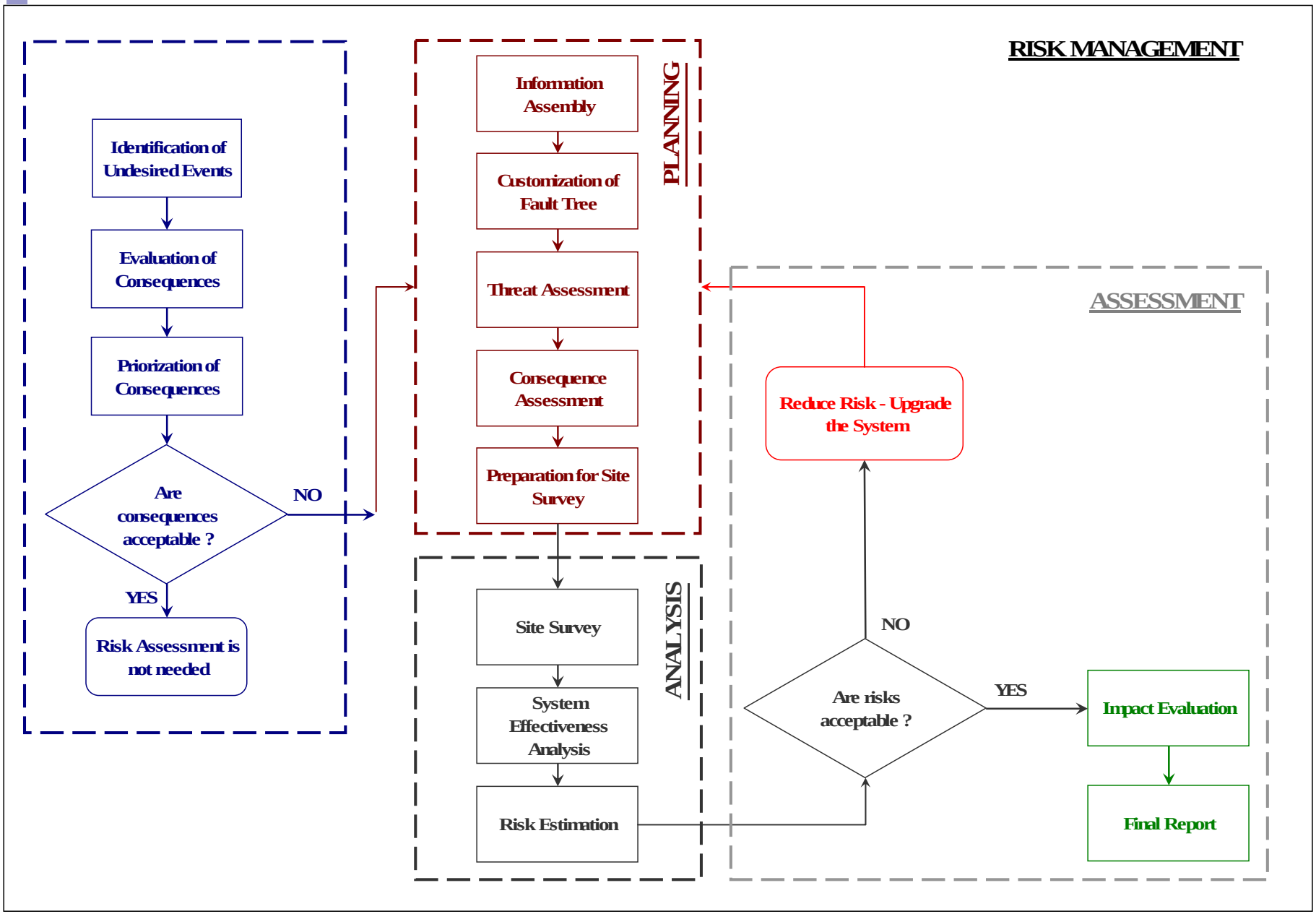
Name: /**Nombre:**	Intermediate Gated	**Label:** /**Etiqueta**	**CA3**	**Location:** **Localización:**	Inside the dam/ Dentro de la presa
List of physical barriers. Listado de barreras fisicas	D2(S2);D15;D7;E3;D3;D37;D33;D18				
Path of the shortest distance to get to the critical asset (estimate distances in meters). Camino más corto a los puntos críticos (estimar la distancia en metros).	D2-100m-D15-700m-100m D2-500m-D7-E3 D3-200m-D37-600m-D33-300m-D18-150m D1-2000m- D33-300m-D18-150m D1-1600m-D32-500M- D7-E3				
Path of most vulnerable way to get to the critical asset. (estimate distances in meters). Camino más vulnerable a los puntos críticos (estimar la distancia en metros).	D2-500m-D7-E3				

WORKSHEET #8. PATHS TO CRITICAL ASSETS

Outline of presentation

1. Background
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. **Analysis**
   - *4.1. Site survey*
   - ***4.2. System effectiveness analysis***
   - *4.3. Estimation of risk*
5. Risk management

Qualitative Security Risk Assessment



4.2. System Effectiveness Analysis

System Effectiveness Analysis

- It estimates the security system effectiveness (P_E)
- System effectiveness (P_E) and system ineffectiveness ($1-P_E$) are complementary functions
- It indicates how well the security system protects against the threats and undesired events
- If system effectiveness is judged low, vulnerabilities will be identified and (P_E) will be used to calculate the risk to the dam
- An integration of the factors (detection, delay, response) that determine the system effectiveness is needed

System Effectiveness Analysis (definitions)

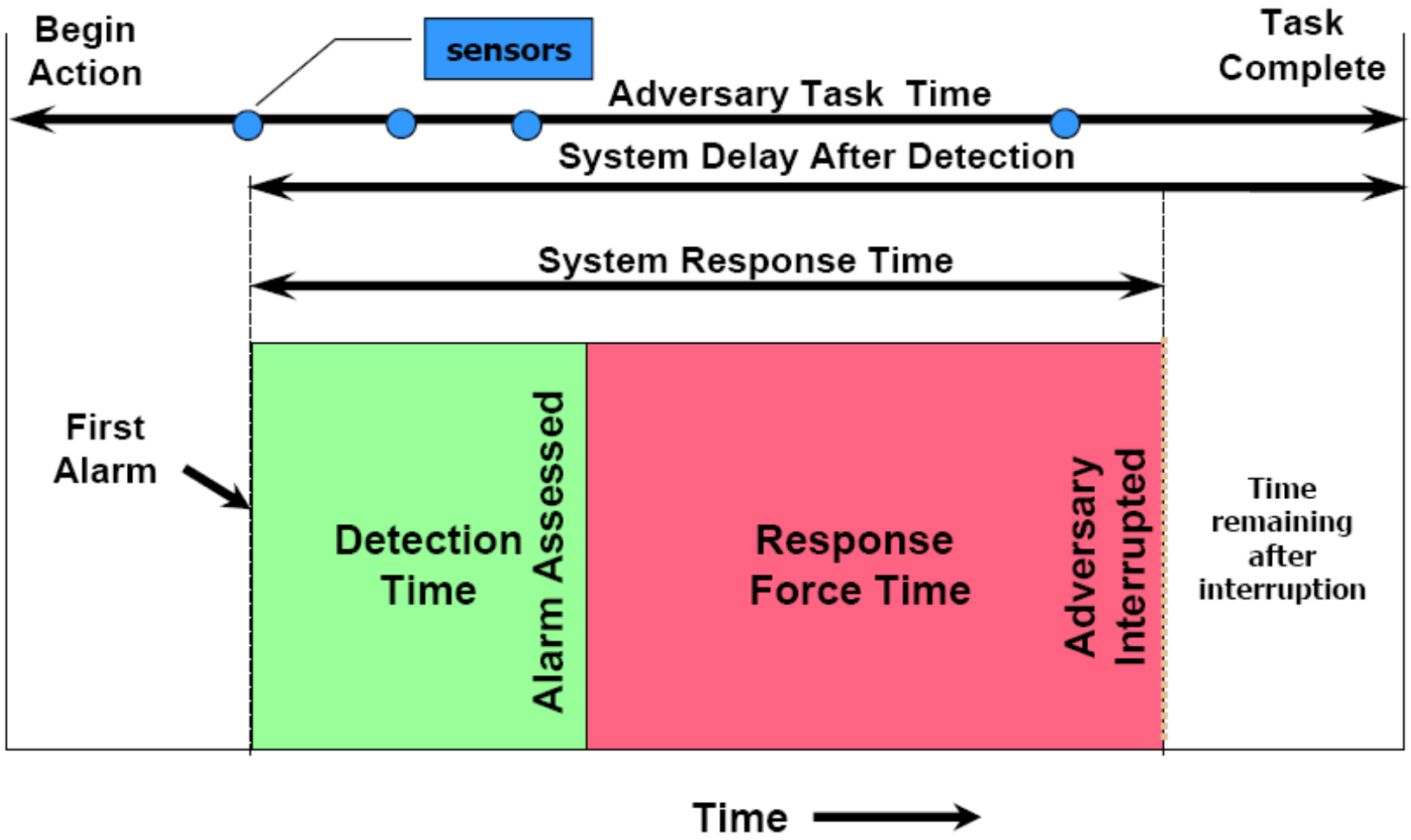
- ***Detection***: sensing, reporting, and assessment of an adversary action
- ***Delay***: a feature that impedes the adversary to progress in a particular step of its action
- ***Protection system***: physical security and cyber-security measures used to counter mission threats and consequences
- These physical system functions (detection, delay, and response) ***must be integrated*** to ensure that the adversarial threat is neutralized

System Effectiveness Analysis (definitions)

- ***Path***: route taken by an adversary from off-site through areas and path elements to reach the target and, optionally, to return off-site. It's a part of a scenario
- ***Scenario***: outline of events along a specific path by which the adversary plans to achieve his objective
- ***Most-vulnerable scenario***: the adversary scenario that takes the greatest advantage of the vulnerabilities of the security system
- ***Vulnerabilities:*** weaknesses or gaps in the protection system

4.2. System Effectiveness Analysis

By kind courtesy of Dr.Matalucci – RAM-D



Detection systems

	VL	L	M	H	VH	NA
1 All Fences		x				

VL for remote area, hardly ever visited
L for no detection system at all
M for random patrols
H for detection system
VH for 24/7 monitoring of detection system

	VL	L	M	H	VH	NA
2 All Vehicle Gates		x				

VL for remote area, hardly ever visited
L for no detection system at all
M for random patrols
H for detection system
VH for 24/7 monitoring of detection system

	VL	L	M	H	VH	NA
3 All Pedestrian doors		x				

VL for remote area, hardly ever visited
L for no detection system at all
M for permanent personnel on the spot
H for detection system
VH for 24/7 monitoring of detection system

Delay times

TABLE 1

	Time (s)
1 Fences	120
2 Vehicle Gates	60
3 Pedestrian doors	90

TABLE 2

Mode	Rate	
1 Walking	7 ft/s	2.2 m/s
2 Running	15 ft/s	4.6 m/s
3 Crawling	4 ft/s	1.2 m/s
4 Climbing (up or down)	1 ft/s	0.3 m/s
5 Driving (pick up)	54 ft/s	16.6 m/s

Response and Mitigation effectiveness

A Communication capability

VL for a very remote area with no communication system
L for no communication system
M for existance of a communication system
H for complete wireless or mobile phone coverage
VH for special emergency protocol and "red button"

B Response time

300 s	For explaining, understanding and making a decision
17 km	Distance to the nearest response force
80 km/h	Maximum speed limit on the road
765 s	Estimated travel time
600 s	To find the way around the dam
1665 s	Total response time

Response-Delay relations

			Result
Delay time	>	2,0 x Response time	**VH**
Delay time	>	1,5 x Response time	**H**
1,5 x Delay time	<	Response time	**L**
2,0 x Delay time	<	Response time	**VL**
Otherwise			**M**

This metrics is used owing to the expected length of most malicious actions that could take place at a dam. They might not last more than an hour.

4.2. System Effectiveness Analysis

Combination of several qualitative scores

- By means of peer review sessions: expert judgment
- Some other agreed criteria:
  - Applying the lowest score
  - Using verbal probability descriptors and operating:
    - Carrying out a gross average of scores
    - Strictly applying probability laws, such as the Central Limit Theorem and the Principle of Independence

DAMSE verbal descriptors proposal

Descriptor	Description of Condition or Event	Order of Magnitude of Probability Assigned
		1
Very High	Occurrence is virtually certain	**0,99**
		0,95
High	Occurrence of the condition or event are observed in the available database	**0,90**
		0,85
Medium	The occurrence of the condition or event is not observed, or is observed in one isolated instance, in the available database; several potential failure scenarios can be identified.	**0,5**
		0,10
Low	The occurrence of the condition or event is not observed in the available database. It is difficult to think about any plausible failure scenario; however, a single scenario could be identified after considerable effort.	**0,05**
		0,01
Very Low	The condition or event has not been observed, and no plausible scenario could be identified, even after considerable effort.	**0,001**

4.2. System Effectiveness Analysis

Example of a two critical assets and one of its potential attacks:

Critical asset

Spillway Gate

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into chamber through D4 or D3	L		90 s			
Get to control panel and gates	L		120 s			
Task	L		300 s			
Total	**L**	**M**	**410 s**	**1665 s**	**VL**	**VL**

Notes.-
Task delay time is assessed by engineering judgement

Combination of several qualitative scores

Bottom outlet at old diversion tunnel

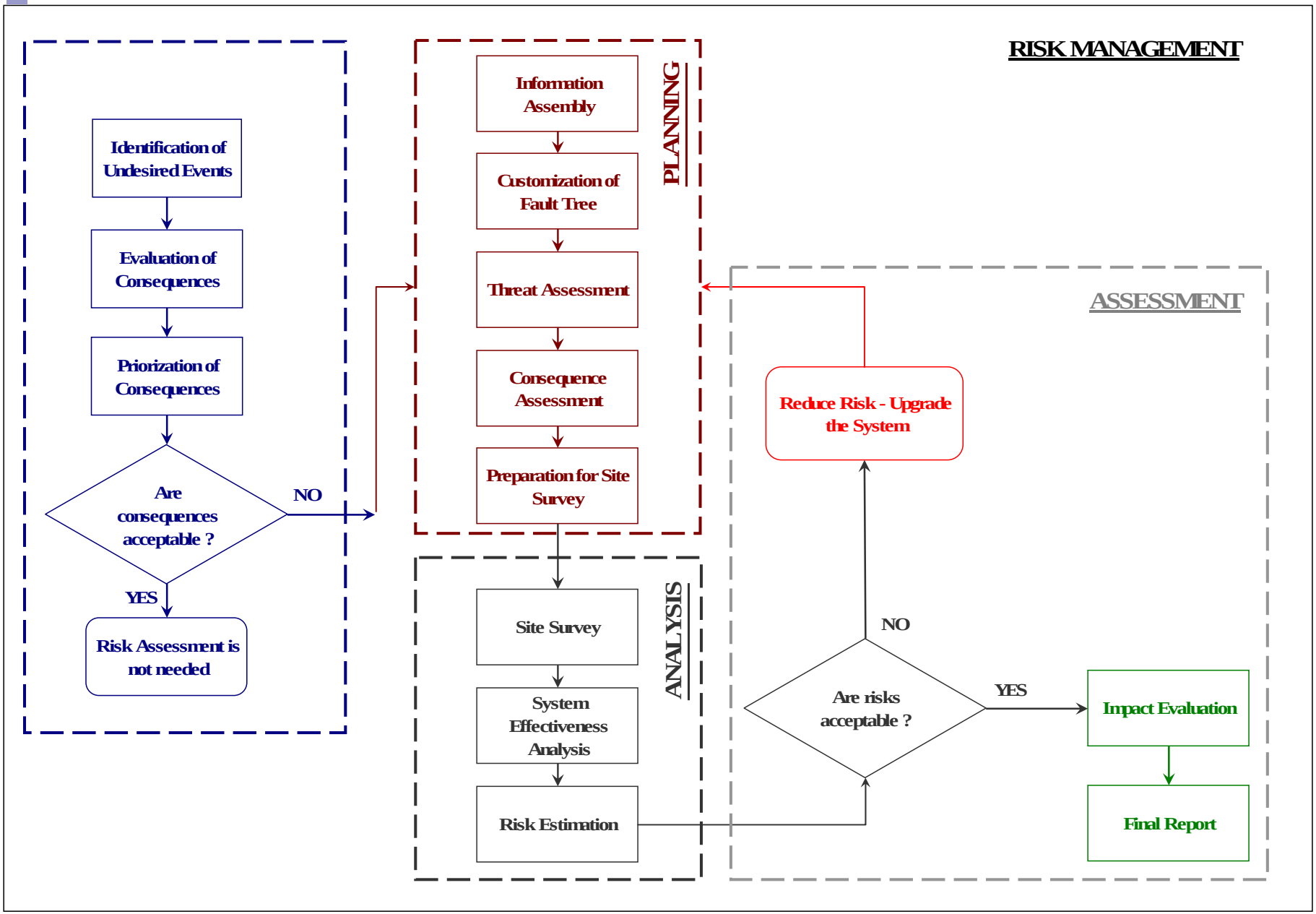
International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through G3 or G4	L		60 s			
Get to tunnel entrance by car (D8) = 80m	L		5 s			
Break into tunnel through D8	L		90 s			
Get to valve chamber = 155m	NA		9 s			
Task	NA		600 s			
Total	**L**	**M**	**723 s**	**1665 s**	**VL**	**VL**

Notes.-
Task delay time is assessed by engineering judgement

Outline of presentation

1. Background
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. **Analysis**
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - ***4.3. Estimation of risk***
5. Risk management

Qualitative Security Risk Assessment



4.3. Estimation of risk

- Some “measure” is needed to make the best decisions to manage security risk
- The security risk value obtained in DAMSE is a *qualitative estimate* of security risk
- The purpose is to provide a reference point for evaluating and comparing other security risks
- The three basic parameters are accounted for: likelihood of adversary attack, system ineffectiveness, and the consequences
- When there’s not enough information to estimate attack likelihood or when consequences are extremely high, *Conditional Risk* can be used (doesn’t include the initiating event and focuses on system ineffectiveness and consequences)

4.3. Estimation of risk

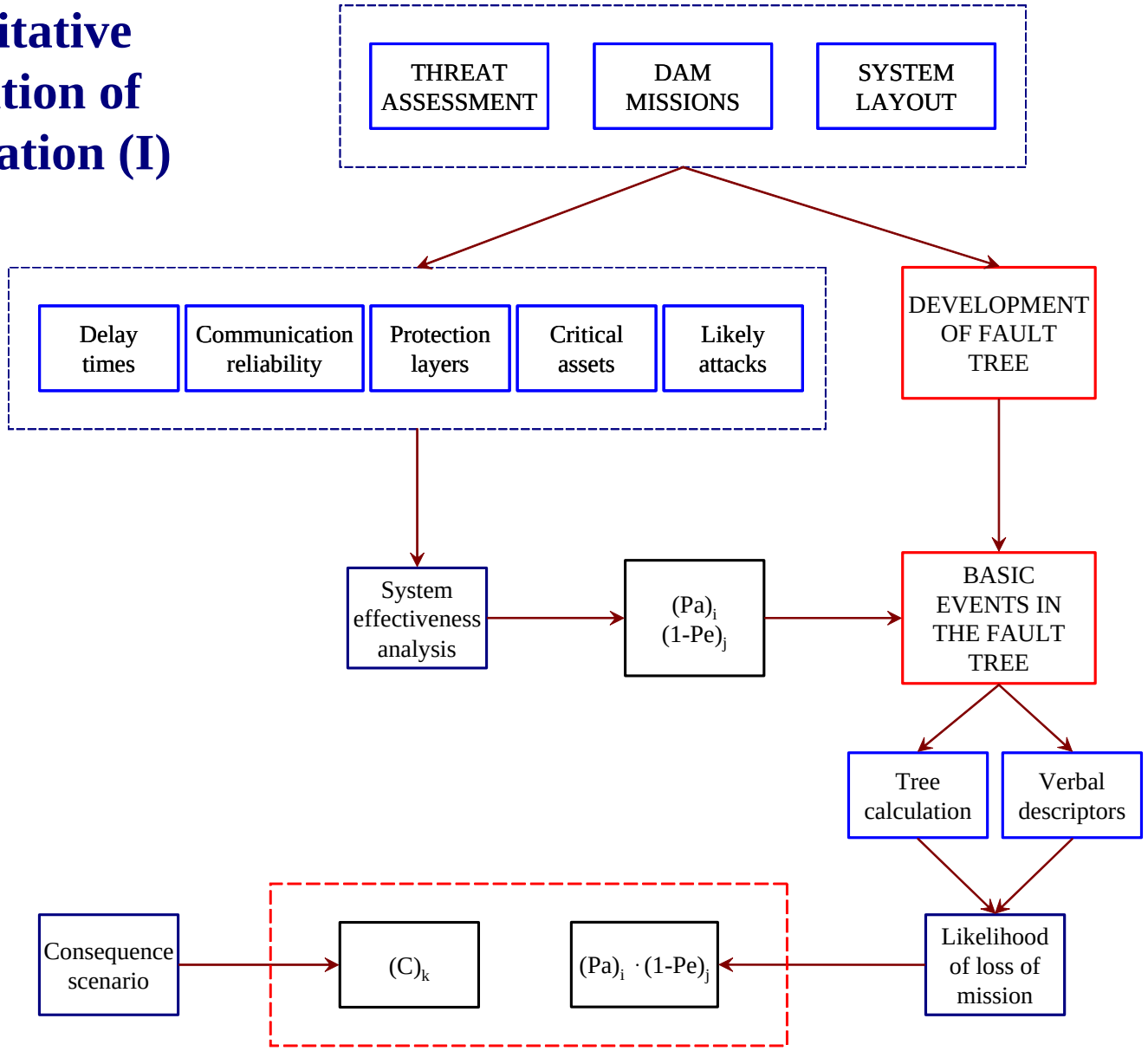
Threat: international terrorist group

Prior to any security upgrade:

	P_A	$(1 - P_E)$	C	R
Damage or breach of gates	M	VH	L	L
Damage or breach of outlet works	M	VH	L	L

4.3. Estimation of risk

Quantitative calculation of risk equation (I)



Quantitative calculation of risk equation (II)

- Since we use a deductive approach with the fault tree, we could have several cut sets depending on the number of basic events that we have
- Each basic event would be also linked to several “i” potential attacks and a “j” system ineffectiveness:

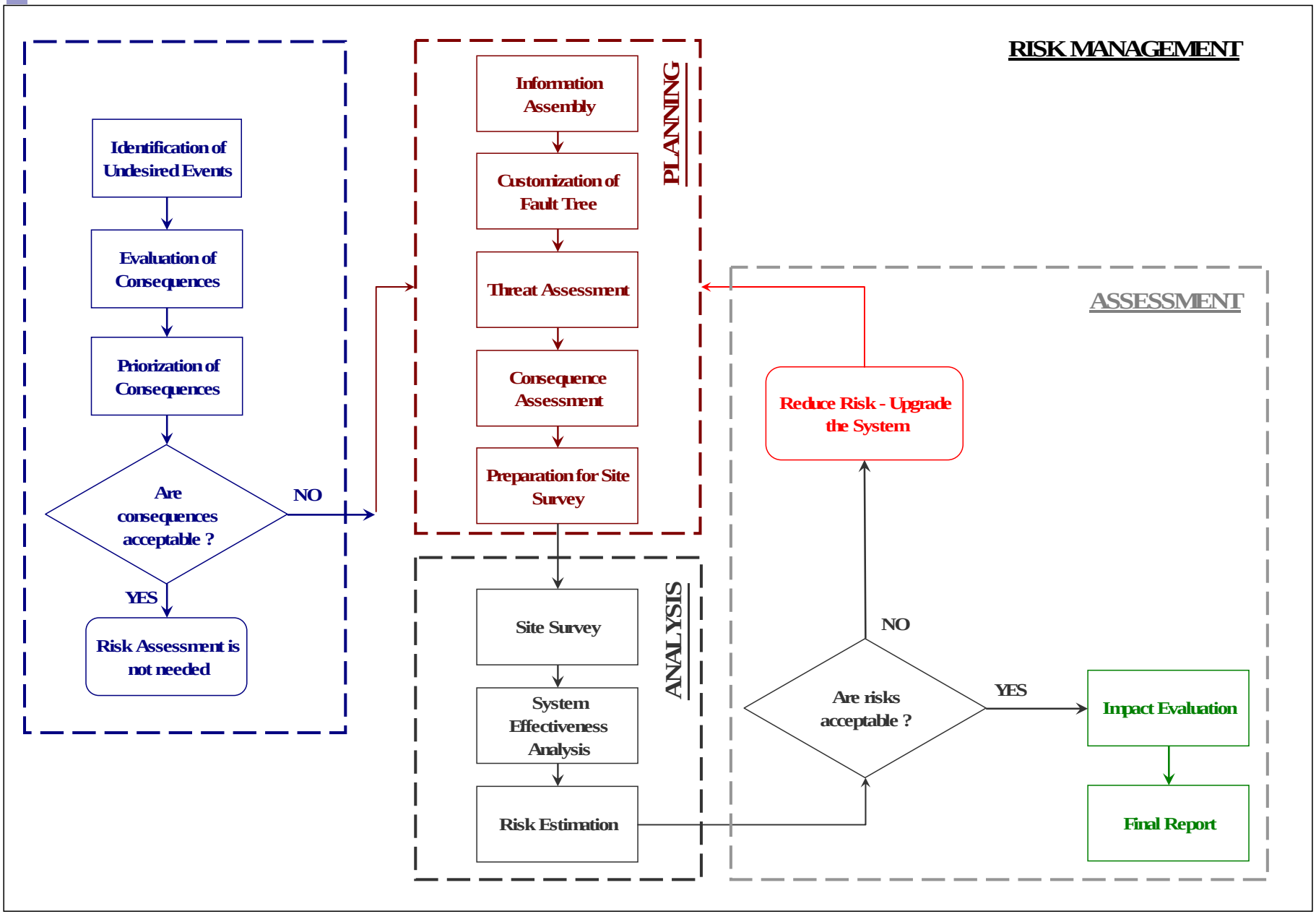
$$[(P_a)_i \cdot (1\text{-}P_e)_j]$$

- Besides, we would estimate several “k” consequence scenarios

Outline of presentation

1. Background
2. Screening analysis
3. Planning
   - *3.1. Facility characterization*
   - *3.2. Customization of Fault Tree*
   - *3.3. Threat assessment*
   - *3.4. Consequences assessment*
   - *3.5. Preparation for site survey*
4. Analysis
   - *4.1. Site survey*
   - *4.2. System effectiveness analysis*
   - *4.3. Estimation of risk*
5. **Risk management**

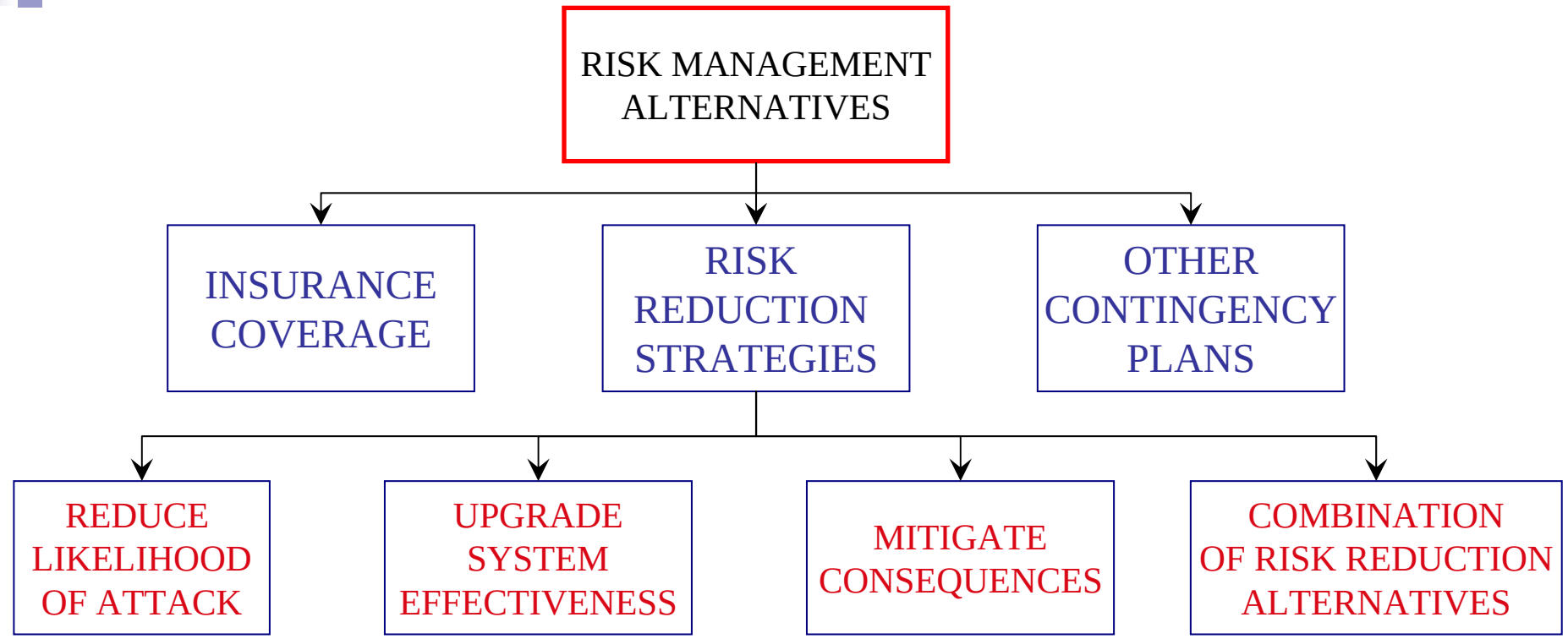
Qualitative Security Risk Assessment



General risk management options:

- Avoid the risk (decommissioning)
- Reduce the probability of undesired events (structural measures)
- Reduce the consequences (non-structural measures)
- Transfer the risk (contractual arrangement or sale)
- Retain or accept residual risk (insurance)

5. Risk Management



- SURVEILLANCE
- DETERRENCE
- NATIONAL DEFENSE

- DETECTION: sensors, cameras, access control
- DELAY: barriers, walls active-passive systems
- RESPONSE FORCE

- HARDENING
- RECOVERY STRATEGIES
- REDUNDANCY
- EMERGENCY ACTIONS

General risk management options:

- Risk reduction strategies are suggested if the estimated risk level is above threshold
- Followed by re-evaluating consequences and protection system effectiveness to measure relative risk reduction
- There's a need to consider:
  - Risk Reduction Upgrades or Packages
  - Their influence on the mission of the dam
  - Their cost-effectiveness

Example of risk reduction measures analysis

Security upgrade implementation:

1. Intrusion detection system:
   - 24/7 monitoring video system
   - Door sensors

2. Implementing onsite security force

Example of risk reduction measures analysis

AFTER SECURITY UPGRADE 1 (intrusion detection system)

Spillway Gate

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into chamber through D4 or D3	VH		90 s			
Get to control panel and gates	VH		120 s			
Task	VH		300 s			
Total	**VH**	**M**	**410 s**	**1665 s**	**VL**	**VL**

Notes.-
Task delay time is assessed by engineering judgement

Bottom outlet at old diversion tunnel

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through G3 or G4	VH		60 s			
Get to tunnel entrance by car (D8) = 80m	NA		5 s			
Break into tunnel through D8	VH		90 s			
Get to valve chamber = 155m	NA		9 s			
Task	VH		600 s			
Total	**VH**	**M**	**688 s**	**1665 s**	**VL**	**VL**

Notes.-
Task delay time is assessed by engineering judgement

Example of risk reduction measures analysis

AFTER SECURITY UPGRADE 2 (onsite response force)

Spillway Gate

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into chamber through D4 or D3	VH		90 s			
Get to control panel and gates	VH		120 s			
Task	VH		300 s			
Total	**VH**	**M**	**410 s**	**120 s**	**H**	**M**

Notes.-
Task delay time is assessed by engineering judgement

Bottom outlet at old diversion tunnel

International Terrorist Group Attack	Detection effectiveness	Communication reliability	Delay time (s)	Response time (s)	Response-delay time relation	System Effectiveness
Break into restricted area through G3 or G4	VH		60 s			
Get to tunnel entrance by car (D8) = 80m	NA		5 s			
Break into tunnel through D8	VH		90 s			
Get to valve chamber = 155m	NA		9 s			
Task	VH		600 s			
Total	**VH**	**M**	**688 s**	**120 s**	**H**	**M**

Notes.-
Task delay time is assessed by engineering judgement

5. Risk Management

Example of risk reduction measures analysis

Prior to any security upgrade:

Threat: international terrorist group

	P_A	$(1 - P_E)$	C	R
Damage or breach of spillway gates	M	VH	L	L
Damage or breach of outlet works	M	VH	L	L

After security upgrade 1: intrusion detection systems

	P_A	$(1 - P_E)$	C	R
Damage or breach of spillway gates	M	VH	VL	VL
Damage or breach of outlet works	M	VH	VL	VL

After security upgrade 2: onsite security force

	P_A	$(1 - P_E)$	C	R
Damage or breach of spillway gates	M	M	L	L
Damage or breach of outlet works	M	M	L	L

Conclusions:

- Dam security should be addressed on a regular basis, in a similar way as dam safety
- Security risk is difficult to quantify, especially because predicting human behavior may never be a random event in the mathematical sense
- It's important to consider all three components of risk: likelihood of attack, system ineffectiveness, and consequences
- Collaboration between Dam Owners, Intelligence Communities, and Emergency Agencies is desirable

Conclusions:

- The security risk value obtained in DAMSE is a *qualitative estimate* that must be checked considering all three components
- The methodology is a meaningful procedure that brings in benefits "along the way"
- It has practical implications, for it gives a systematic basis for security management decision making

THANK YOU SO MUCH!