

March 23-25, 2005
Stevens Institute of Technology Campus
Hoboken, New Jersey

Approach to Identify the Defense Elements within a Transport System

Alain Cointet
Paris Mass Transport System - RATP

- ✧ Goals
- ✧ Systems
- ✧ Methodology
- ✧ Example
- ✧ Conclusion



© RATP - AUDIOVISUEL

236477 - 04/09/1998

RISKS CONTROL

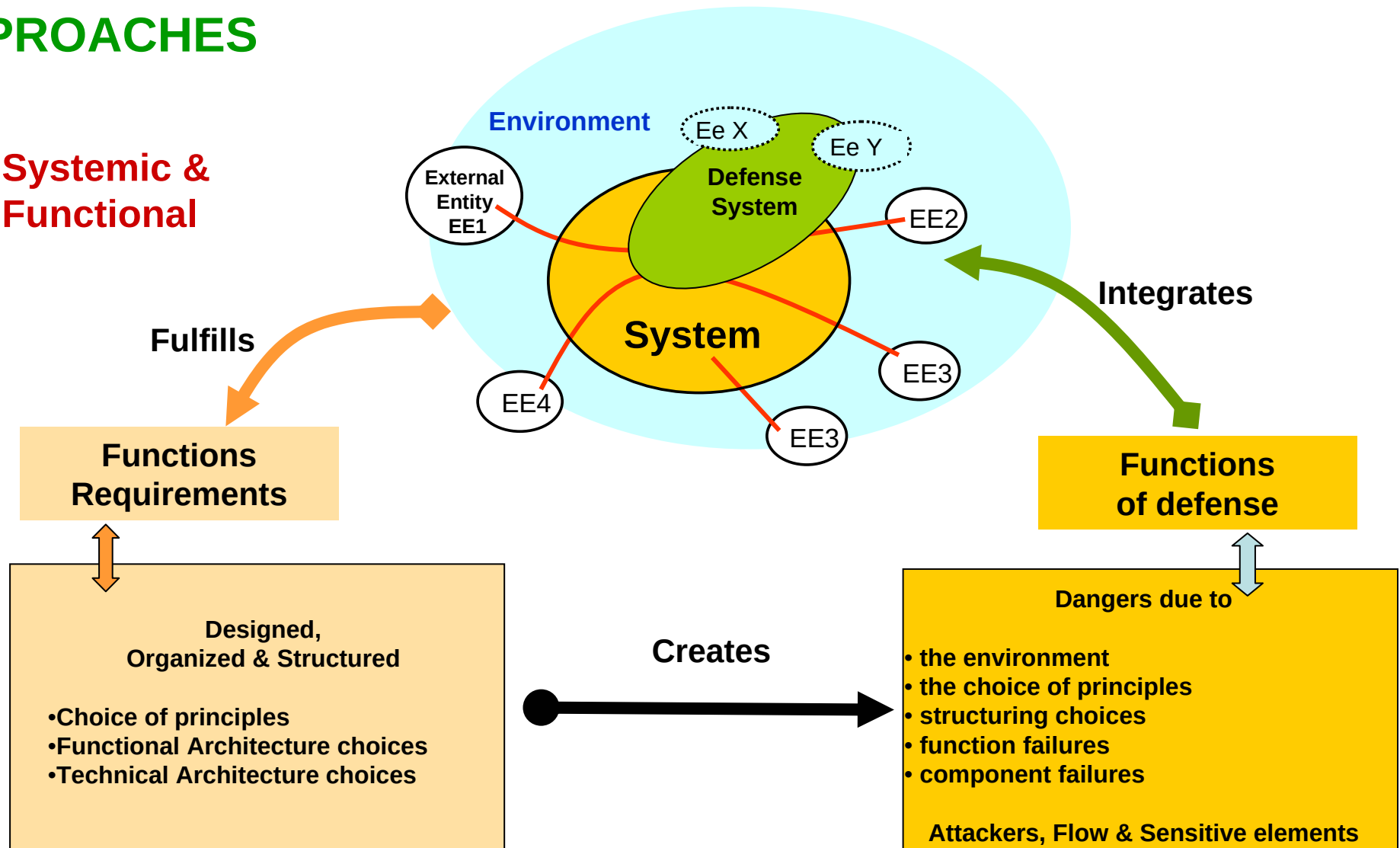
To face the complexity of a transport system,

- ❑ A **SYSTEMIC APPROACH** is essential **TO CONTROL** the **RISKS** inherent in the system by taking into account aspects such as:
 - ▶ Technology, Humans, Organization, Economy,
 - ▶ Environment (interactions & evolutions),
 - ▶ The set of life cycles of the whole system as well as of each component, operating modes and interfaces.

- ❑ A **REPRESENTATION of DEFENSE PROVISIONS (REFERENCE)** contributing to the control of risks is indispensable to obtain a clear vision of the **SAFETY LEVEL**.
 - ▶ In coherence with existing approaches,
 - ▶ Usable by security experts and decision makers.

APPROACHES

Systemic & Functional



FUNDAMENTALS

DEFENSE IN DEPTH

Defense instead of Security

- dynamic & initiative
- global approach & systemic

1

Depth

- origin of threats
- existence of several lines of defense
- phases of life & environment

2

Approach

- analysis focused on effects
- combination of inductive & deductive approaches
- gravity of incident depends more of remaining defense means than on those which were crossed

3

FINALITY & DEFINITION

□ Finality :

▶ The “**Defense-in-Depth**” is a global and dynamic defense, implementing several coordinated lines of defense, against internal and external aggressions, potential or proven - and that on all the life cycle of the transport system

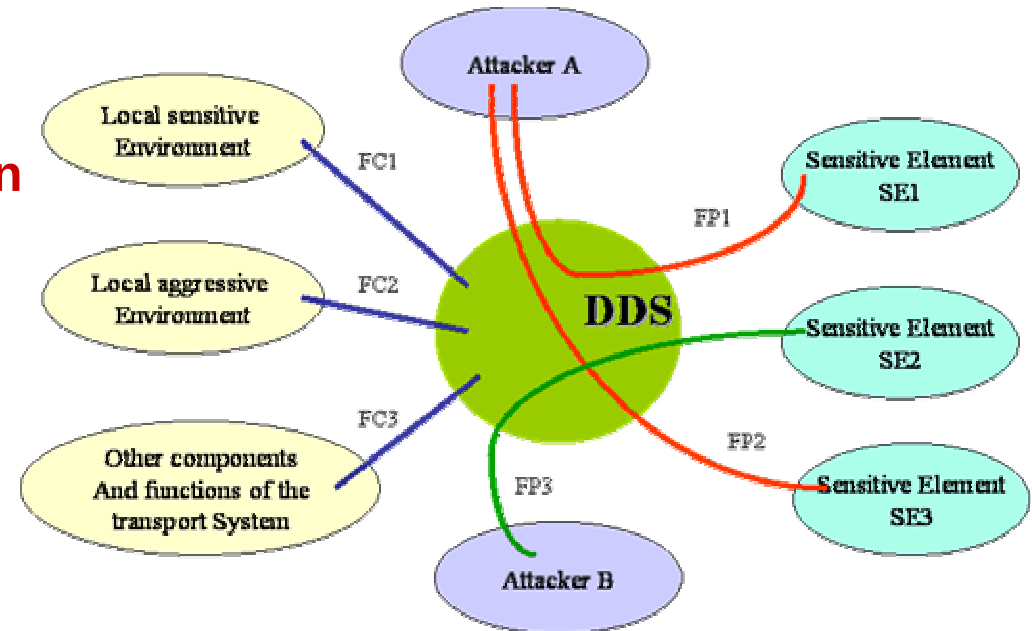
□ Definition :

▶ A “**Defense-in-Depth System**” is the set of the provisions and means organized, contributing to the control of the potential final effects susceptible to be created by all forms of aggressions on sensitive elements (men, system, company and/or environment). .

DEFENSE IN DEPTH

FUNCTIONALITIES OF DEFENSE SYSTEM

Functions of a defense system are expressed taking into consideration implied entities (sensitive element, Flow, Attacker)



Examples:

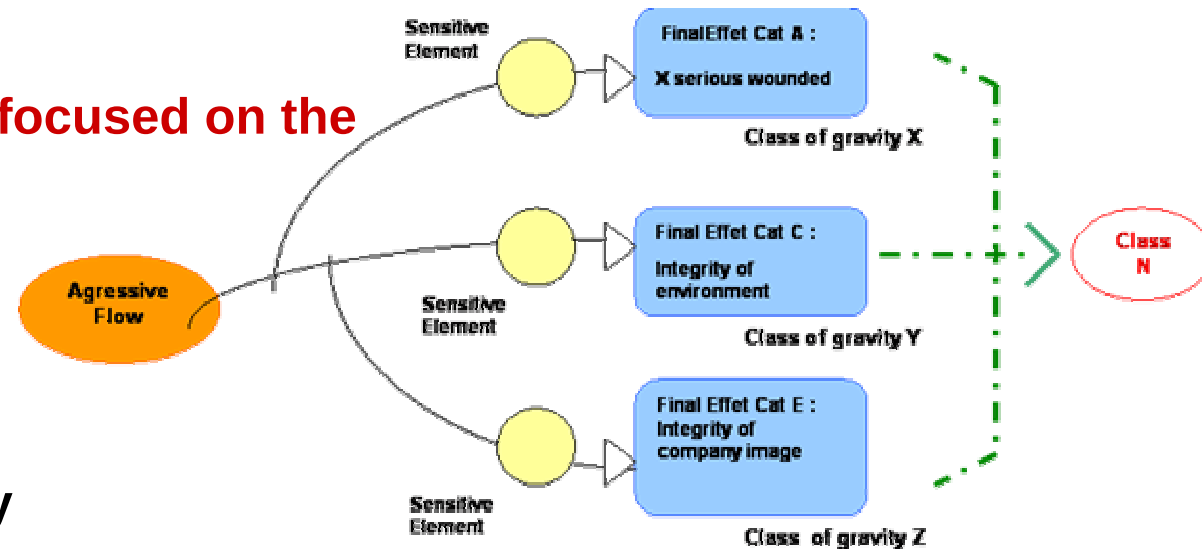
- ❑ To ensure the physical integrity of the train upstream with respect to the kinetic flow of the train downstream ,
- ❑ To ensure the physical integrity of operation and maintenance staff with respect to the kinetic flow of the convoy in motion
- ❑ To guarantee the nominal conditions of adherence of the rail with respect to the deposits of grease left by the track worksites

ACCEPTABILITY OF FINAL EFFECTS

Concept of Defense in Depth is focused on the control of final effects

DEFENSE IN DEPTH

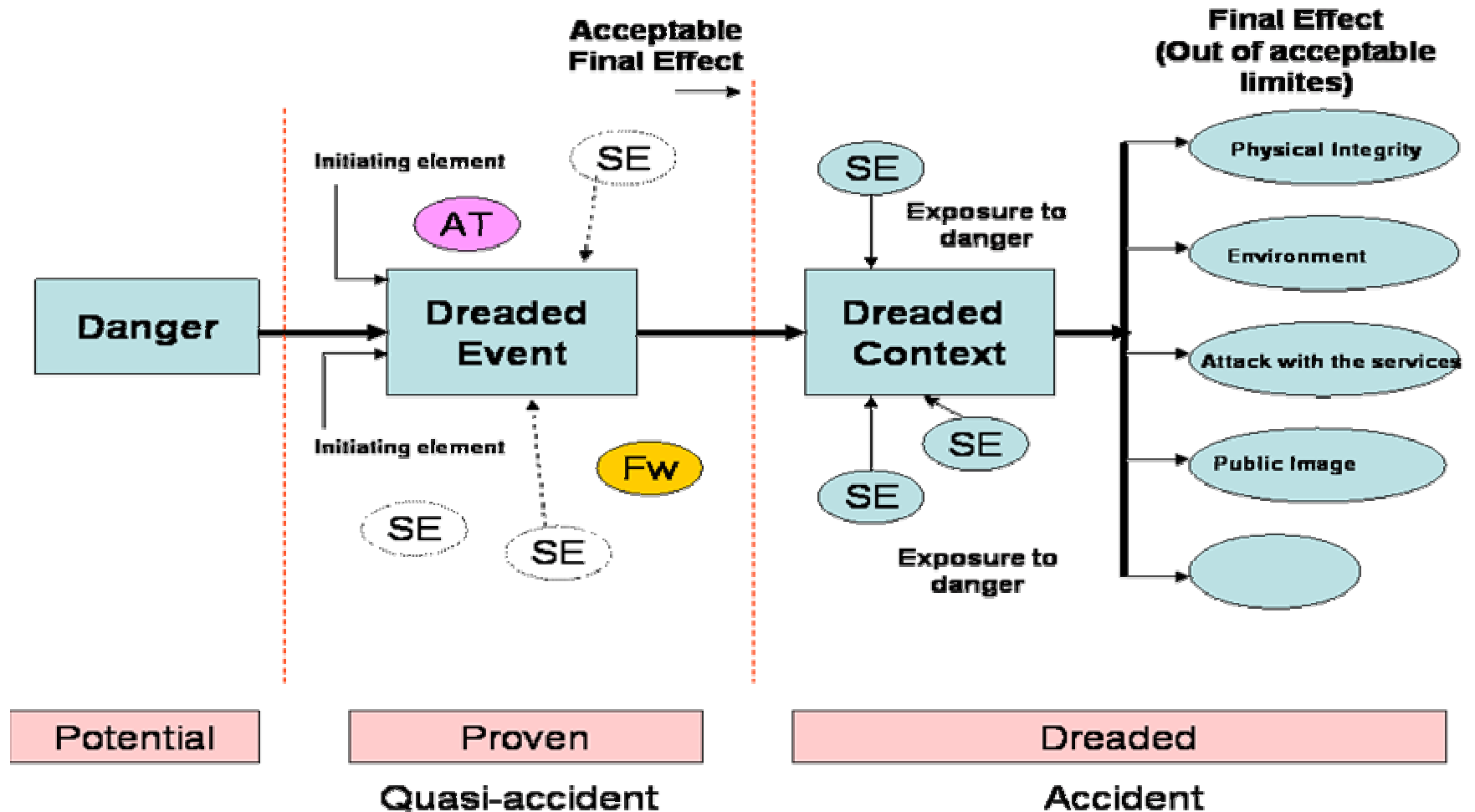
- ▶ Function of defense
- ▶ Requirements
- ▶ Level of acceptability



The determination of the final effects levels of acceptability is done in a given system of values, at a given time.

ACCEPTABLE – TOLERATED - UNACCEPTABLE

DREADED EVENT & CONTEXT



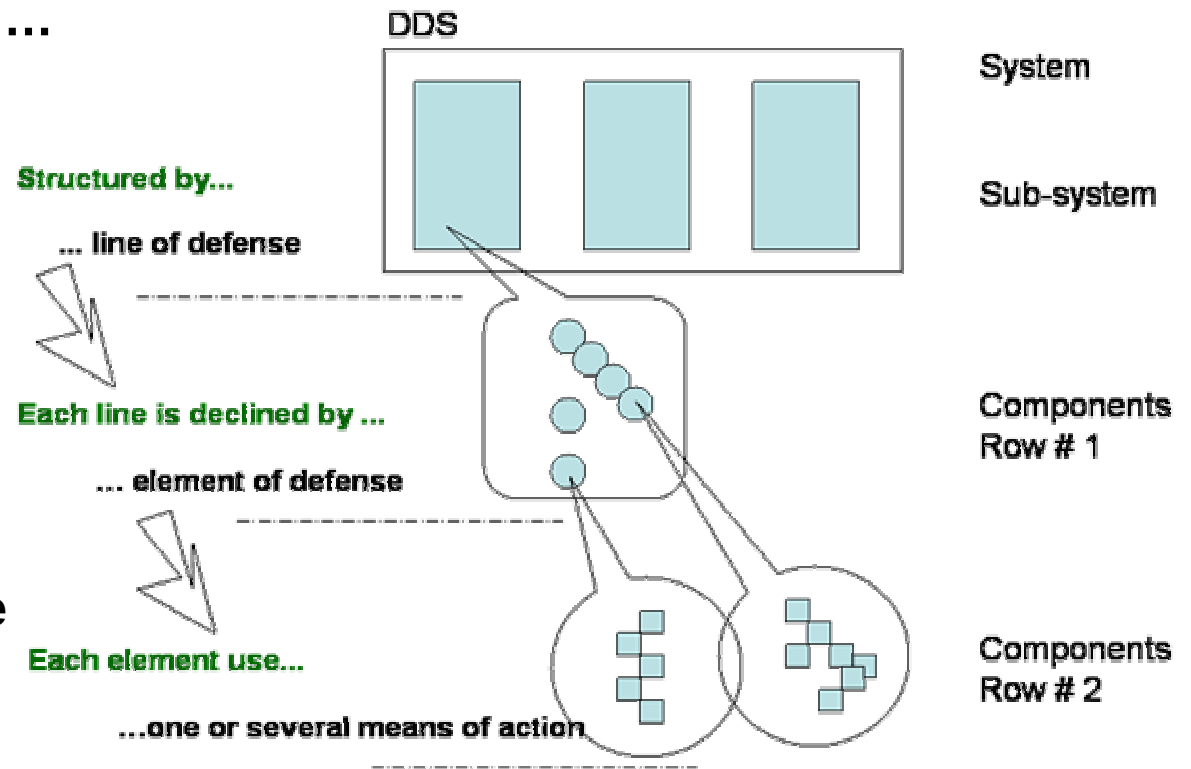
ARCHITECTURE & TYPOLOGY

The principles of architecture facilitate the systems design or the modeling of an existing system...

They provide a generic and simple framework for the development of a reference frame of defense...

BASES

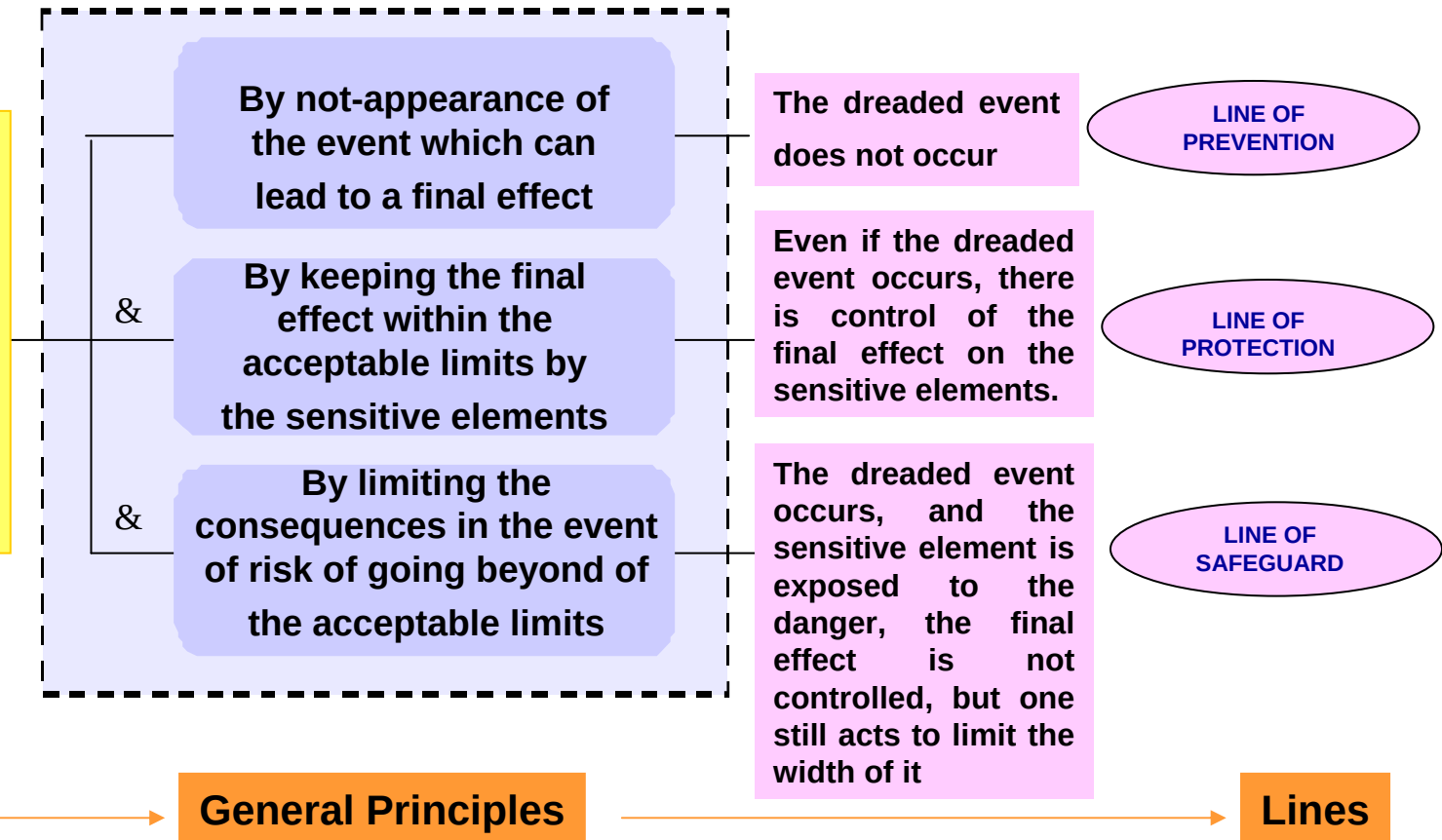
- ❑ Lines of defense,
 - ▶ finality of defense
- ❑ Principles of action
 - ▶ awaited actions
- ❑ Means of actions
 - ▶ implemented devices



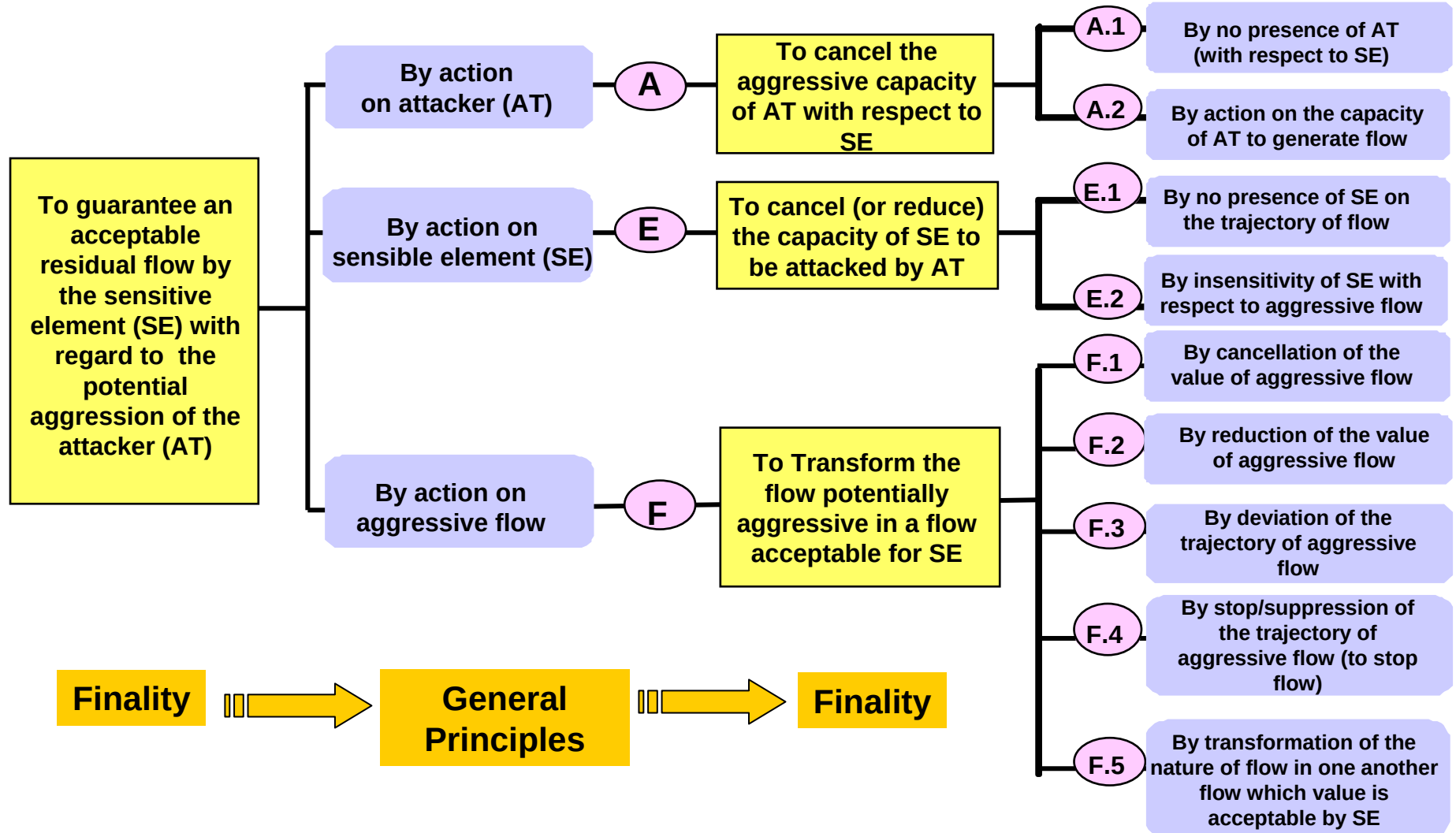
LINES OF DEFENSE

BASES

To ensure defense in depth of sensitive elements with regards to aggressions

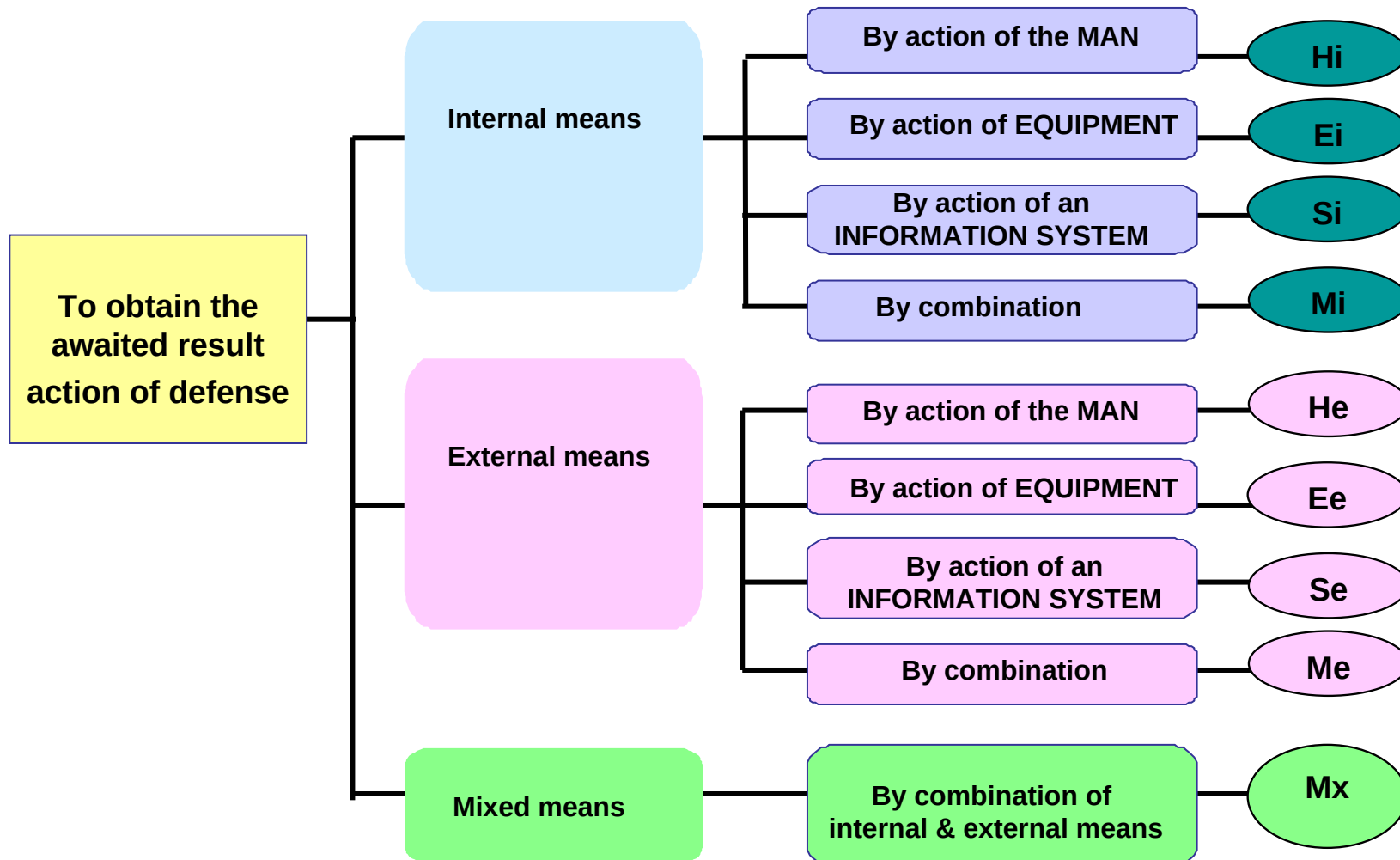


PRINCIPLES OF ACTION

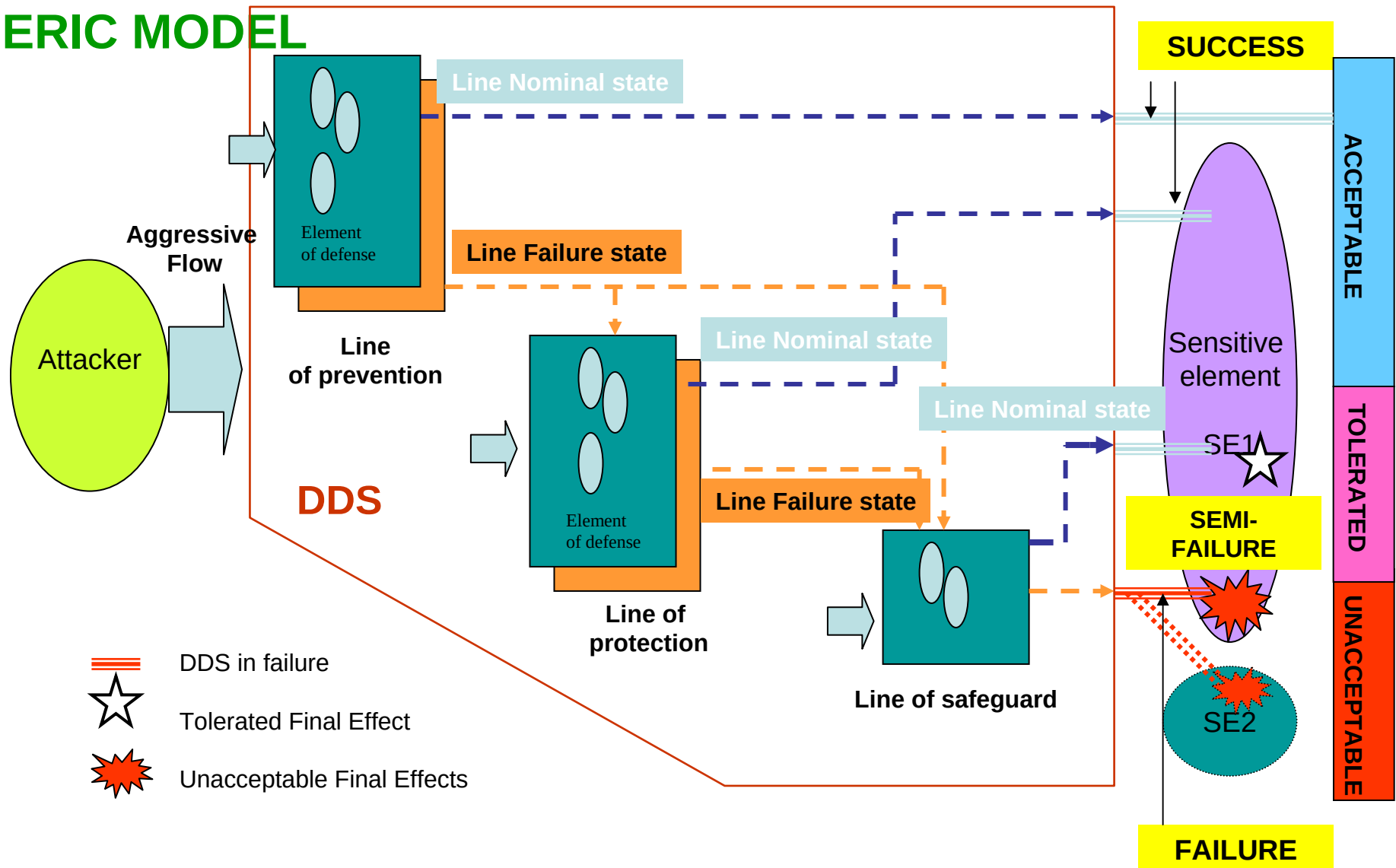


BASES

MEANS OF ACTION



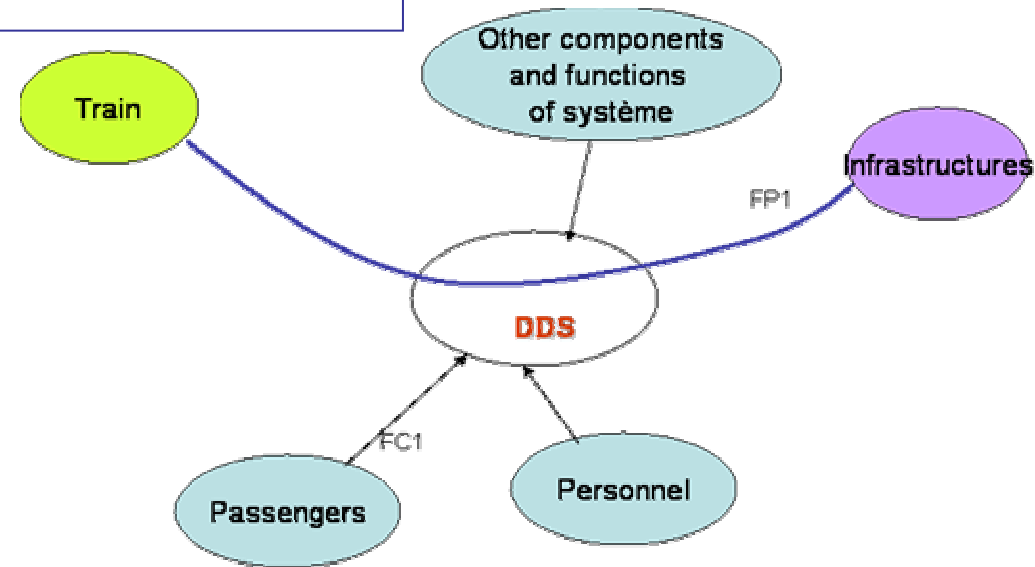
GENERIC MODEL



SPECIFICATIONS OF DEFENSE SYSTEM

In a given context...,

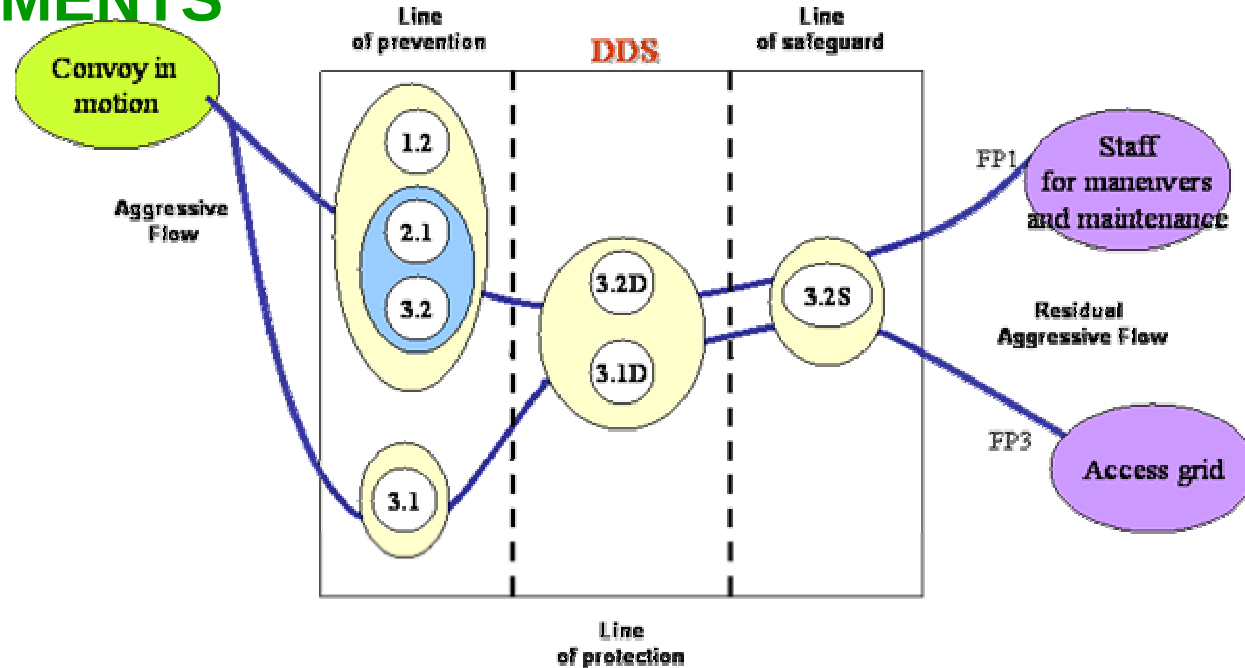
- ❑ To identify the sensitive elements,
- ❑ To identify flows (nature, characteristics, residual value),
- ❑ To identify attackers
- ❑ To formalize functions of defense



STEPS

IDENTIFICATION OF ELEMENTS

Per function of defense and,
For a given line of defense ...,



STEPS

- ❑ To identify the set of defense elements implemented within the system (according to their contexts of use and their contribution to the finality of defense),
- ❑ To identify relations of interdependence between elements of defense
- ❑ To precise principles of actions that defense element implements,
- ❑ To precise means performing awaited action of defense element

ANALYZE

**Per function of defense and,
For a given line of defense ...,**

- ☐ To establish the recommendations relating to the **INSUFFICIENCIES** of the elements of defense ,
 - ▶ To identify the insufficiencies,
 - ▶ To evaluate the corresponding risk,
 - ▶ According to acceptability level, to establish the recommendations
- ☐ To establish the recommendations relating to the **NON RESPECT** of the requirements
 - ▶ To identify the requirements which were not respected,
 - ▶ To determine the causes of these non-observances,
 - ▶ To evaluate the corresponding risk,
 - ▶ According to acceptability level, to establish the recommendations

“Palliative Measures” to be taken for the risk of loss of adherence of the trains, after the realization of work on the tracks.

FINALITY OF DDS: to guarantee the nominal conditions of adherence of the rails

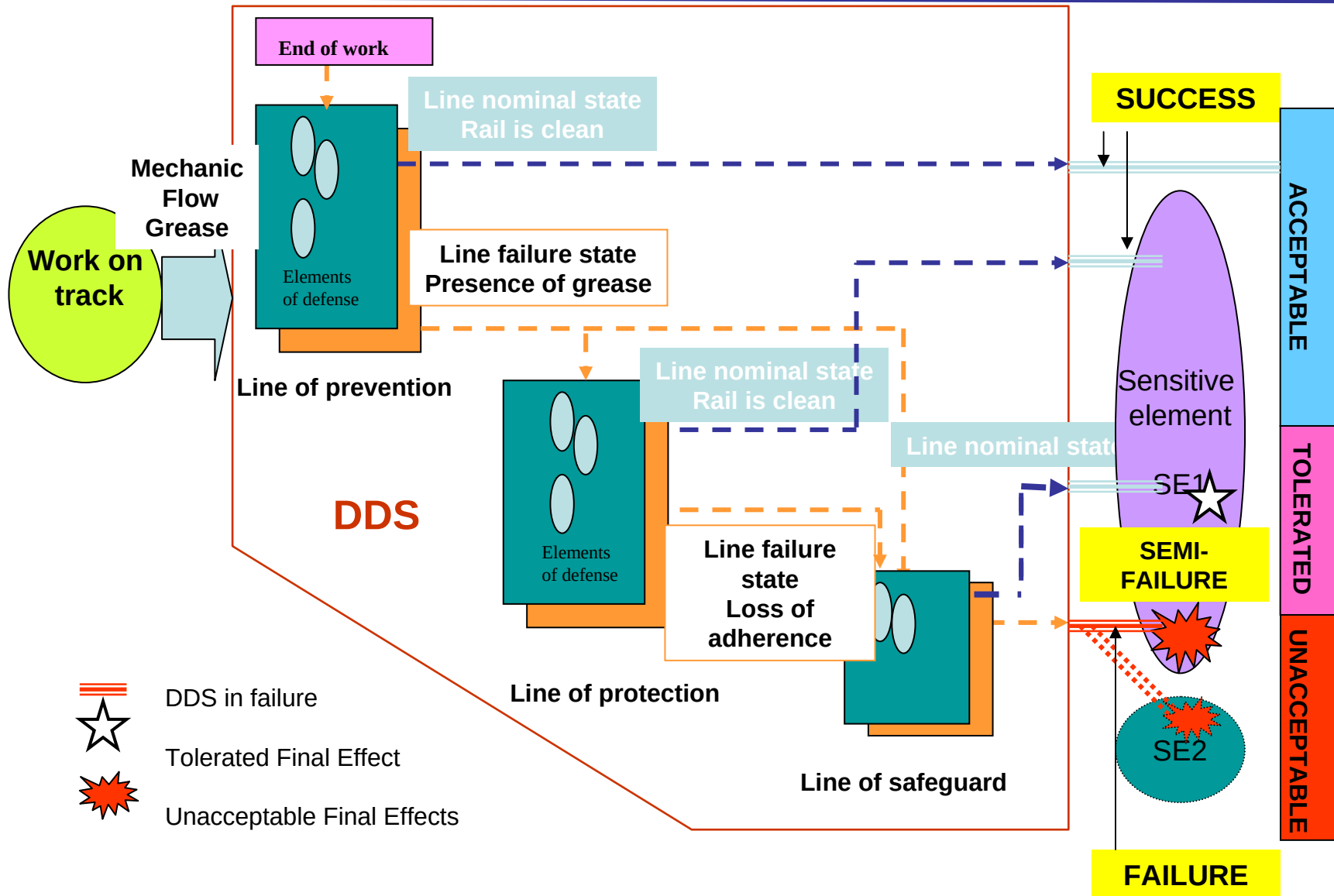
Attacker	Workers and maintenance tools for the track
Flow	Static mechanic flow (grease)
Danger	POLLUTION OF RAIL
Sensitive elements	Trains
Final effect	Change of the rail characteristics: surface quality and capacity of associated adherence
Dreaded event	Presence of grease on rails
Dreaded context	Presence of grease on rails and wheels of train Slip of a train during a braking , Skating of a train to starting

PREVENTION

PROTECTION

SAFEGUARD

Trigger	End of work	Report of presence of grease	Report of loss of adherence of a train
Principle of actions	Action on the emission of flow by the attacker	Action on the sensitivity of the element and on flow	Action by cancellation of flow
Element of defense	▶ Checking of the rails at the end of the work ▶ Cleaning before any passage of train ▶ Control following the passage of two trains	▶ Report of presence of grease by any worker (A) ▶ Alarm of the chief of regulation (B) ▶ Careful walk with all the trains (C) ▶ Urgent intervention of the track service (D)	▶ (A) Report of loss of adherence ▶ (B) Sand spreading
Dependence	Sequential	Sequential for (A) and (B) Simultaneity of (C) and (D) triggered by (B)	Sequential
Active means	Worker (rail cleaning)	(A) et (B) workers (C) Train equipment (D) Tools of track service	(A) Train driver (B) Sand



CONTRIBUTIONS & OUTLINES

Defense in Depth

Architecture

Modeling

- ☐ A concept in coherence with the systemic approach and engineering system ,
- ☐ A concept complementary to the existing steps,
- ☐ Common representation of the system of defense suggested to the various actors ,
- ☐ Synthetic representation of the system of defense suggested to the decision makers

CONTRIBUTIONS & OUTLINES

Method can be applied.....

- ☐ To analyze an incident (in complement of the experience feedback),
- ☐ To analyze a function system (guidance of the trains, distribution of energy.),
- ☐ To analyze an internal or external flow to the system (electric flow.),
- ☐ To analyze an association [Attacker, Flow, sensitive element],

To feed the reference frame of defense

But also.....

- ☐ To analyze a plan of crisis
- ☐ To analyze a guideline, an instruction, a procedure

To make sure of coherence of enacted measures (Instructions, procedures)

