EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ATCC BUILDING SYSTEM SAFETY ASSESSMENT - FUNCTIONAL HAZARD ASSESSMENT

SAF.ET1.ST03.1000.BUIL-01-00

Edition	:	1.0
Edition Date	:	28/08/2003
Status	:	Released Issue
Class	:	General Public

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT IDENTIFICATION SHEET

DOCUMENT DESCRIPTION

Document Title

ATCC BUILDING SYSTEM SAFETY ASSESSMENT -
FUNCTIONAL HAZARD ASSESSMENT

EWP DELIVERABLE REFERENCE NUMBER

PROGRAMME REFERENCE INDEX	**EDITION :**	**1.**
SAF.ET1.ST03.1000.BUIL-01-00	**EDITION DATE :**	**28/08/2003**

Abstract

This document provides guidance material on application of SAM-FHA (Safety Assessment Methodology - Functional Hazard Assessment) to ATCC (Air Traffic Control Centre) building.

Keywords

ATCC Building
Safety Objectives
Safety Assessment
FHA

CONTACT PERSON : P.MANA	**TEL :** 93295	**DIVISION :** DAP/SAF

DOCUMENT STATUS AND TYPE

STATUS		CATEGORY		CLASSIFICATION	
Working Draft	☐	Executive Task	☐	General Public	☑
Draft	☐	Specialist Task	☑	EATMP	☐
Proposed Issue	☐	Lower Layer Task	☐	Restricted	☐
Released Issue	☑				

ELECTRONIC BACKUP

INTERNAL REFERENCE NAME :

HOST SYSTEM	MEDIA	SOFTWARE(S)
Microsoft Windows	Type : Hard disk	
	Media Identification :	

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Chairman of the Safety Assessment Methodology Task Force	P.MANA	28/08/2003
Chairman of the EATMP Safety Group	E.MERCKX	28/08/2003
EATMP Project Leader	W. PHILIPP	28/08/2003

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION	DATE	REASON FOR CHANGE	SECTIONS PAGES AFFECTED
0.1	10/042003	First issue based on SOFIA CNATCC building Functional Hazard Assessment	All
1.0	28/08/2003	Update after review	All

TABLE OF CONTENTS

DOCUMENT IDENTIFICATION SHEET ..... **i**

DOCUMENT APPROVAL ..... **ii**

DOCUMENT CHANGE RECORD ..... **iii**

TABLE OF CONTENTS ..... **iv**

1. INTRODUCTION **1**

2. REFERENCE DOCUMENTS **2**

3. SCOPE OF THE ANALYSIS **3**

4. BUILDING PRESENTATION **4**

5. ORGANISATION OF THE STUDY **5**

6. SAFETY OBJECTIVES ANALYSIS **6**

6.1 Analysis Limitations **6**

6.2 Methodology **7**

6.3 Safety Objectives Setting **10**

6.3.1 Data gathered at the Building level 10

6.3.2 Data gathered at sub-systems level 10

6.3.3 Operational Environment Requirements 12

6.3.4 Quantitative Safety Objectives 12

6.3.5 Hazards table 14

6.4 Safety Objectives Specification and Synthesis **28**

6.4.1 Building and infrastructure synthesis 28

6.4.2 Sub-systems synthesis 28

6.4.3 Safety Objectives Specification 29

7. CONCLUSION **35**

1. INTRODUCTION

This document provides guidance material for identifying Safety Objectives for an ATCC Building.
These Safety Objectives are set applying EATMP SAM – FHA (Ref 3) methodology.
This Guidance Material does not specify any specific operational environment and consequently defining the specific Operational Environment in which this ATCC Building operates is a pre-requisite allowing either:

- customising some Safety Objectives (quantification) or
- delete not applicable hazards or
- add new hazards or
- modify the effects on ATCC and ATM or
- modify the worst credible effect severity.

Consequently, this Guidance Material does not provide Safety Objectives as such but proposes a basis to be assessed for its suitability to a specific project.

2. REFERENCE DOCUMENTS

Item	Reference Document	Issue	Rev.	Date
	EUROCONTROL			
1	- EATMP Safety Policy ref. SAFET1.ST01.1000.POL.01.00	2 1	0 1	08/25/99 07/15/97
2	- EATMP Safety Policy Implementation Guidance Material ref. SAF.ET1.ST01.1000.GUI.01.00	1	0	04/17/00
3	- EATMP Safety Policy : Air Navigation System Safety Assessment Methodology - FHA (ref. : SAF.ET1.ST03.1000-MAN-01-00)			
4	- ESARR4 “Risk assessment and Mitigation in ATM”	1	0	17/04/01

3. SCOPE OF THE ANALYSIS

The present document is intended to determine how safe the system needs to be for providing full and safe Air Traffic Management services.

The scope of the analysis is an ATCC building in a operational environment (which is not generic and needs to be specified for a project).

It includes the fitting and equipment of the ATCC with the human and procedural aspects of it.

The ATC Centre itself (Control Working Positions (CWP), Simulator, Radar Data Processing (RDP), Flight Data Processing (FDP), …) are out of scope as well as the structure of the building.

Determining the Safety Objectives (How safe does the system need to be?) is the outcome of the Functional Hazard Assessment process (FHA) following EATMP Safety Assessment Methodology (SAM).

It is achieved by identifying the potential failure modes and hazards. Then, the consequences on the safety aircraft operations and ATM service provision in an operational environment are assessed.

The elaboration of the Safety Objectives necessitates a description of a high level function implemented by the system. (Appendix 1)

This present document intends to identify the Safety Objectives of an ATCC.

4. BUILDING PRESENTATION

The building could be composed of the following blocks as an example:

- Block Offices;
- Block Conference room and military operating hall;
- Block Main administration offices;
- Block Training centre and civil operating hall;
- Block hotel rooms;
- Block Technical building;
- Block Sports building;
- Block Main entrance guard house;
- Block Chillers.

5. ORGANISATION OF THE STUDY

The ATCC system and the safety management group organisation are not directly analysed; they are taken into account through their interface in the different analysis.

To achieve the Safety Assessment, the following analyses shall be performed step by step:

- **A Functional Analysis (external and internal)** leading to the functional description of the Building, at the system and sub-systems level. The functional analysis approach will take into account external elements having incidence on the ATC system good running.

- **A Functional Hazard Assessment** intending to define the **Safety Objectives**. Safety Objectives are generated using results of the External Functional Analysis.

- **A Failure Modes, Effects and Criticality Analysis (FMECA)**

  The FMECA is performed using the design and the technical elements of the studied system.

  Using the Internal Functional Analysis results, the approach consists in defining the failure modes (loss or degradation of a function) and in analysing the possible failure causes.

  For each failure cause identified, their consequences will be analysed. The criticality of each failure will be classified using the cause and consequence associated.

  Actions in risks reduction will be proposed for failures having a high criticality level.

- **A failure tree for critical hazard events.** It will identify the elements involved in the chain of events that generate hazards.

- **A functional analysis of risks** in using results of the different previous analyses (i.e. a risk identification). A risk is the combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.).

  This step will allow to elaborate, to organise, to classify the identified risks, to evaluate the safety documentation, to make recommendations upon management procedures.

The present document addresses the second step: Functional Hazard Assessment.

6. SAFETY OBJECTIVES ANALYSIS

The Safety Objectives analysis is performed in accordance with the EATMP document (see item 3). The way the methodology is applied in the framework of a Building ATCC project is presented hereafter (cf. § 6.2).

6.1 Analysis Limitations

Safety Objectives intends to set a tolerable level of safety to operate the overall ATCC system which hosts an ATM system (1), based on ATC system (2) operations and a global ground system (3).

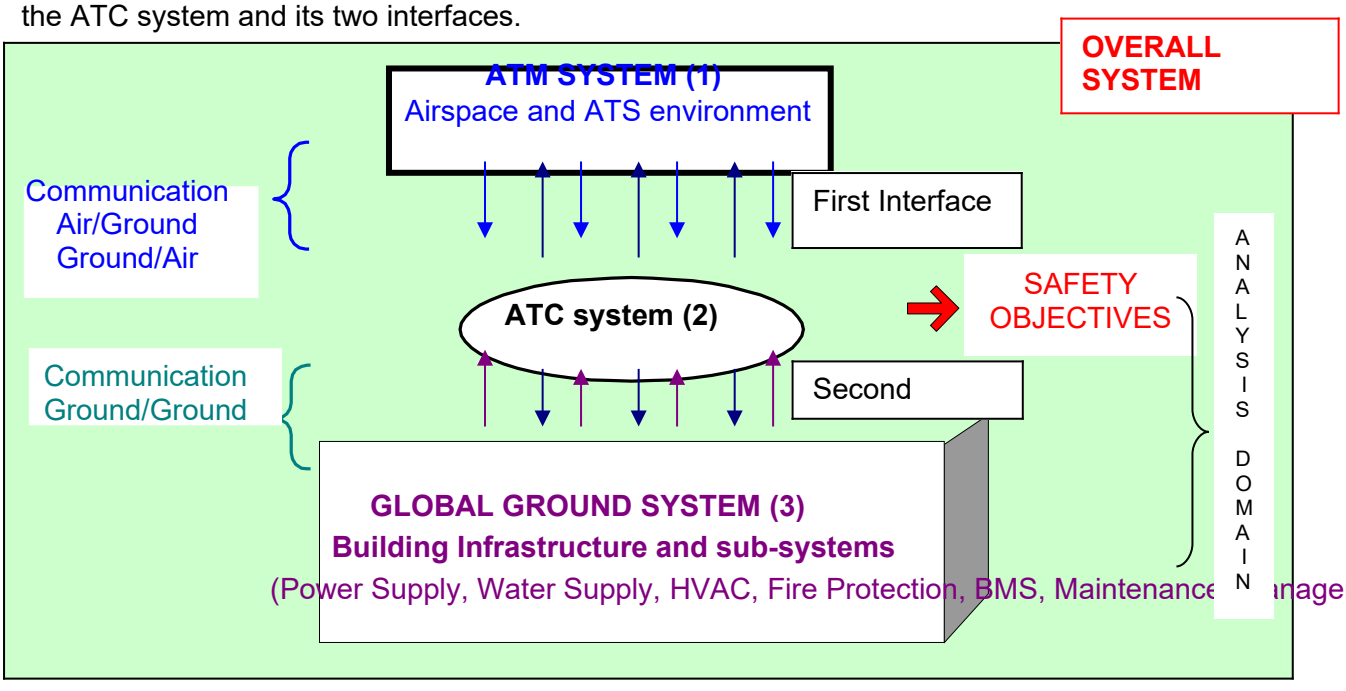
The building infrastructure hosts the Operational Room and is supplied with the following sub-systems:

- PS (Power Supply),
- HVAC (Heating Ventilation and Air Conditioning),
- FP (Fire Protection),
- WS (Water Supply) and
- BMS (Building Management System).

The following interfaces will be assessed when setting the safety objectives:

1. The interface between the ATC system and the ATM system. As ATM service provision is not only made of ATCC equipment, procedure and human elements, it can affect the operational effects of building failures and failure modes on ATM service provision.
2. The interface between the ATC system and the global ground system. The ATCC robustness (ability to be fault-resistant or fault-tolerant to external events) has to be defined through some safety objectives.

The following scheme defined the overall operational system in its environment and shows the ATC system and its two interfaces.



In the present case with respect to the operational environment in which the ATC system operates, the two functional domains are entirely defined by:

1. The ATM system;
2. The global ground system with respect to the operational objective: to maintain safe ATC activities during the time required transferring them to an another FIR.

Safety Objectives are elaborated at the ATC system level and take into account the building infrastructure, its five sub-systems (Power supply, HVAC, Water supply, Fire protection, Building Management System), the maintenance and the management.

6.2 Methodology

Safety Objectives are defined by developing the following steps in accordance with EATMP SAM (see item 3, Safety Assessment Methodology) :

1. **a functional description** of the building infrastructure and its sub-systems (definition of main and secondary functions).

   The first step (FHA initiation step) intends to provide a high level definition of the system, which includes all information required to perform a FHA.

   The FHA initiation objective is achieved by performing the External Functional Analysis.

2. **an identification of hazards** at the scope level, which can lead to a loss or a degradation of the sub-system,
3. **a description of effect**s on operation at the ATCC system level considering the worst credible case,
4. **a description of effects** on the ATM services including aircraft operations while considering the worst credible case,
5. **an assessment of the severity** regarding the potential unsafe conditions of operation according to the effects on operations (column 4) and hazard description (Cf table hereafter)
6. **a specification of the Safety Objectives** in accordance with the severity of the effect of the hazard.

The severity is assessed using the EATMP SAM table hereafter:

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
Effects on Operations	**Accidents**	**Serious Incidents**	**Major Incidents**	**Significant Incidents**	**No Safety Effect**
SEVERITY INDICATORS SET1: EFFECTS ON AIR NAVIGATION SERVICE					
Effect on Air Navigation Service within the area of responsibility	Total inability to provide or maintain safe service	Serious inability to safe provide or maintain service	Partial inability to provide or maintain safe service	Ability to provide or maintain safe but degraded service	No safety effect on service
ATCO and/or Flight Crew Working Conditions	Workload, stress or working conditions are such that they cannot perform their tasks at all	Workload, stress or working conditions are such that they are unable to perform their tasks effectively	Workload, stress or working conditions such that their ability is significantly impaired	Workload, stress or working conditions are such that their abilities are slightly impaired	No effect
ATCO and/or Flight Crew Ability to Cope with Adverse Operational and Environmental Conditions	Unable to cope with adverse operational and environmental conditions	Large reduction of the ability to cope with adverse operational and environmental conditions	Significant reduction of the ability to cope with adverse operational and environmental conditions	Slight reduction of the ability to cope with adverse operational and environmental conditions	No effect
SEVERITY INDICATORS SET 2: EXPOSURE					
Exposure time	The presence of the hazard is almost permanent. Reduction of safety margins persists even after recovering from the immediate problem.	Hazard may persist for a substantial period of time	Hazard may persist for a moderate period of time.	Hazard presence is such that no significant consequences are expected.	Too brief to have any safety-related effect
Number of aircraft exposed	All aircraft in the area of responsibility	All aircraft in several ATC Sectors	Aircraft within a small geographic area or an area of low traffic density	Single aircraft	No aircraft affected
Likelihood to experience adverse operational and environmental conditions	Frequent to permanent presence of the considered adverse operational and environmental conditions	Relatively high likelihood to experience the considered adverse operational and environmental conditions	Slight likelihood to experience the considered adverse operational and environmental conditions	Low likelihood to experience the considered adverse operational and environmental conditions	Rare presence of the considered adverse operational and environmental conditions

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
SEVERITY INDICATORS SET 3: RECOVERY					
Annunciation, Detection and Diagnosis	Misleading indication. Hard to detect or diagnose. Diagnosis very likely to be incorrect	Ambiguous indication. Not easily detected. Incorrect diagnosis likely	May require some interpretation. Detectable. Incorrect diagnosis possible	Clear annunciation. Easily detected, reliable diagnosis	Clear annunciation. Easily detected and very reliable diagnosis
Contingency measures (other systems or procedures) available	No existing contingency measures available. Operators unprepared, limited ability to intervene.	Limited contingency measures, providing only partial replacement functionality. Operators not familiar with procedures or may need to devise a new procedure at the time.	Contingency measures available, providing most of required functionality. Fall back equipment usually reliable. Operator intervention required, but a practised procedure within the scope of normal training	Reliable, automatic, comprehensive contingency measures	Highly reliable, automatic, comprehensive contingency measures
Rate of development of the hazardous condition, compared to the time necessary for annunciation, detection, diagnosis and application of contingency measures	Sudden. It does not allow recovery	Faster	Similar	Slower	Much slower. Plenty of time available

6.3 Safety Objectives Setting

Safety Objectives are elaborated using the output of the External Functional Analysis of the building infrastructure and sub-systems (mains and secondary functions see annex 2).

Following the External Functional Analysis, the analysis approach is split into two parts:

- the Building infrastructure and
- the 5 sub-systems,

6.3.1 Data gathered at the Building level

The two main functions of the Building are the following one:

F_{P1}	To protect equipment/environment users
F_{P2}	To ensure a back-up to elements necessary for users' comfort and equipment running/ATC

The following external events (able to generate building malfunction) have been considered:

- Extreme climatic conditions: high or low temperature, hailstorm, snow, storm, flood…
- Earthquake
- Irradiation
- Vibration
- External noise
- Air pollution
- External fire

Note: Terrorism/intrusion inside the site and outside by switching off the power or turning off the public network water will not be considered within that safety analysis as only unintended malfunction is considered. Anyhow it is recommended to complement that safety analysis with a security analysis (some security recommendations will be raised hereafter in this document when identified as necessary)

6.3.2 Data gathered at sub-systems level

Each sub-system has been studied in its environment (inside the Building). The main and secondary functions of each sub-system are the following one:

POWER SUPPLY

F_{P1}	To continuously supply with electricity the ATC system, technical equipment and rooms
F_{S1}	To detect any breakdowns or failures on the electrical network in order to inform the surveillance system (BMS) which will take the appropriate measures

WATER SUPPLY

F_{P1}	To provide users with drinking water inside the buildings
F_{P2}	To provide water to the indoor and outdoor building process.
F_{S1}	To detect any failures on the water supply network

HVAC

F_{P1}	To ventilate premises and equipment
F_{S1}	To extract smoke in the zone in which a fire has been detected
F_{S2}	To detect any failures in the HVAC sub-system

FIRE PROTECTION

F_{P1}	To prevent fire risks
F_{P2}	To detect a fire starting point
F_{P3}	To protect the ATC equipment and users when a fire has been detected
F_{S1}	To detect any failures on the Fire Protection sub-system

BMS

F_{P1}	To monitor status of the key parameters of each sub-system
F_{P2}	To control the operations of each sub-system

A partial or a total loss of sub-system functions could be due to:

- External event (see §6.3.1),
- Failure of a function of the sub-system (fire, noise, human error, equipment failure…),
- A partial or a total loss of another sub-system if links exist between sub-systems.

Each secondary function mainly performs monitoring and is taken into account at the BMS level (partial or total loss of the BMS main function).

6.3.3 Operational Environment Requirements

As a result of discussions with operations management, it should be decided that maintaining ATC operations within the building during a minimum of X minutes shall be considered as an operational requirement driving safety objective specification.

This value of X minutes has to be assessed and approved by the ATMSP taking into consideration airspace characteristics. As the worst credible case could lead to the inability to provide ATC operations and services, this X minutes duration intends to allow to:

- Detect a failure;
- Diagnose;
- Evacuate non-operational staff;
- Derive safely all traffic (either en-route or TMA (Terminal Manoeuvre Area));
- Evacuate ATC operational staff.

6.3.4 Quantitative Safety Objectives

Safety Objectives can be specified either qualitatively (See table hereafter) or quantitatively.

Likelihood classes	Similar technology used in similar conditions	**Emerging technology and/or used in other conditions**
Extremely Rare	No failure has been detected	All conditions are joined to guarantee the lack of failure The technology is controlled
Rare	Remotely failures appear	Not all conditions are joined to guarantee the lack of failure. The technology is controlled
Occasional	The experience shows that a lot of problems appear	Nothing to prevent failure from appearing The technology is controlled
Likely	The experience shows that repetitive failures always appear	Nothing to prevent failure from appearing The technology is not controlled

The following Safety Objective Classification Scheme is used:

Severity Class	**Maximum Tolerable Likelihood of Occurrence**
1	Extremely rare
2	Rare
3	Occasional
4	Likely
5	None

Quantitative likelihood classes are based on the following criteria:

- First a TLS (Target Level of Safety) has to be set for the ATCC system
- Then this TLS has to be derived to set quantitative safety objective per severity class for each single hazard
- For Severity Class 1, ESARR4 sets a TLS (Target Level of Safety) for the overall ATM direct contribution to accident of $1.55x10^{-8}$ per flight-hour
- The approximate air traffic volume in the airspace in year 2000 was of Y flight-hours (+/- 10%).
- ESARR4 traffic evolution was considered (+6.7 % per year till 2015)
- A conservative approach was to consider 2015 TLS (as required by ESARR4) as applicable to the ATCC design as the building is supposed to be operated at that time.
- A conservative approach was to allocate entirely ATMSP TLS to ATCC Building, as no mitigation means were considered as acceptable (so the tolerable frequency of occurrence of the effect is fully allocated to the safety objective of the hazard).
- An order of magnitude of 1 has been considered for severity classes 2 and 3 and of 2 for severity class 4 (as it seems to be a domain characteristic to have a lot of low severity events). Order of magnitude 2 means 10^{-2}, order of magnitude 1 means 10^{-1}
- A maximum of 10 (ten) hazards having an end effect severity of Class 1 can be identified (this analysis has found 8)
- The quantitative safety objectives unit will be per operational hour.

Consequently, the TLS for the ATMSP is: TDB

From this TLS, quantitative Safety Objectives can be derived **per hazard** having an effect whose worst credible severity is (effect tolerable occurrence equals safety objective of the hazard by conservative approach):

- For Severity Class 1: ST1 (TBD)
- For Severity Class 2: ST2 (TBD)
- For Severity Class 3: ST3 (TBD)
- For Severity Class 4: ST4 (TBD)

In case of quantitative approach, the following likelihood classes definition is used:

Likelihood classes	Quantitative	Meaning
Extremely Rare	SO1	Shall never happen during the building operational lifetime
Rare	SO2	As approximately 10 of such safety objectives have been identified, it means that one single event (severity 2) is tolerated to occur once during the building operational lifetime
Occasional	SO3	As approximately 10 of such safety objectives have been identified, it means that one single event (severity 3) is tolerated to occur once every TBD.
Likely	SO4	As approximately 10 of such safety objectives have been identified, it means that it can happen that one single event (severity 4) is tolerated to occur once TBD.

6.3.5 Hazards table

The format of tables used to present results is given in annex 3. Columns are presented hereafter:

Column 1	definition of the reference of the element (building or sub-system) studied associated to its iteration
Column 2	name of the element and designation on which the failure is applied
Column 3	Identification of hazards (main or secondary function) associated to the element studied
Column 4	Description of the effect at the ATCC system level
Column 5	Description of effect of hazard at the ATM services level due to consequences on the ATCC system upon the occurrence of hazard associated to the element studied
Column 6	Assessment of the severity regarding the end effect of the hazard (ATM service provision and/or end user) (see severity indicators)
Column 7	**Comments/Remarks**

Tables are provided hereafter for each element of the system. Elements are presented following the External Functional Analysis:

List of elements	Abbreviation used in the table
Building	**BU**
Power Supply sub-system	**PS**
Water Supply sub-system	**WASU**
HVAC sub-system	**HVAC**
Fire Protection sub-system	**FIRE**
BMS sub-system	**BMS**

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BU_1	Building ATC rooms	**Total loss of ATC rooms** due to object collision (aircraft, meteorite, vehicle…), severe damage of building	Immediate evacuation of personnel. No way to operate	Total inability to provide or maintain safe ATM services. Loss of the service.	1	Event so unlikely to happen. It has been decided to do nothing to avoid or to mitigate this hazard (sometimes nothing can be done). This risk is classified as acceptable by management.
H-BU_2	Building ATC rooms	**Total loss of ATC rooms** due to weather conditions (earthquake, tornado, lightning, wind, snow, flooding ….) leading to evacuate the personnel of the building, severe damage of building	Immediate evacuation of the personnel No way to operate	Total inability to provide or maintain safe ATM services. Loss of the service.	1	Building structure shall be designed to fulfil the standards in force with respect to : - earthquake - tornado - lightning - wind speed - snow - flood
H-BU_3	Building ATC rooms	**Total loss of ATC rooms** due to hostile action (terrorism, alert, bomb….) leading to evacuate the personnel of the building	Immediate evacuation of the building. No way to operate	Total inability to provide or maintain safe ATM services Loss of the service	1	Aspect out of scope of this safety analysis. However a Security policy on site shall be defined (prevention of intrusion at strategic points : PS facilities, BMS office, operational room…)
H-BU_4	Building	**Total loss of ATC rooms** due to chemical		Total inability to operate	1	Building environment shall be taken into account to prevent

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
	ATC rooms	pollution, leading to loss of the staff	No way to operate	safe ATM services. Sudden or unexpected interruption of ATM services.		chemical pollution.
H-BU_5	Building ATC rooms	**Total loss of ATC rooms** due to pollution (exterior fire smoke**)** leading to evacuate the staff	Unexpected evacuation of staff. Workload increased (degradation of nominal consoles configuration)	Partial inability to provide or maintain safe ATM services. Degradation of service provided	3	Building shall be designed to dissipate or extract smoke for guarantee ATC operations during X minutes
H-BU_6	Building ATC rooms	**Total loss of ATC rooms** due to electromagnetic irradiation	Workload increased (sudden failure of consoles, possible loss of information)	Partial inability to provide or maintain safe ATM services. Degradation of service provided	2	Building design shall be defined to prevent against electromagnetic irradiation (from inside and outside) Level shall not exceed (TBD) with respect to ATC system equipment
H-BU_7	Building ATC rooms	**Total loss of ATC rooms** due to : - switch off of the Power Supply public network (failure) - strike of the Power Supply public network	No way to operate	Total inability to safe provide or maintain ATM services	1	Building backup System shall be designed to provide sufficient PS to the ATC rooms. Minimum level of PS backup mode shall be (TBD in non / short break) to maintain safe services in any case of circumstances. Duration of the PS backup mode shall be TBD.

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BU_8	Building ATC rooms	**Partial loss of ATC operations due to noise**	Workload increased (evacuation of staff could be)	Ability to provide or maintain safe ATM services. Decrease of the service	4	Building shall be designed against noise. Noise level shall not exceed (TBD) during a time not greater than (TBD) at CWP.
H-BU_9	Building ATC data communicati on	**Total loss of ATC data** (voice, radar, network, phone, meteorology, others FIR's)	No information to operate	Total inability to communicate and to provide safe ATM services.	1	Data and systems communication shall be designed accordingly
H-BU_10	Building ATC rooms	**Partial loss of ATC rooms** due to earthquake, vibration…, leading to a degradation of the building facilities	No way to operate nominally. Workload increased Evacuation of building	Ability to provide or maintain safe ATM services. Possible non permanent interruption of the service Degradation of service	3	The ATC system information /data shall be transferable.
H-BU_11	Building ATC rooms	**DEGRADED CONDITIONS IN ATC ROOMS** DUE TO : - turning off the potable Water Supply public network - strike of the Water Supply public network	No direct effect Discomfort of users	Total ability to provide or maintain safe ATM services.	5	Building backup system of WS shall be defined to function independently during many days (TBD) covering operators needs.

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BU-12	Building ATC rooms	**Degraded conditions for ATC rooms** due to fire personnel or emergency personnel (unavailability)	No direct effect Discomfort of users	Ability to provide or maintain safe ATM services.	4	Fire Emergency Policy shall be defined on site

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-PS_1	Power Supply ATC rooms	**Total loss of power supply** due to : - water, fire, flood, earthquake, lightning, - equipment failures (wiring damages..)	No way to operate ATC system or sub-system (lighting of operation room and escape routes, BMS, HVAC, FP & WS)	Sudden loss of ATM services Total inability to provide or maintain safe ATM services	1	PS backup shall be designed to provide a minimum PS level (TBD in degraded mode) according to the operational time (X minutes)
H-PS_2	Power Supply ATC rooms	**Partial loss of power supply** due to : - water, fire, flood, earthquake, lightning - equipment failures (wiring damages …) - micro breakdown **operational room lighting is affected**	Workload increased (degraded consoles configuration) Discomfort of users Possible inability to light escape routes Possible inability to supply other sub-systems	Serious inability to safe provide or maintain degraded ATM services (decreasing services)	2	The loss of nominal power supply shall not exceed a time (TBD). Escape route lighting shall be operational in continuous during a times TBD.
		operational room lighting is not affected	Workload increased Possible inability to light escape routes Possible inability to supply other sub-systems		3	Minimum level of lighting shall be defined (TBD) with respect to operators at CWP.

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-WASU_1	Water Supply ATC rooms	**Total loss of the Water Supply functions**: Loss of the drinking and non-drinking (technical used) water supplies due to: - equipment or internal WS network failures - partial loss of PS - fire, earthquake	No direct effect Discomfort for the users Water unavailable in the case of fire start-up, workload increased and possible degradation of the nominal configuration of consoles (possible loss of the HVAC cooling ..)	Possible slight decrease of the service Partial inability to safe maintain ATM services (could be)	4 3	Minimum level of Water Supply shall be defined (TBD, degraded mode) to secure keys elements of ATC system.
H-WASU_2	Water Supply ATC rooms	**Partial loss of the Water Supply functions:** Loss of the drinking water due to: - equipment or internal WS network failures - partial loss of PS - fire, earthquake - internal WS network pollution	Discomfort of the users. No direct effects	Total ability to provide and maintain safe ATM services	5	

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-HVAC_1	HVAC	**Total loss of HVAC: loss of the consoles ventilation, rooms ventilation, smokes extraction due to:** - fire - partial loss of PS - earthquake - Equipment or network failure	Direct effects Discomfort of the users (loss room ventilation) Workload increased (degradation of nominal configuration of consoles)	Possible Serious inability to safe provide or maintain ATM services Possible slight decrease of the service	2	Minimum level (degraded mode) of HVAC shall be defined (TBD) for : - the operation - the equipment
H-HVAC_2	HVAC	**Partial loss of HVAC functions : loss of the consoles ventilation due to :** - partial loss of PS - equipment or network failures - fire, earthquake	Discomfort of users Workload increased (degradation of the nominal consoles configuration could be)	Partial inability to provide or maintain safe ATM services. Possible slight decrease of the service	3	Minimum level of console ventilation shall be maintained during a time TBD in strategic places.
H-HVAC_3	HVAC	**Partial loss of HVAC functions : loss of the smokes extraction (in the ATC rooms and the escapes way) due to :** - partial loss of Fire Detection - partial loss of PS - equipment failures - Fire, earthquake,	No direct effect	Ability to provide or maintain safe ATM services.	4	Minimum level of smoke extraction shall be maintained during a time TBD in strategic places

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-FIRE_1	Fire Protection ATC rooms	**Total loss of fire Protection functions : loss of Fire Prevention, fire detection, users and equipment protection** due to: - partial loss of PS - earthquake - materials degradation - partial loss of the BMS	No direct effect No detection of fire start-up, discomfort of operators	Possible serious inability to provide or maintain safe ATM services	5 2	Fire protection shall be designed with a minimum level (degraded mode) for : - Fire Prevention (TBD) - Fire detection (TBD) - Fire Protection (TBD) to protect users, rooms, equipment in strategic places.
H-FIRE_2	Fire Protection ATC rooms	**Partial loss of the Fire Protection functions: loss of the fire prevention** (included **equipment protection)** due to: - materials degradation or equipment failure or degradation of protection means - earthquake	No direct effect No prevention of fire start-up, discomfort of users	Possible serious inability to provide or maintain safe ATM services	5 2	Minimum level of fire prevention shall be maintained during operational time (X') in strategic places / keys elements.
H-FIRE_3	Fire Protection ATC rooms	**Partial loss of the Fire Protection functions : loss of the fire detection** due to: - partial loss of PS - partial loss of the BMS - equipment failure - earthquake	No direct effect. No detection of fire start-up and possible propagation, immediate evacuation of users Discomfort of users	Possible serious inability to provide or maintain safe ATM services	5 2	Minimum level of fire detection shall be maintained during operational time (X') in strategic places/ keys elements

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BMS_1	BMS Office	**Total loss of the BMS office** due to : - fire - flood altering network - network out of order (section cut-off) leading to an inability to supervise, monitor and to control the equipment of the sub-systems.	No direct effects No detection of an intrusion or a potential dysfunction/loss of sub-systems Safety and evacuation of the BMS staff.	No direct effects on service. Possible serious inability to safe provide or maintain ATM services (could be)	5 2	Security policy shall be defined to prevent intrusion in site and at strategic places. BMS location shall be analysed with respect to fire and environment. BMS network shall be designed with respect to other sub-systems network (WS, FP, HVAC, PS) to avoid crossings or proximity environment damage. BMS commands of keys elements shall be performed from different places.
H-BMS_2	BMS Office	**Total loss of the BMS office** due to: - partial loss of PS acting on BMS room	No direct effect No detection of a potential dysfunction/loss of sub-systems. Workload of BMS staff increased	No direct effect on service. Partial inability to provide or maintain safe ATM services Loss of service if loss of PS sub-system. Degradation of service if loss of HVAC sub-system	5 3	BMS shall be supplied by a minimum level of Power Supply (degraded mode-TBD) in case of emergency BMS shall be supplied by a minimum level of HVAC (degraded mode-TBD) in case of emergency (depending on sub-system architecture)

Hazard REF	Function	Hazard	ATCC effect	ATM effect	Severity	Comments/Remarks
H-BMS_3	BMS Control function	**Partial loss of the BMS** due to a loss of control functions (sub-systems elements failures, server failure, control station failures, loss of monitor functions..).	No direct effects No control functions available to stop or restart the equipment. or actuated elements incriminated.	No direct impact on the service. Possible partial inability to provide or maintain safe ATM services.	5 3	Keys elements/equipment of sub-systems shall be manually controlled.
H-BMS_4	BMS Monitoring function	**Partial loss of the BMS** due to a total loss of the monitoring function (sub-systems elements failures, server failure, work station failure,….)	No direct effects No monitoring function available to give the status of sub-systems equipment involving in the ATC operation process	No direct impact on service Serious inability to provide or maintain safe ATM services. Possible decrease of the service.	5 2	Monitoring of keys elements/equipment of sub-systems shall be hardware visible and accessible.
H-BMS_5	BMS Software	**Total loss of the BMS** due to a bug of the software (main program generating a false alarm or unwarranted command…) - where the issue freezes or shuts down SW application,	Direct effect could be Inability to maintain ATC operations. Complete loss of safety margins (false control generated of dysfunction or loss of sub-systems, false command, false alarm, discomfort of users, unnecessary evacuation….)	Direct impact on service could be Serious inability to provide or maintain safe ATM services. Possible loss of the service.	2	A degraded version of the BMS software shall be available for keys functions That is assuming an architecture and transforming the safety objective on the BMS function into a safety requirement on the software

SOFTWARE CASE

The Case of Credible Corruption data is approached in the paragraph 6.4.2.

6.4 Safety Objectives Specification and Synthesis

The synthesis presents:

- the results of the analysis tables (see § 6-3-1) and
- the synthesis tables.

The synthesis is sorted by severity that has been allocated to the effects (1 being the most severe and 5 the least severe).

We have called the severity effect level of [1- 2]: ”first order”.

The “first order” corresponds respectively to:

- accidents and complete loss of safety margins and
- serious incidents and large loss of the safety margins.

Out of this interval the severity level is called “second order”.

The presentation is organised around:

- the building and the infrastructure level,
- the 5 sub-systems level,
- the synthesis tables with the severity level of the “first order”.

6.4.1 Building and infrastructure synthesis

The severity level for the Building and the Structure is mainly found within [1-2].

It stresses that a major part of external events can lead to a loss of the building or sub-system(s) and consequently lead to a total or strongly degraded loss of safety margins.

External events have been defined as natural (climate, environment…) or extra-natural (intrusion, plane crash…).

Concerning communication, the severity level is the most severe (equal to 1).

6.4.2 Sub-systems synthesis

Concerning the other sub-systems, the **Power Supply** appears as major in the operational ATC system. This sub-system supplies all other sub-systems, the operational room and consoles. The severity level is mainly of the “first order”.

This could be true also for the **HVAC** sub-system concerning the following applications:

- Ventilation of the consoles and
- Extraction of smokes. But in this case the ATC system is able to operate, and a total loss of the HVAC sub-system will lead to a severity level equal to 2.

The severity level of the **Water Supply** sub-system is of the “second order”; it is found within [3-5]. Hazards have no effects on console ventilation to maintain a service in safe conditions.

The severity level of the **Fire Protection** sub-system is of the “first order” concerning a total loss, but also a loss of fire prevention (including protection of equipment). These two last cases have a strong effect on the operational ATC system. Fire protection addresses the question of Fire strategy.

Severity level of the **BMS** sub-system addresses surveillance aspect. It is found within [2-5]. It is of “first order” concerning a total loss of BMS office (destruction) and a loss of the monitoring function.

In the case of software bug the severity is 2. Among these cases, software appears as the predominant case.

Particular attention must be paid to the “Credible Corruption” of data. In this case erroneous data coming from sub-systems are seen as valid by the BMS sub-system, and the operator as well. Signal is not generated and alarm not sent. The operator doesn’t know that something goes wrong.

The hazard could lead to a total loss of the BMS. But a partial loss could be the worst case, because the effect of the hazard will depend on the sub-system impacted by the “Credible Corruption of data”.

6.4.3 Safety Objectives Specification

6.4.3.1 “First Order” Safety Objectives

Hereafter the synthesis tables present the Safety Objectives of the “first order” classified according to the severity level for the building and its structure and sub-systems.

Safety objectives are specified qualitatively hereafter, however using §6.3.4, they can be specified quantitatively when applicable.

Hazard Ref	Function	Hazard	Severity	Safety objectives	SO Ref
H-BU_1	Building ATC rooms	**Total loss of ATC rooms** due to object collision (aircraft, meteorite, vehicle…), severe damage of building	1	No safety Objective. As this event is so unlikely to happen, it has been decided to do nothing to avoid or to mitigate this hazard (sometimes nothing can be done). This risk is classified as acceptable by management.	SO-BU_1
H-BU_2	Building ATC rooms	**Total loss of ATC rooms** due to weather conditions (earthquake, tornado, lightning, wind, snow, flooding ….) leading to evacuate the personnel of the building, severe damage of building	1	The total loss of ATC rooms due to weather conditions shall be no greater than Extremely Rare. The structure of the building shall be dimensioned with margins to fulfil the standards in force and taking into consideration Local meteorological conditions (historical data collected) with respect to : - earthquake, tornado, lightning - wind speed, snow, flood	SO-BU_2
H-BU_3	Building ATC rooms	**Total loss of ATC rooms** due to hostile action (terrorism, alert, bomb….) leading to evacuate the personnel of the building	1	No safety Objective. This is out of scope of this safety analysis. However the recommendation is to define a Security policy to prevent intrusion inside the site and at strategic points (PS facilities, BMS office, operational room, …..)	SO-BU_3
H-BU_4	Building ATC rooms	**Total loss of ATC rooms** due to chemical pollution, leading to loss of the staff	1	The total loss of ATC **rooms** due to chemical pollution shall be no greater than Extremely Rare.	SO-BU_4
H-BU_7	Building ATC rooms	**Total loss of ATC rooms** due to : - switch off of the Power Supply public network (failure) - strike of the Power Supply public network	1	The **Total loss of ATC rooms** due to external total loss of Power Supply shall be no greater than Extremely Rare.	SO-BU_7
H-BU_9	Building	**Total loss of ATC data** (voice, radar, network, phone, meteorology, others FIR's)	1	The **Total loss of ATC data** shall be no greater than Extremely Rare.	SO-BU_9

Hazard Ref	Function	Hazard	Severity	Safety objectives	SO Ref
	ATC data communication				
H-PS_1	Power Supply ATC rooms	**Total loss of power supply** due to : - water, fire, flood, earthquake, lightning, - equipment failures (wiring damages..)	1	The **Total loss of ATC rooms** due to internal total loss of Power Supply shall be no greater than Extremely Rare.	SO-PS_1
H-BMS_5	BMS Software	**Total loss of the BMS** due to software bug (main program generating a false alarm or unwarranted command…)	2	The Total loss of the BMS due to software bug shall be no greater than Rare.	SO-BMS_5
H-PS_2	Power Supply ATC rooms	**Partial loss of power supply** due to : - water, fire, flood, earthquake, lightning, equipment failures (wiring damages …) , micro breakdown	2	The **Partial loss of power supply leading to loss of ATC room lighting and escape route lighting** shall be no greater than Rare.	SO-PS_2
H-HVAC_1	HVAC	**Total loss of HVAC: loss of the consoles ventilation, rooms ventilation, smokes extraction due to:** - partial loss of the Power Supply, fire earthquake, equipment or network failure	2	The **Total loss of HVAC for more than TBD** shall be no greater than Rare.	SO-HVAC_1
H-FIRE_1	Fire Protection ATC rooms	**Total loss of fire Protection functions : loss of the Fire Prevention, the fire detection, the users and equipment protection** due to: - partial loss of PS, partial loss of the BMS, earthquake, , materials degradation	2	The **Total loss of fire Protection functions for more than TBD** shall be no greater than Rare.	SO-FIRE_1
H-FIRE_2	Fire Protection ATC rooms	**Partial loss of the Fire Protection functions: loss of the fire prevention** (including equipment protection) due to: - materials degradation or equipment failure**,** earthquake	2	The **Partial loss of the Fire Protection functions in ATC rooms or more than TBD** shall be no greater than Rare.	SO-FIRE_2
H-BMS_1	BMS	**Total loss of the BMS office** due to :	2	The **Total loss of the BMS office** shall be no greater than	SO-BMS_1

Hazard Ref	Function	Hazard	Severity	Safety objectives	SO Ref
	Office	- fire, flood leading to an inability to supervise, monitor and to control the equipment of the sub-systems.		Rare.	
H-BMS_4	BMS Monitoring function	**Partial loss of the BMS** due to a total loss of the monitoring function (sub-systems elements failures, server failure, work station failure,….)**.**	2	The **Partial loss of BMS** monitoring function **for more than TBD** shall be no greater than Rare.	SO-BMS_4
H-FIRE_3	Fire Protection ATC rooms	**Partial loss of the Fire Protection functions : loss of the fire detection** due to: - partial loss of PS, partial loss of the BMS - equipment failure - earthquake,	2	The **Partial loss of the Fire Protection functions (fire detection) in ATC rooms or more than TBD** shall be no greater than Rare.	SO-FIRE_3
H-BU_6	Building ATC rooms	**Total loss of ATC rooms** equipment due to electromagnetic irradiation	2	The **Total loss of ATC rooms** equipment due to electromagnetic irradiation shall be no greater than Rare.	SO-BU_6

6.4.3.2 "Second Order" Safety Objectives

REF	Function	Hazard	Severity	Safety objectives	SO REF
H-BU_5	Building ATC rooms	**Total loss of ATC rooms** due to pollution (exterior fire smoke**)** leading to evacuate the staff	3	The total loss of ATC rooms due to external air pollution shall be no greater than Occasional.	SO-BU_5
H-BU_10	Building	**Partial loss of ATC rooms** due to earthquake, vibration…, leading to a degradation of the	3	The Partial loss of ATC rooms due a degradation of the building structure shall be no greater than Occasional.	SO-BU_10

REF	Function	Hazard	Severity	Safety objectives	SO REF
	ATC rooms	building facilities			
H-WASU_1	Water Supply ATC rooms	**Total loss of the Water Supply functions**: Loss of the drinking and non-drinking water supplies due to: - equipment or internal WS network failures - partial loss of PS - fire, earthquake	3	The Total loss of the all Water Supply functions for more than TBD shall be no greater than Occasional.	SO-WASU_1
H-HVAC_2	HVAC	**Partial loss of HVAC functions : loss of the console ventilation due to :** - partial loss of PS - equipment or network failures - flood, fire, earthquake	3	The total loss of console ventilation for more than TBD shall be no greater than Occasional.	SO-HVAC_2
H-BMS_2	BMS Office	**Total loss of the BMS office** due to: - partial loss of PS acting on BMS office	3	The partial loss of power in the BMS room for more than TBD shall be no greater than Occasional.	SO-BMS_2
H-BMS_3	BMS Control function	**Partial loss of the BMS** due to a loss of control functions (sub-systems elements failures, server failure, control station failures, loss of monitor functions..).	3	The total loss of BMS control function for more than TBD shall be no greater than Occasional.	SO-BMS_3
H-BU_8	Building ATC rooms	**Partial loss of ATC operations** due to noise	4	The Partial loss of ATC operations due to noise shall be no greater than Likely.	SO-BU_8
H-BU-12	Building ATC rooms	**Degraded conditions for ATC rooms** due to fire or *emergency personnel* (unavailability)	4	Degraded conditions for ATC rooms due to fire personnel or emergency personnel (unavailability) shall be no greater than Likely.	SO-BU-12
H-HVAC_3	HVAC	**Partial loss of HVAC functions : loss of the smokes extraction (in the ATC rooms and the escapes routes) due to :** - partial loss of Fire Detection	4	The total loss of smoke extraction in ATC rooms and escape routes for more than TBD shall be no greater than Likely.	SO-HVAC_3

REF	Function	Hazard	Severity	Safety objectives	SO REF
		- partial loss of PS - equipment failures - Fire, flood, earthquake,			
H-BU_11	Building ATC rooms	**DEGRADED CONDITIONS IN ATC ROOMS** DUE TO : - turning off of the potable Water Supply public network - strike of the Water Supply public network	5	No safety objective.	SO-BU_11
H-WASU_2	Water Supply ATC rooms	**Partial loss of the Water Supply functions:** Loss of drinking water due to: - temperature - loss of PS - fire, earthquake	5	No safety objective.	SO-WASU_2

7. CONCLUSION

The present Safety Objectives are elaborated by identifying effects of the loss or degradation of the main functions implemented by the operational “global ground system” on the ATM service provision and on the end user (namely the aircraft and aircrew).

Safety objectives specify the maximum tolerable frequency of occurrence of a hazard identified at the building level when assessing the operation of sub-system hosted by the Building system.

For each hazard, a severity of its worst credible effect has been allocated using EATMP SAM scheme.

Values are found within the interval [1-5] ([1] the most severe to [5 the least severe]).

The most stringent Safety Objectives (severity level within [1- 2]) are listed and classified in the synthesis tables.

These Safety Objectives should be apportioned into Safety Requirements on system or sub-systems elements.

For the building fitting and equipment, operation, maintenance and the infrastructure, it means that the design should take them into account.

As external “communication system” is not included in the “global ground system”. It means that the organisation and implementation of the external “communication system” shall comply with its own safety objectives.

For the Power Supply, which appeared as major risk area, it means that the design of the Power Supply shall take into account a zero-break requirement.

For the BMS, the software part appears as the predominant case for Safety.

APPENDIX 1

EXTERNAL FUNCTIONAL ANALYSIS

1- DEFINITION OF THE DIFFERENT USED FUNCTIONS

A functional analysis involves four kinds of functions :

- **The main functions (F_P)** correspond to the essential functions for which the product has been designed and which ensure the service expected by the user.

- **The service complementary or secondary functions (F_S)** correspond to a need which shall be satisfied in the same way as the main need.

- **The constraints functions (F_C)** result from a limit of conception liberty of the system. They decode “adaptation” actions of the system to its environmental elements.

- **The technical functions** result from solutions and building choices adopted for enabling to satisfy the service functions. These functions are used on the synthesis tables of the internal functional analysis.

2- THE EXTERNAL FUNCTIONAL ANALYSIS

The functional analysis is initiated at the system level by an **external analysis.**
It consists in structuring the system functions (main, secondary and constraints).

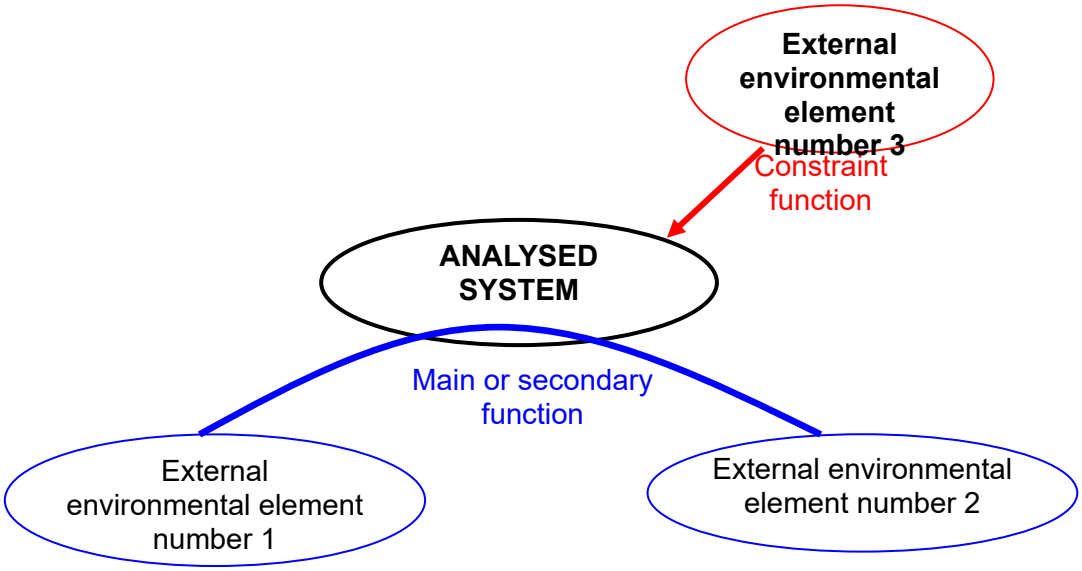
The system is considered as a “black box ” which interfaces its environment.

A Venn Diagram is used to perform the external functional analysis where the functions are represented as follows (see scheme 1 hereafter) :

- a *main or secondary* function is represented by the connection of two exterior elements through the studied system.
- a *constraint* function is symbolised by a direct arrow between an exterior element (constraint origin) towards the system.

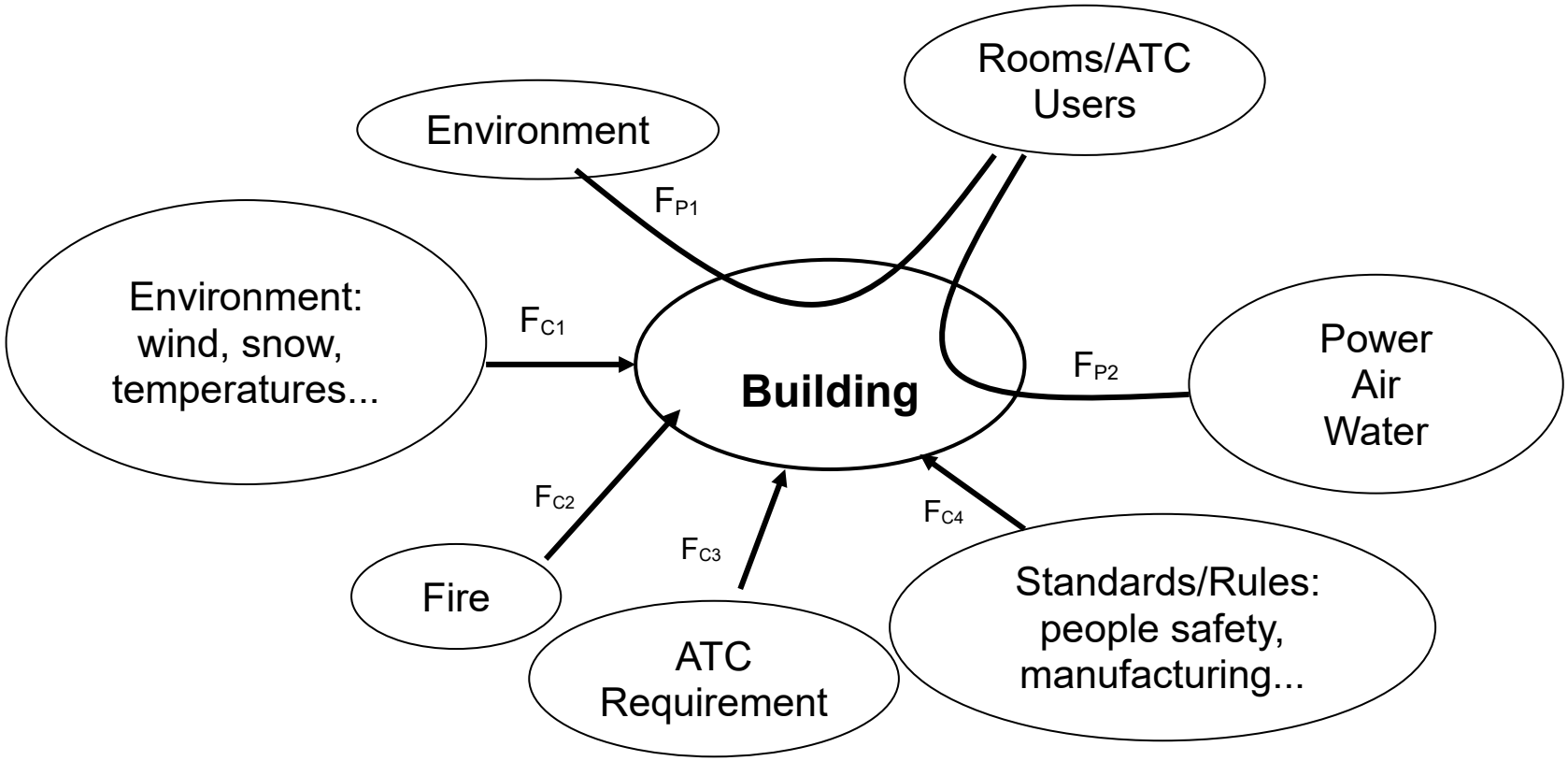
The external environmental elements can be:

- Human elements (WARNING: human factors (ATCO, maintenance staff, …) are part of the analysis, so what are these “external” human elements?)
- Meteorological elements (flooding, earthquake, lightning)
- Technical elements (Power Plants, Water Network, …)
- Pollution



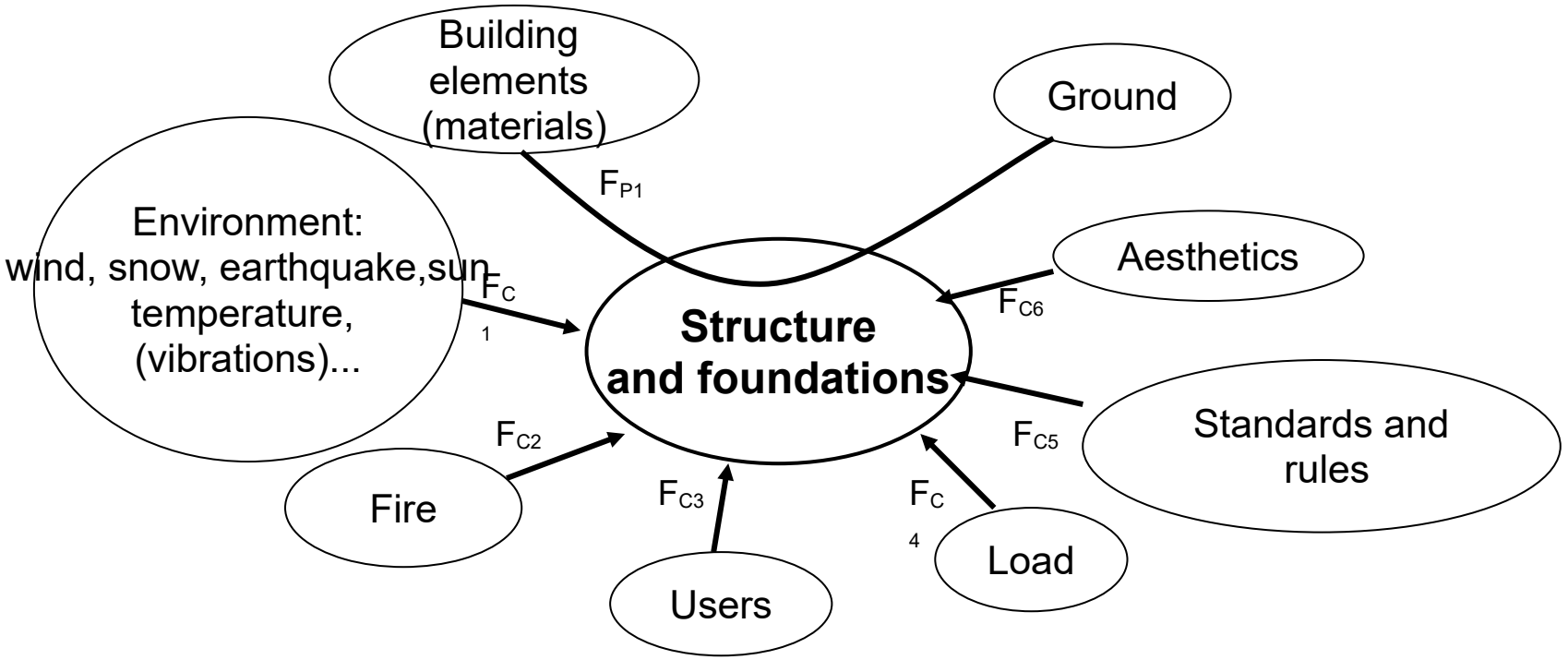
EXTERNAL FUNCTIONAL ANALYSIS DIAGRAMS

System functional analysis diagram : « Building »



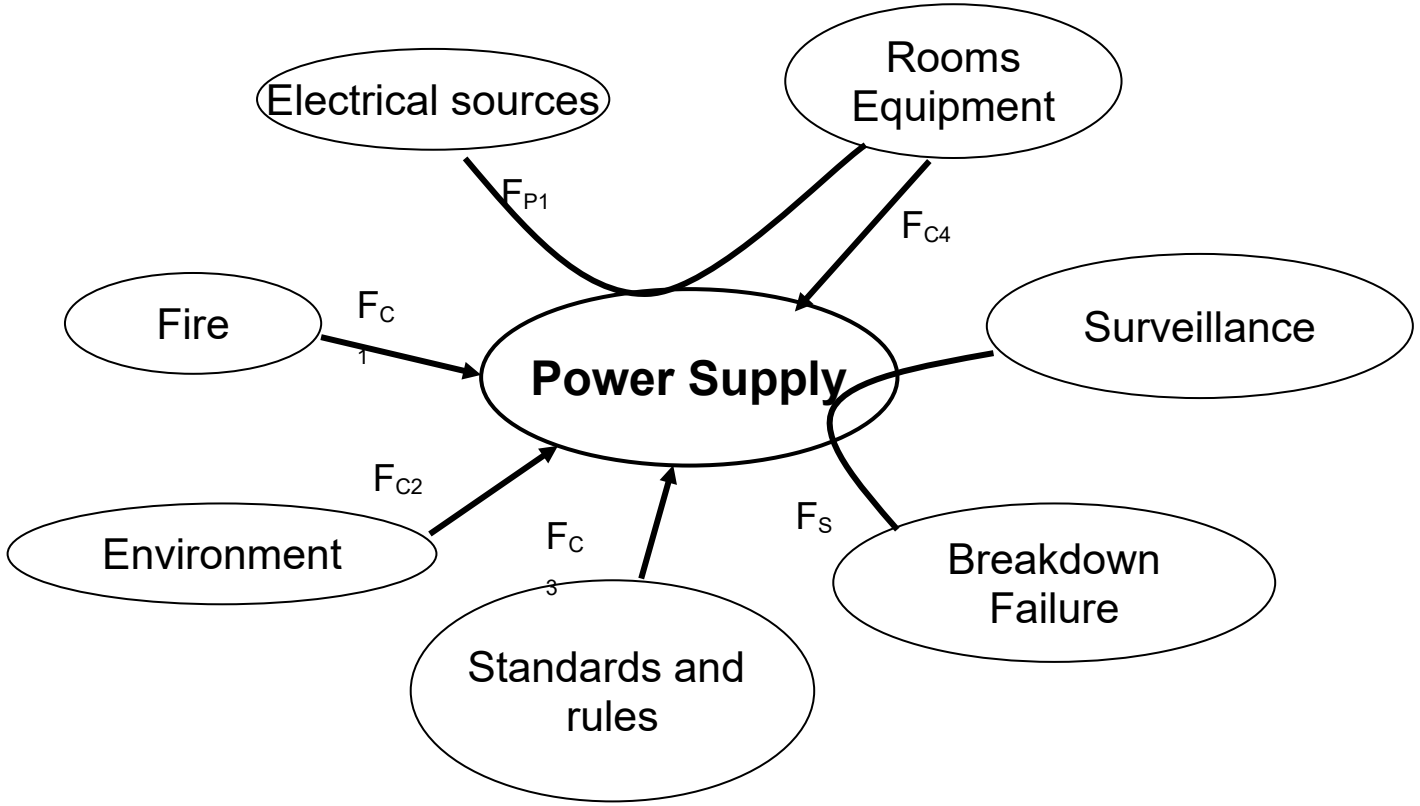
F_{P1}: To protect equipment /environment users
F_{P2}: To ensure a back-up to elements necessary for users ' comfort and equipment running / ATC
F_{C1}: To resist to climate phenomenon
F_{C2}: To resist to fire
F_{C3}: To comply with ATC operational requirements
F_{C4}: To comply with in-force standards and rules

Sub-system: « Structure »



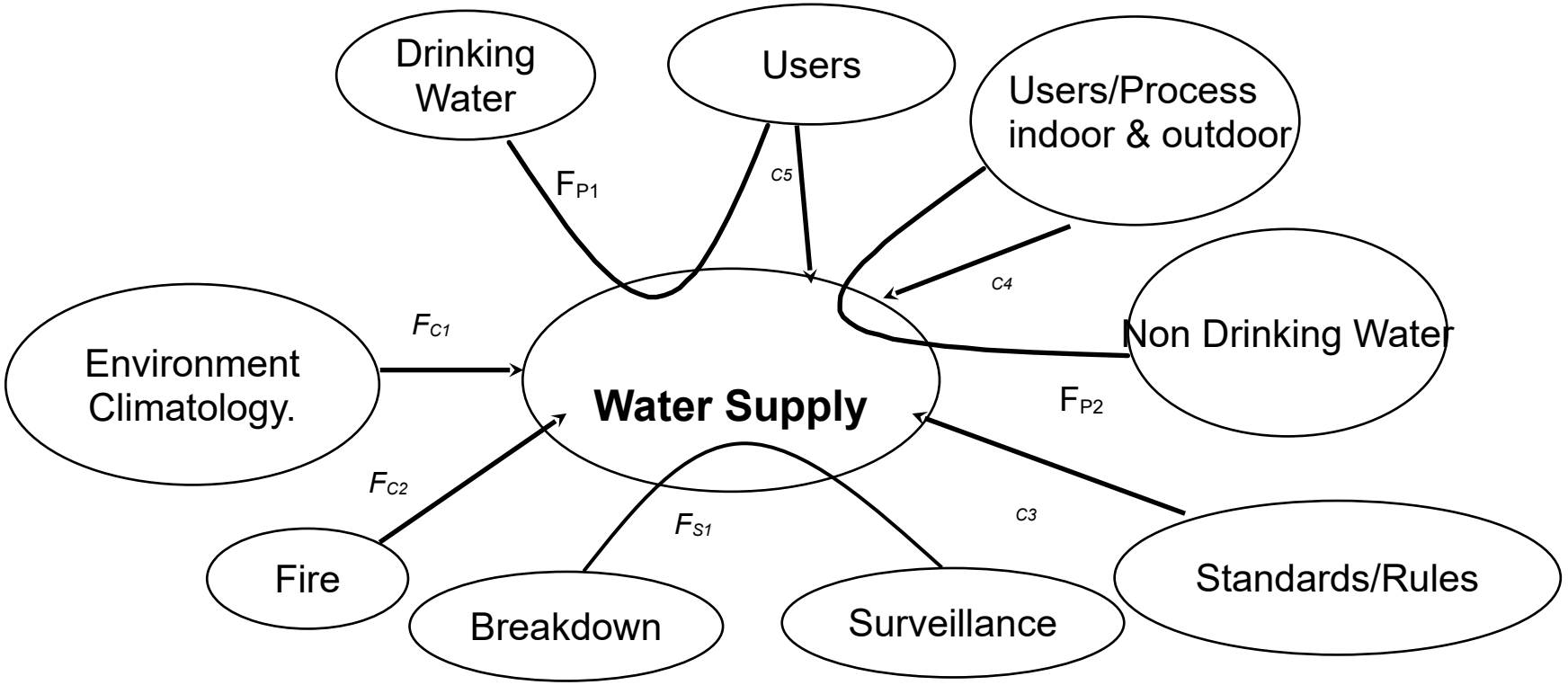
F_{P1}: To support the whole building
F_{C1}: To resist to climate phenomenon
F_{C2}: To resist to fire
F_{C3}: To provide users with comfort (easy access, acoustics, mechanical transportation …)
F_{C4}: To support the load
F_{C5}: To comply with in-force standards and rules
F_{C6}: To fulfil aesthetic criteria

Sub-system: « Power Supply »



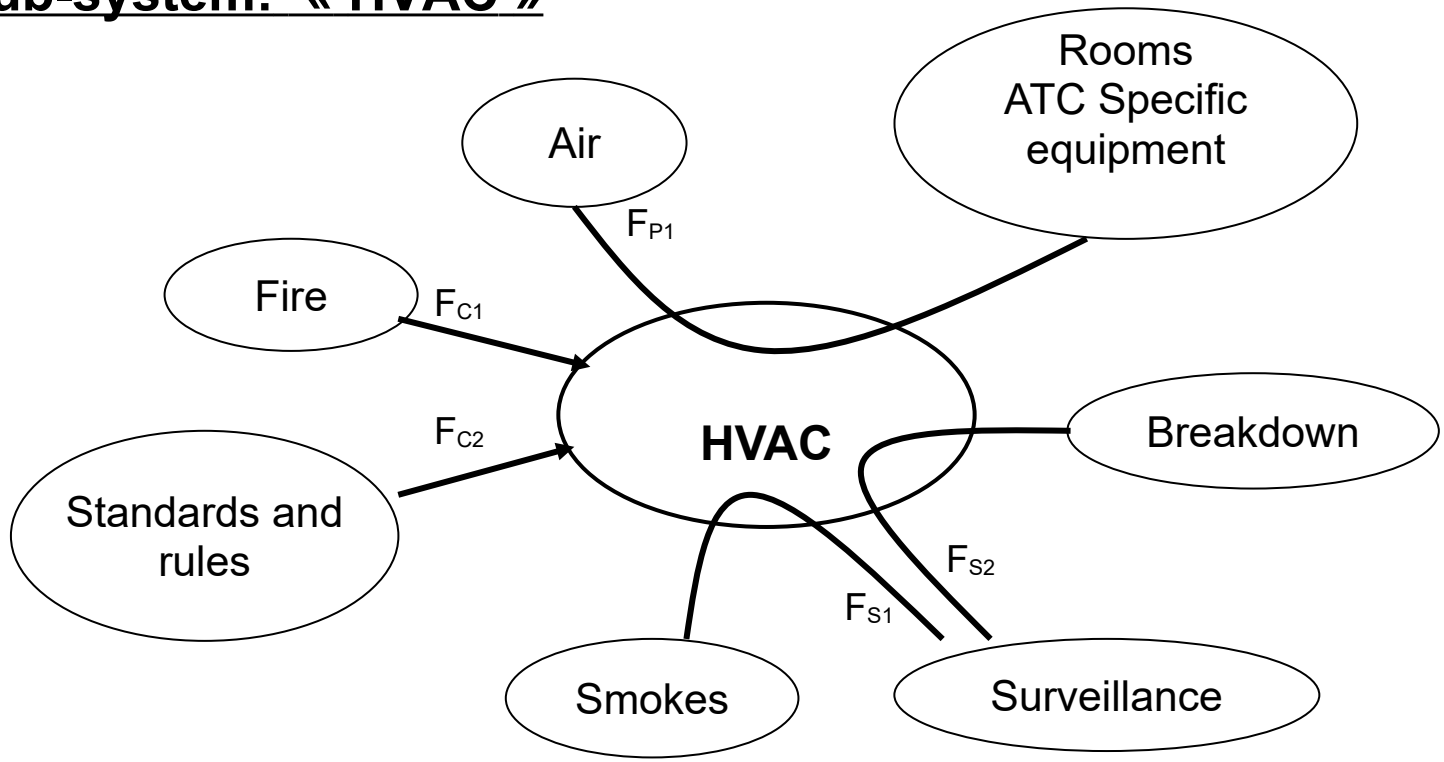
F_{P1}: To continuously supply equipment and rooms
F_{S1}: To detect any electrical breakdowns on the Power Supply network
F_{C1}: To resist to fire (thermal insulation)
F_{C2}: To resist to climate phenomenon
F_{C3}: To comply with standards and rules
F_{C4}: To dimension the Power Supply system with regard to the electrical needs required by the building

Sub-System : « Water Supply »



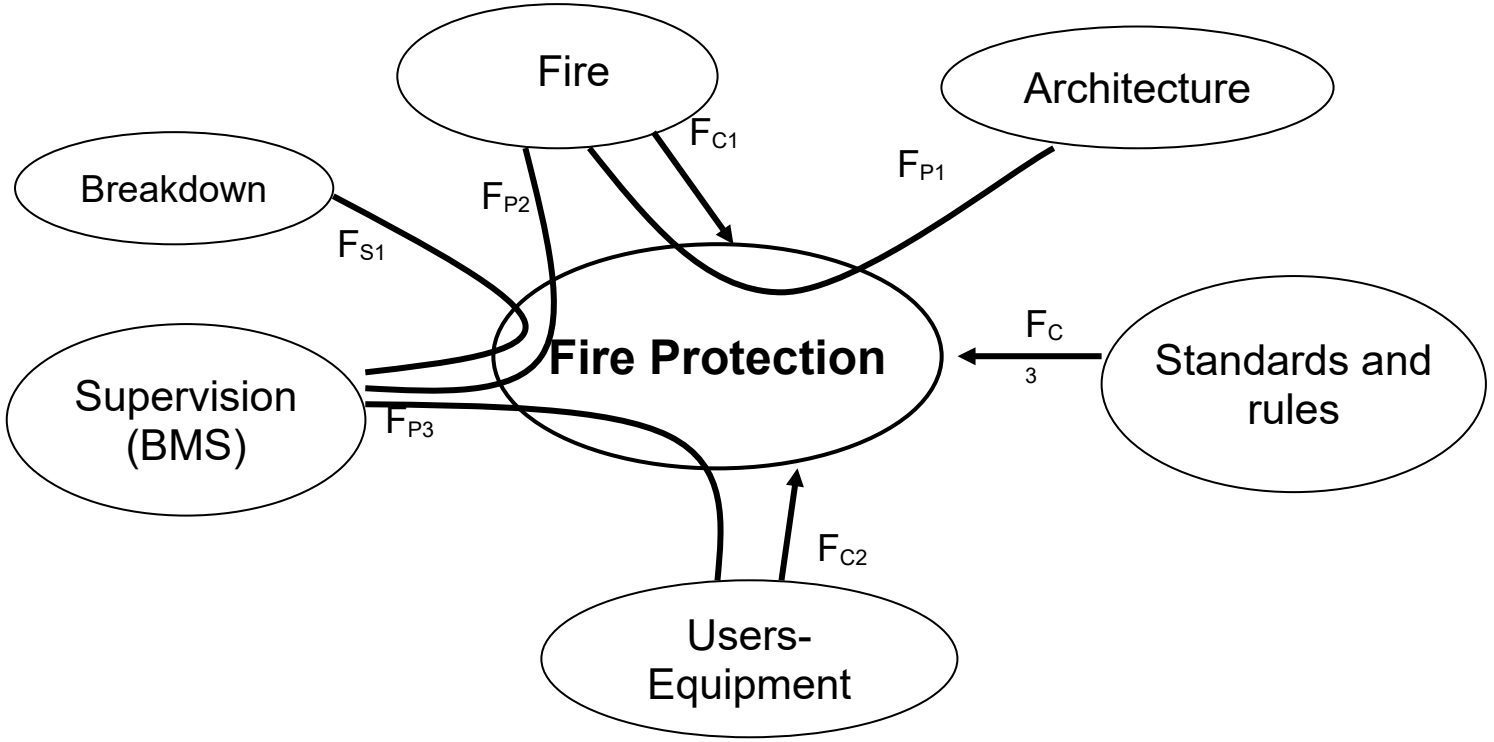
F_{P1}: To provide users with drinking water
F_{P2}: To provide water to indoor and outdoor building process
F_{S1}: To detect any failures on the Water Supply network
Fc_1 : To resist against natural elements
Fc_2 : To be fire resistant (indoor equipment).
Fc_3 : To comply with the standards and rules
Fc_4 : To comply with the process requirements
Fc_5 : To comply with the users requirements

Sub-system: « HVAC »



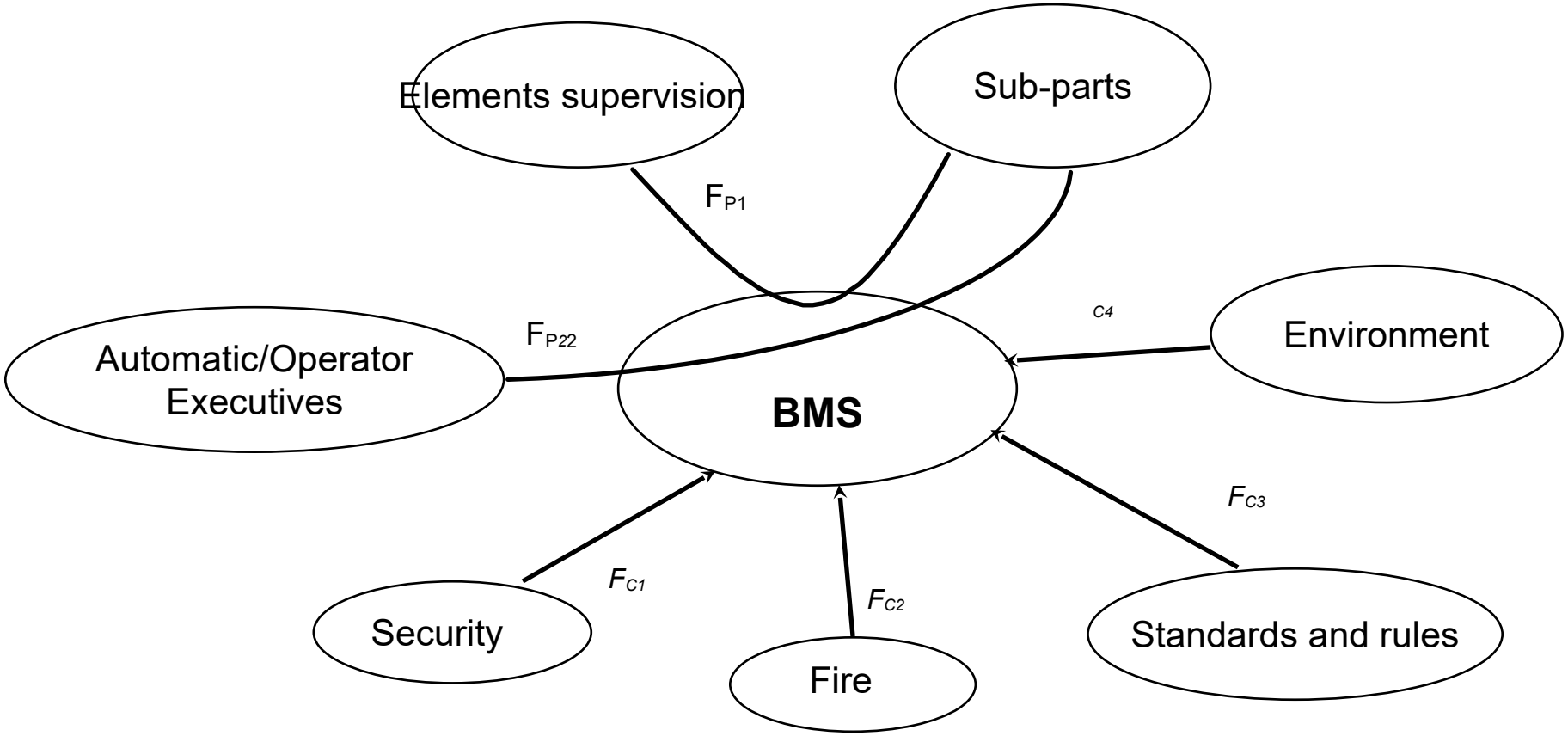
F_{P1}: To ventilate facilities air and ATC equipment
F_{S1}: To extract smoke in the area in which fire has been detected
F_{S2}: To detect any failures of the HVAC sub-system
F_{C1}: To resist to fire
F_{C2}: To comply with in-force standards and rules

Sub-system: « Fire Protection »



F_{P1}: To prevent fire risks
F_{P2}: To detect fire
F_{P3}: To protect « ATC » equipment and users against fire
F_{S1}: To detect any failures on the « Fire Protection » sub-system
F_{C1}: To resist to fire
F_{C2}: To avoid damage equipment and users ' health
F_{C3}: To comply with standards and rules about safety

Sub-System : « BMS »



F_{P1}: To monitor the status of the key parameters of the sub-systems
F_{P2}: To control the operations of the sub-systems (nominal & degraded mode)
Fc_1 : To foresee a protected access
Fc_2 : To resist to fire
Fc_3 : To comply with the standards requirements
Fc_4 : To be designed taking into account internal environmental parameters (water, humidity, temperature,..)

APPENDIX 2

FORMAT OF HAZARDS TABLE

1. REF	**2. Function**	**3. Hazard**	**4 ATCC effect**	**5 ATM effect**	**6 Severity**	**7 Comments/Remarks**

Page intentionally left blank