Airbus Product Safety
Xavier Jolivet
Safety Enhancement

System Safety Analysis

CS 25.1309 CERTIFICATION BASIS

CS-25
Large Aeroplanes

EUROPEAN AVIATION SAFETY AGENCY
AGENCE EUROPEENNE DE LA SECURITE AERIENNE
EUROPAISCHE AGENTUR FUR FLUGSICHERHEIT

BOOK 1 – CS 25.1309
SUBPART F - EQUIPMENT

(a) The airplane equipment and systems must be designed and installed so that:

(1) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under the airplane operating and environmental conditions.

(2) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(1) of this paragraph.

(b) The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that :

(1) Any catastrophic failure condition
(i) is extremely improbable; and
(ii) does not result from a single failure; and

(2) Any hazardous failure condition is extremely remote; and

(3) Any major failure condition is remote.

CS 25.1309 CERTIFICATION BASIS

CS-25
Large Aeroplanes

EUROPEAN AVIATION SAFETY AGENCY
AGENCE EUROPEENNE DE LA SECURITE AERIENNE
EUROPAISCHE AGENTUR FUR FLUGSICHERHEIT

BOOK 1 – CS 25.1309
SUBPART F - EQUIPMENT

(c) Information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. A warning indication must be provided if immediate corrective action is required. Systems and controls, including indications and annunciations must be designed to minimize crew errors, which could create additional hazards.

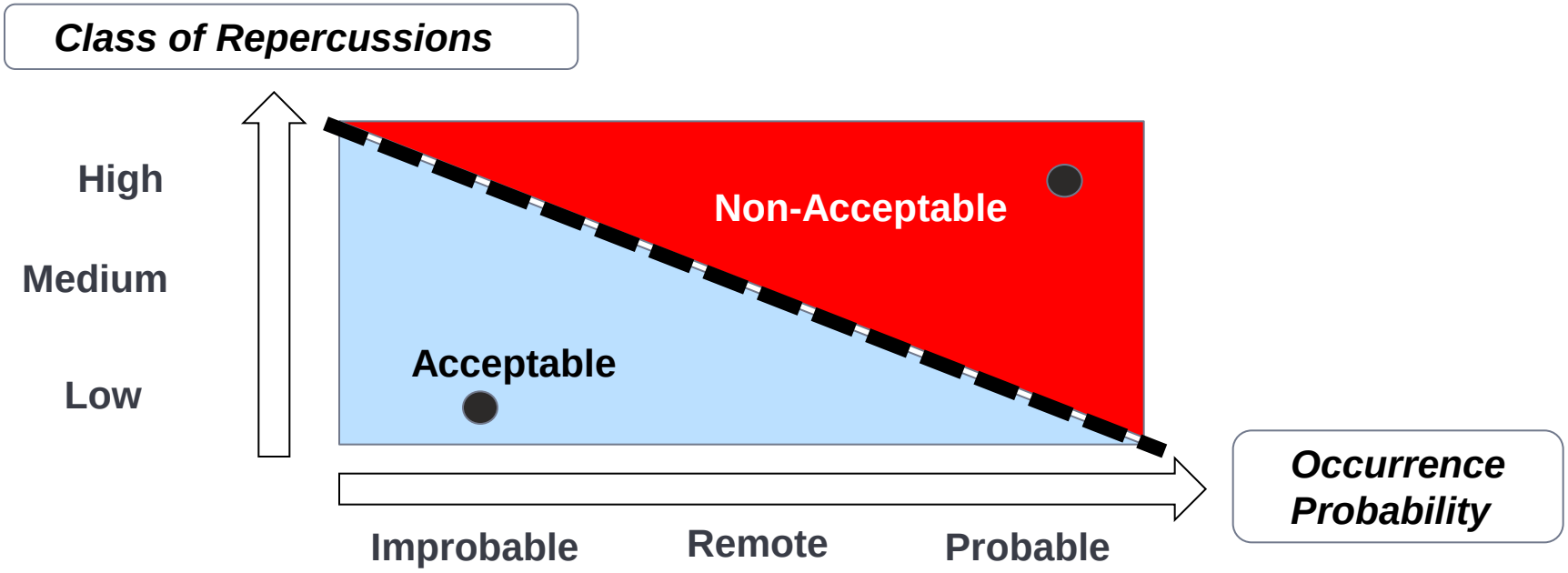
(d) Electrical wiring interconnection systems must be assessed in accordance with the requirements of CS 25.1709.

[Amdt. No.: 25/5]
[Amdt. No.: 25/6]

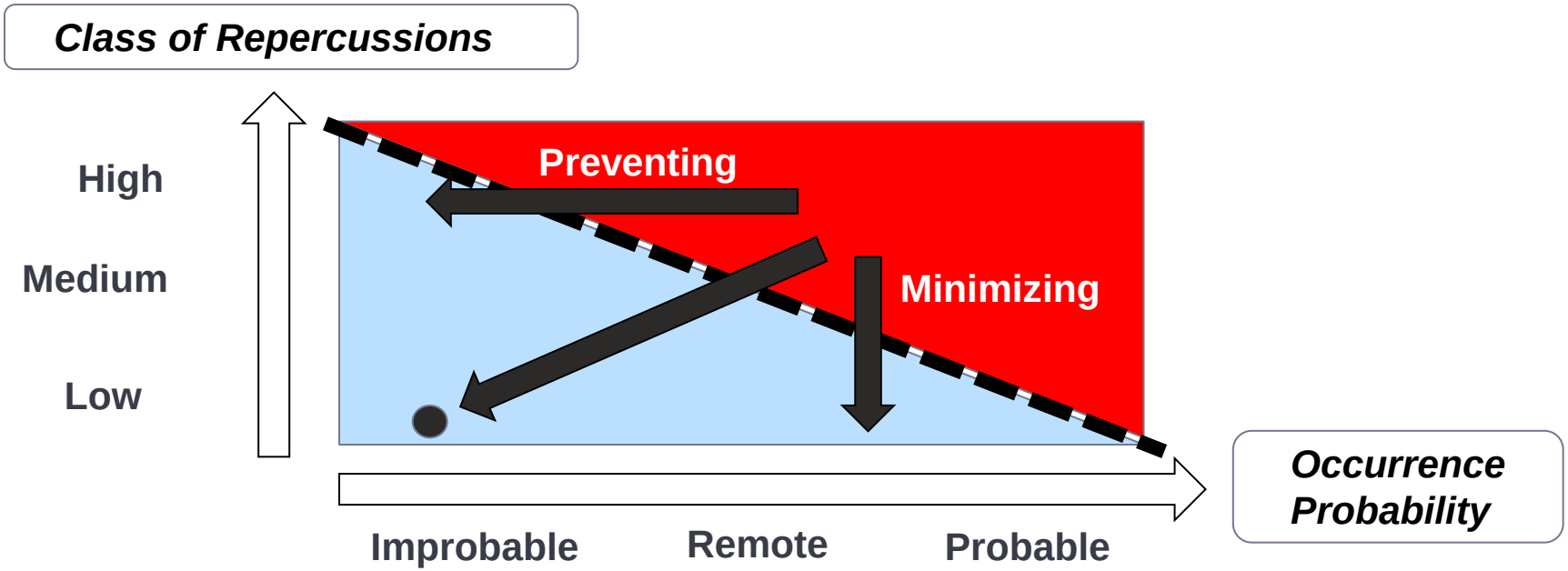
CS 25.1309 & AMC / Risk matrix

Risk = { Occurrence ; Repercussions }

- **Occurrence stands for Occurrence Conditions, Frequency, Rate, Probability …**
- **Repercussions Stands for Class of repercussions, Severity, Field of repercussions, Consequences level, …**



CS 25.1309 & AMC / Risk matrix



Failure Condition

Failure condition definition (from ACJ No1 to 25.1309)

- *A failure condition is defined at the level of each system by its effect on each functioning of that system.*
- *It is characterised by its effects on the other systems on the complete aircraft.*
- *All single failures and combinations of failures including failures on other systems, which have the same effect on the system under consideration are grouped in the same failure condition.*

Examples of failure conditions

At A/C level (multi system Failure Conditions):

- Total loss of deceleration capability at landing or during a RTO
- Loss of one engine
- loss of landing gear retraction
- Loss of navigation data

At system level :

- Spurious engine fire warning
- Loss of anti-skid at landing or during a RTO
- Flight control surface runaway
- Erroneous display of attitude or altitude information

Class of repercussions per AMC 25.1309

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation

Class of repercussions per AMC 25.1309

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of Failure Conditions	No Safety Effect	<-----Minor------>	<-----Major------>	<--Hazardous-->	Catastrophic

Class of repercussions per AMC 25.1309

Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<---------- > $<10^{-3}$	<---------- > $<10^{-5}$	<---------- > $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor------ >	<-----Major------ >	<--Hazardous-- >	Catastrophic

Class of repercussions per ACJ No1 to JAR 25.1309

Classification of failure condition (in accordance with ACJ No1 to JAR 25.1309)

MINOR EFFECTS:

- SLIGHT REDUCTION IN SAFETY MARGINS
- SLIGHT INCREASE OF CREW WORKLOAD
- CONFORT PASSENGER DECREASE

MAJOR EFFECTS:

- SIGNIFICANT REDUCTION IN SAFETY MARGINS
- DIFFICULTY FOR CREW TO COPE WITH ADVERSE CONDITIONS
- OCCUPANT INJURIES

HAZARDOUS EFFECTS:

- LARGE REDUCTION IN SAFETY MARGINS
- CREW EXTENDED BECAUSE OF WORKLOAD OF ENVIRONMENTAL CONDITIONS
- SERIOUS OR FATAL INJURY TO A SMALL NUMBER OF OCCUPANTS

CATASTROPHIC EFFECTS:

- MULTIPLE DEATHS, USUALLY WITH LOSS OF AIRCRAFT

Safety Objectives per ACJ No1 to JAR 25.1309

Safety Objectives

- The Safety objectives will give the maximum allowable probability for the failure conditions, taking into account the associated predicted consequences as laid down in the ACJ N° 1 of JAR 25-1309:

Classification	Objectives at FC level
Catastrophic	$< 10^{-9}$/hr + Fail Safe criterion
Hazardous	$< 10^{-7}$/hr
Major	$< 10^{-5}$/hr
Minor	no objective

System Safety Assessment

System **S**afety **A**ssessments (SSA) are a chosen means of demonstrating compliance with 25.1309 and associated ACJ or AMJ (and AMC)

- Main steps of the methodology are:
  - Functional description of the system
  - Identification by the application of Functional Hazard Assessment (FHA) of
    - all significant Failure Conditions (whether arising from single or multiple failures, taking into account modifying factors and causes external to the system) and the associated objectives.
    - criticality of functions.
  - Only Failure Conditions leading to Major, Hazardous or Catastrophic consequences is studied by appropriate means (Engineering Judgement, Fault Tree Analysis, failure Mode and effects analysis/FMEA, …).
  - Establishment of failure diagrams (i.e. Fault Logic Diagrams, Dependence Diagrams, etc.) associated with Failure Conditions.

SSA Detailed process - FHA

System Functional Failure Assessment

- 4 basic failure modes: total loss of the system function, Partial loss, Inadvertent operation of function and Erratic functioning
- As single failure or in combination with other failure from the system or from other systems, or with an Event (e.g. severe icing conditions, fire event, ...)
- Effects at system and aircraft level (on other systems, handling qualities, comfort, ...…) for each relevant flight & ground phases
- Failure effects graduations (classification) defined according to **:**
  - safety margin decrease
  - workload increase
  - comfort decrease, injuries, fatalities.

SSA Detailed process - SSA

SSA quantitative approach

The quantitative approach takes account of following :

- Flight duration, Flight phases duration, Risk Time *(Period of time within the flight during which an item must fail in order to cause the studied failure effect.)*
- Hidden failure latency: Maintenance Tasks test interval
- Failure probability of component/equipment of the system: *FMES*
- Failure probability of dependent systems failures
- Events probabilities
  - *e.g. icing conditions, fire event, ...*

Note that most of these figures are given in Appendix of Format & Contents Document

Qualitative assumption associated with quantitative evaluation:

Failure that are considered in combination in Fault tree (input of a AND gate) or dependence diagram are considered as independent.

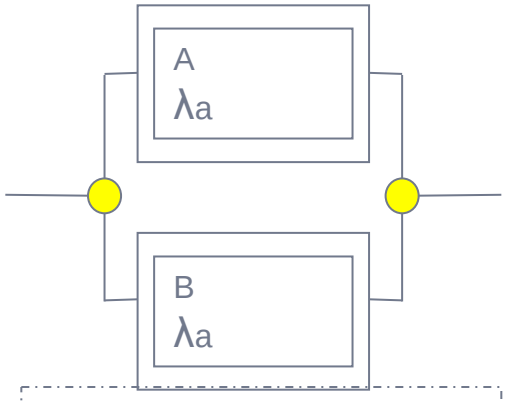
SSA

Detailed process - SSA

SSA quantitative approach

Probability calculation / Flight Hour / for Failure Conditions (aircraft level)

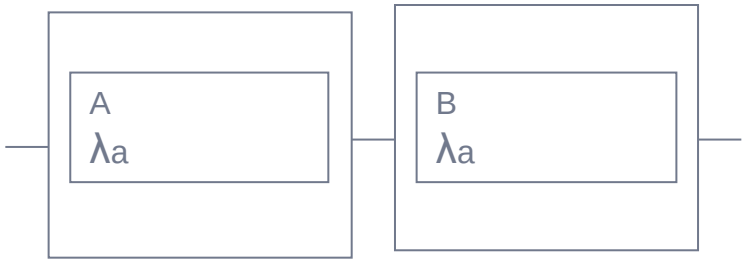
FAILURE CONDITION (aircraft level) Occurs in case of failure of equipment A and equipment B



A and B are independent

=> $\lambda = \lambda a \times \lambda a \times To$

FAILURE CONDITION Occurs in case of failure of equipment A or in case of failure or equipment B



$\lambda = \lambda a + \lambda a$

SSA SUMMARY

SYSTEM SAFETY ASSESSMENT

– **Is a Means of Compliance**

– Each Failure Condition (FC) gather all aircraft failures which leads to the same consequence.

– All significant Failure Conditions are detailed and their link with FMEA/FMES is established,

– Periodic Task Interval are defined and their periodicity is included in the MRBD (& CMR),

– Operational Procedures that must be applied in case of failure in flight are mentioned (AFM & FCOM)

SSA

FC EXAMPLE

Failure condition Description

FAILURE CONDITION SUPPORTING MATERIAL (obj. and proba. are per flight hours ex. otherwise stated)				
FC : 0201A	Title : LOSS OF AC NORMAL GENERATION		Safety/O.R. objective : 5.0E-07	Design Objective :
	Class : MAJ/	Risk Time :	Expected Proba : 3.3E-07	Imposed Proba : 5.0E-07
Effect on aircraft : During transient phase 4PP is supplied from batteries 2 and 4XP is supplied from battery 1 via static inverter as well as Hot buses. With emergency generator on line loss of 1XP, 2XP, 1PP, 2PP, 3PP.				
Crew detection : Overhead panel : - RAT & EMER GEN Fault Light (as long as Ess TR is not on line) - GEN 1 Fault Light - GEN 2 Fault Light ECAM : Elec Page - AC1, TR1, 0V, DC1 amber - AC2, TR2, 0V, DC2 amber - DC BAT amber - GEN 1, GEN 2 amber. Warning : - Continuous repertitive chime - Master Warning - Message : EMER CONFIG procedure				

Illustration only in the context of presentation

Comment : During Rat extension and CSM/G power up, the aircraft handling remains normal due to flight control computers still supplied through battery Hot buses. PFD Capt and ECAM Upper remains available.

RAT deployment duration is considered to be 10 sec. maximum (flight test measurement indicate about 5 sec.).

After CSM/G is on line, electrical flight controls are supplied through 4PP Bus Bar or Hot battery buses.

Maintenance task (See chapter 5.1) : MT14

SSA

FC EXAMPLE

Failure condition Diagram

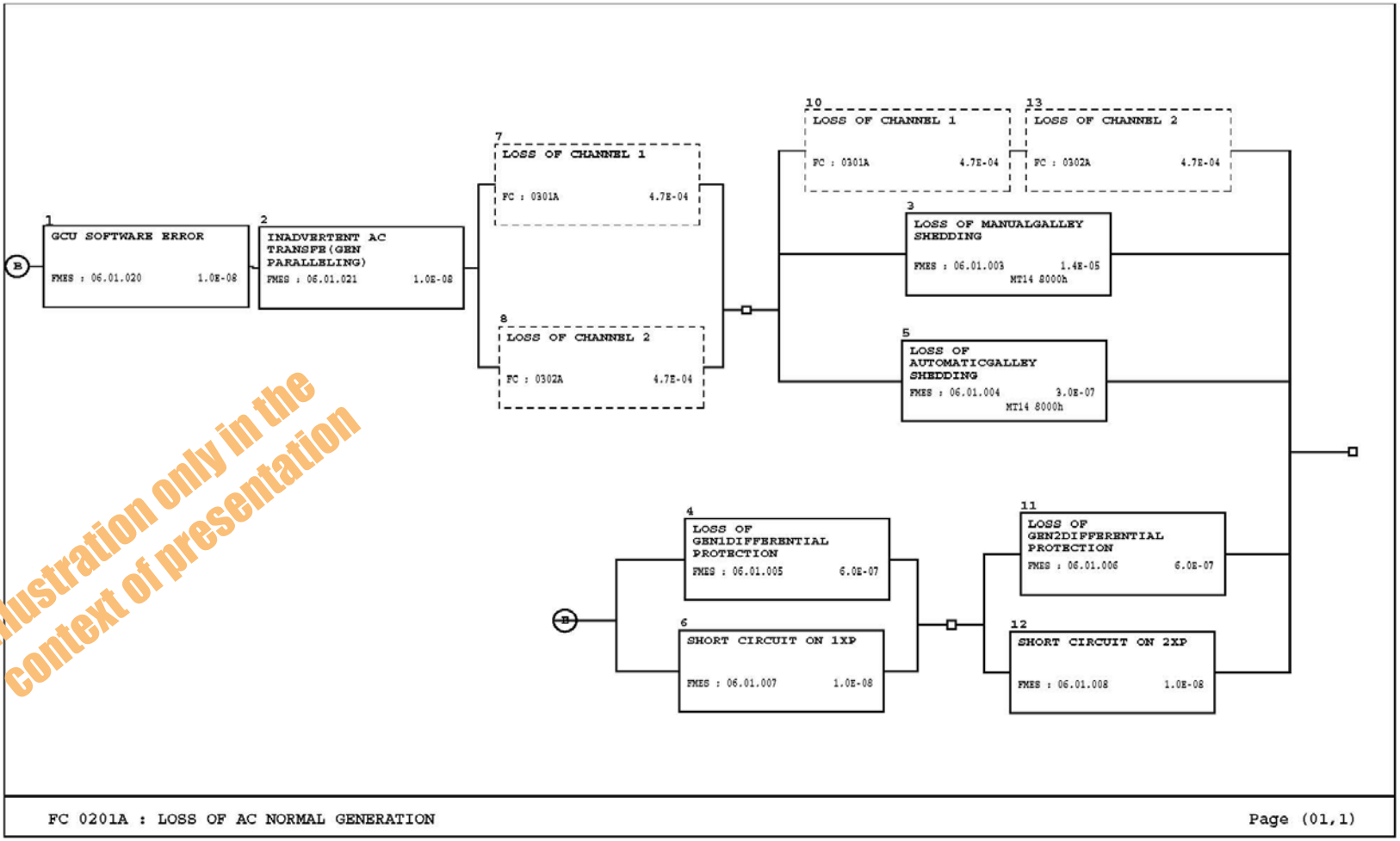


Illustration only in the context of presentation

SSA

Link with FCOM

A318/319/320/321 FLIGHT CREW OPERATING MANUAL	ABNORMAL AND EMERGENCY	3.02.24	P 15
	ELECTRICAL	SEQ 001	REV 26

ELEC EMER CONFIG

LAND ASAP

MIN RAT SPEED ..... 140 KT

CAUTION

At a speed below 140 KT the RAT will stall, and the aircraft electrical supply will be from batteries only.

– GEN 1 + 2 ..... OFF THEN ON

● **IF UNSUCCESSFUL :**

– BUS TIE ..... OFF

Setting BUS TIE pushbutton switch to OFF segregates both generator channels.

– GEN 1 + 2 ..... OFF THEN ON

Note : If any generator reset is successful, reset both FAC's.

· DC and AC ESS BUSES are still supplied by EMER GEN. After landing gear extension emergency generator is no longer powered ; DC and AC ESS BUSES are supplied by normal electrical network. If landing gear is reselected up, essential bus bars remain supplied by the restored generator(s).

– EMER ELEC PWR (if EMER GEN not in line) ..... MAN ON

CAUTION

In case of simultaneous engine generator failure, the probability of a successful APU GEN coupling is low. Therefore APU start attempts should be avoided, as this will consequently reduce the flight time on batteries only (by about 3.5 minutes for one start attempt).

– ENG MODE SEL ..... IGN

Engines are fed by gravity only.

– VHF1/ATC1 ..... USE

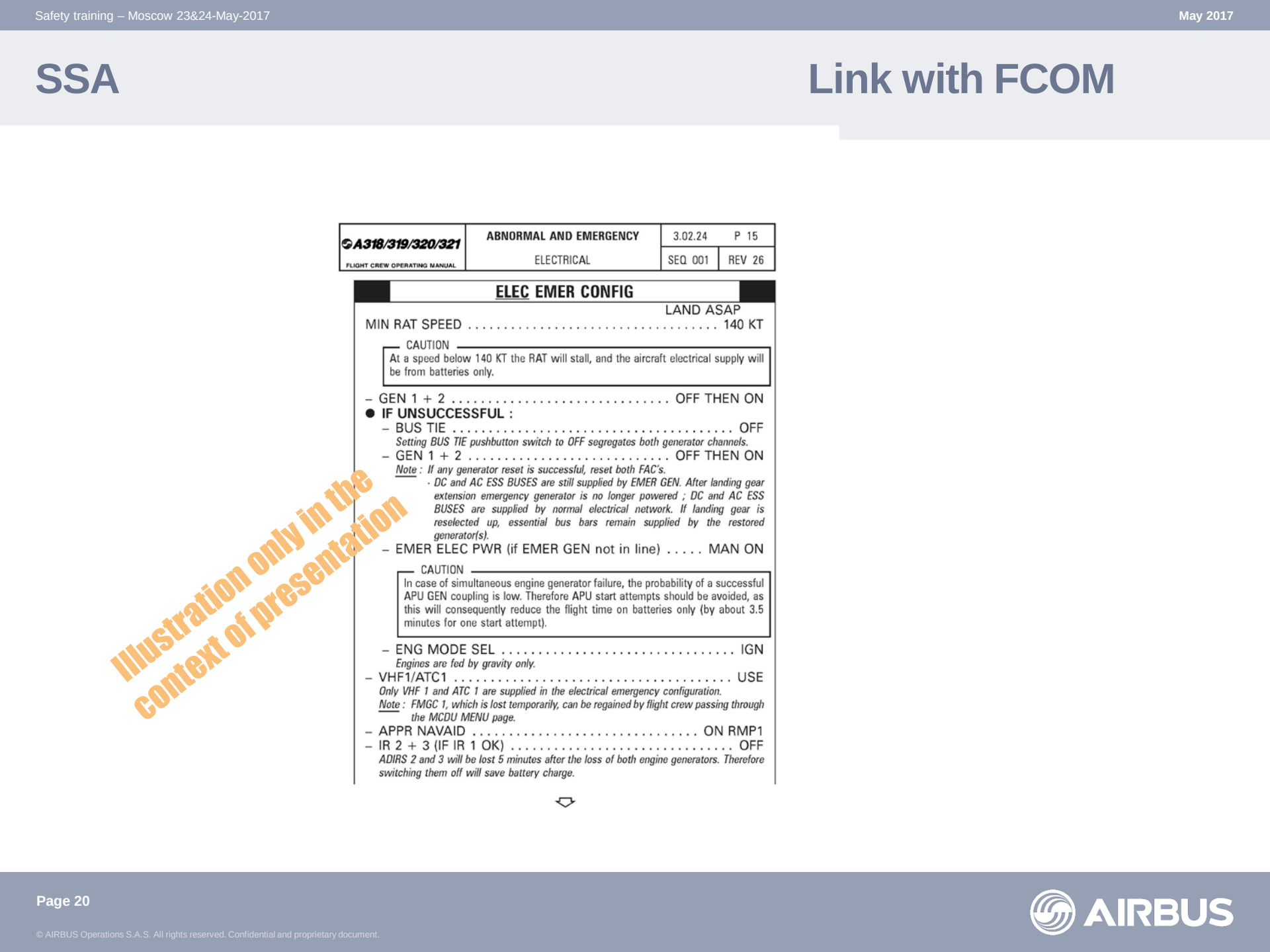
Only VHF 1 and ATC 1 are supplied in the electrical emergency configuration.

Note : FMGC 1, which is lost temporarily, can be regained by flight crew passing through the MCDU MENU page.

– APPR NAVAID ..... ON RMP1

– IR 2 + 3 (IF IR 1 OK) ..... OFF

ADIRS 2 and 3 will be lost 5 minutes after the loss of both engine generators. Therefore switching them off will save battery charge.



SSA

Link with MRB

	MSI REFERENCE	TASK	MSI AND TASK DESCRIPTION	FEC	INTERVAL	ZIP REFERENCE	APPLICABILITY
	24.00.00		ELECTRICAL POWER				
	24.20.00		AC GENERATION				
R		OP	01 OPERATIONAL CHECK OF EMERGENCY GENERATING SYSTEM (THIS TASK COVERS TASKS 24.30.00/01 AND 24.50.00/01)	8	I: 36 HRS (ELAPSED)		A320 PRE 24701 PRE 27189 PRE 28413
R		OP	02 OPERATIONAL CHECK OF STATIC INVERTER (THIS TASK COVERS TASKS 24.30.00/02 AND 24.50.00/02)	8	I: 36 HRS (ELAPSED)		A320 PRE 24701 PRE 28160
		OP	03 OPERATIONAL CHECK OF GPCU VIA CFDS	9	I: 600 FH		PRE 27140 OR POST 34895
		OP	04 READ CFDS FOR CLASS 3 FAULTS	9	I: 600 FH		ALL
		DI	05 CHECK IDG OIL LEVEL AND DIFFERENTIAL PRESSURE INDICATOR	6	I: 150 FH NOTE 5		ALL
		DS	06 DISCARD IDG SCAVENGE FILTER, DRAIN AND REPLENISH OIL SYSTEM	6	I: 800 FH		A318 WITH CFM ENGINES INSTALLED PRE 30352 OR A319 PRE 30352 PRE 30375 OR A320 PRE 30352 PRE 30375 OR A321 PRE 30352 PRE 30375
		FC	07 CHE[illegible] TORQUE OF IDG QAD TENSION BOLT	6	I: 2400 FH		ALL
		OP	08 OPERATIONAL CHECK OF TRANSFER INHIBITION	9	I: 6000 FH		ALL
		OP	09 OPERATIONAL CHECK OF AC ESS GENERATION SWITCHING	9	I: 6000 FH		ALL
			* * * * * C O N T I N U E D * * * * *				
	ISSUE: DEC 01/07		ELECTRICAL POWER		SECTION: C-24		PAGE 1

SSA

Link with AFM

A318/319/320/321 FLIGHT MANUAL	EMERGENCY PROCEDURES	3.02.00 P 05	
		02 MAR 07	REF 300

ELEC – EMER CONFIG (both engine generators failed)

LAND ASAP

Minimum RAT speed : 140 kt
Turn off then on all generators one after the other.

- If no generator reset successful :
  Set BUS TIE to OFF.
  Attempt a further all generators reset.
  - If any generator reset is successful :
    Turn off then on both FACs one after the other.
  - If generator reset still unsuccessful :
    Note : 1. For communications, only VHF 1 and ATC 1 are available.
    2. Flight controls are in alternate law. Refer to F/CTL – ALTN LAW (chapter 4).
R *3. Engines are fed by gravity. Refer to FUEL GRAVITY FEEDING (chapter 4).*
    4. The cockpit door locking system (CDLS) is inoperative (if installed).
    Manually confirm emergency electrical power on.
    Set ENG MODE selector to IGN START.
    Turn off then on FAC 1.
R Set BUS TIE to auto.
R Start APU if available.
    Set ventilation blower and extract to OVRD.
- For approach and landing :
R
R *Note : Slats and flaps extend slowly.*
    Landing distance : multiply by 2.90
R *Note : 1. Antiskid is inoperative. Refer to BRAKES – A/SKID N/WS FAULT or OFF (chapter 4).*
    2. Half spoilers are inoperative.

COMMON CAUSE ANALYSES

- As per ARP4754A / ARP4761(A), the set of Common Causes Analyses consists in:

  - ❑ CMA : Common Mode Analysis
  - ❑ PRA : Particular Risks Analyses
  - ❑ ZSA : Zonal Safety Analyses

- These analyses complement and support the FHA/SSA activities presented above.

COMMON CAUSE ANALYSES - CMA

- CMA is a qualitative analytical method used to support evaluation of independence.
- When performing CMA, engineering experience is systematically applied to review in a logical way the following aspects:
  - Function,
  - Architecture,
  - Development/design,
  - Implementation,
  - Manufacturing,
  - Maintenance and operation.

COMMON CAUSE ANALYSES – PRA (dedicated presentation)

PARTICULAR RISKS ANALYSES

Aim at:

- Analysing the consequences of such an event at A/C level (not necessarily limited to one system and to one zone of the A/C
- Minimising the repercussions due to these hazards

The process for each one includes :

- determination of an approved risk model,
- study of repercussions associated with this model
- Demonstration of compliance with associated requirement or design/installation change request.

COMMON CAUSE ANALYSES – ZSA (dedicated presentation)

ZONAL SAFETY ANALYSES

ZSA is a qualitative safety assessment systematically carried out in each zone of the aircraft

- to check that all system installation and segregation rules are properly applied
- to investigate the potential interferences between systems and between systems and structures
- to assess the potential risk on systems and structures resulting from the maintenance errors and other events not originating from the aircraft.