Development Assurance Level Assignment

Eng.Nelson José Wilmers Júnior
S. J. C. GGCP 22/10/2010

ANAC

Program

- BASIC CONCEPTS AND DEFINITIONS.
- DEVELOPMENT ASSURANCE PROCESS.
- DEVELOPMENT ASSURANCE LEVEL.
- FDAL and IDAL
- FDAL & IDAL ASSIGNMENT PROCESS.
- DAL ASSIGNMENT WITHOUT ARCHITECTURE CONSIDERATIONS.
- DAL ASSIGNMENT WITH ARCHITECTURE CONSIDERATIONS.
- INDEPENDENCE ATRIBUTES.
- FDAL AND IDAL ASSIGNMENT CASES.
- FDAL ASSIGNMENT TAKING CREDIT FOR EXTERNAL EVENTS.

ANAC

BASIC CONCEPTS AND DEFINITIONS

- **Function : The intended behavior of a product based on a defined set of requirements regardless of implementation. A function can exist at aircraft, system or item level.**
- **ITEM: One or more hardware and/or software elements treated as a unit, having bounded and well-defined interfaces.**

ANAC

BASIC CONCEPTS AND DEFINITIONS

- **Failure: An occurrence which affects the operation of a component, part or element such that it can no longer function as intended(this includes both loss of function and malfunction). AC/AMJ nº 25.1309 Arsenal**

ANAC

BASIC CONCEPTS AND DEFINITIONS

- **ERROR: 1. An occurrence arising as a result of an incorrect action or decision by personnel operating or maintaining a system. (EASA AMC 25.1309) 2. A mistake in requirements, design, or implementation.**
- **DEVELOPMENT ERROR: A mistake in requirements determination, design or implementation.**
- **Note: errors may cause Failures, but are not considered to be Failures. (AC/AMC 25.1309)**

ANAC

BASIC CONCEPTS AND DEFINITIONS

- **FAILURE CONDITION: A condition having an effect on the aircraft and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions or external events (AC/AMC 25.1309).**
- **A Failure Condition can be caused by one or more Failures or Errors.**

ANAC

DEVELOPMENT ASSURANCE PROCESS

- **The mitigation of Failures is performed by setting safety qualitative and/or quantitative requirements, including the fail-safe design concept of AC/AMC 25.1309 which influence the system architectures.**
- **Errors are mitigated by implementation of a Development Assurance Process.**

ANAC

DEVELOPMENT ASSURANCE LEVEL

- **The Development Assurance Process establishes confidence that system development has been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.**
- **The Development Assurance Level is the measure of rigor applied to the development process to limit, to a level acceptable for safety, the likelihood of Errors occurring during the development process of Functions (at aircraft level or system level) and Items that have an adverse safety effect .**

FDAL and IDAL

- **FUNTION DEVELOPMENT ASSURANCE LEVEL (FDAL): The level of rigor of development assurance tasks performed to functions**
- **ITEM DEVELOPMENT ASSURANCE LEVEL (IDAL): The level of rigor of development assurance tasks performed to items**

ANAC

FDAL and IDAL

- **The Development Assurance Level of a Function or Item applies not only to the development process of this Function or Item, but also to the development of the interfaces with all the other Functions or Items inter-related to the extent that they may affect the Function or Item being examined.**
- **The assigned development assurance level has no relationship with equipment random hardware failure probabilities, i.e. the probability analysis of the failure condition is still required to demonstrate a compliant design.**

ANAC

FDAL & IDAL Assignment Process

- **The Development Assurance Level assignment process begins with FDAL assignment to the Aircraft Functions, then assigning System functions FDALs and then assigning item IDALs.**

ANAC

Aircraft Level Functions FDAL Assignment

FDAL is assigned to top-level Aircraft Functions, based on its most severe Failure Condition Classification in accordance with Table1. This is performed for Aircraft Function

Top Level Failure Condition Severity Classification	Associated Top Level Function FDAL Assignment
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Table 1

ANAC

System Level Functions FDAL Assignment

- **Once a FDAL is assigned to an Aircraft Function based on the Function's Failure Conditions severity classification, the architecture of the system Functions involved in that Aircraft Function is examined to determine the Development Assurance levels of those system Functions.**

- **There are the following possibilities:**
  - DAL assignment without architecture consideration
  - DAL assignment with architecture considerations

ANAC

DAL assignment without architecture considerations

If a Failure Condition (FC) could result from a possible development error in an Aircraft level, System level or item level (e.g. at Function, sub-function, hardware, software), then the associated Development Assurance process is assigned level according to table 2:

Failure Condition Severity	Associated FDAL/IDAL
Catastrophic	A
Hazardous/Severe Major	B
Major	C
Minor	D
No Safety Effect	E

Table 2

DAL Assignment without Architecture Consideration

- Table 2 can be used to directly assign the FDAL at the same level as the Top-Level Function FDAL, for all Functions and IDAL for all Items in the architecture, supporting the Top Level Function.
- When the mitigation strategy for systematic errors is a single FDAL A development process for a Catastrophic Failure Condition, the the applicant may be required to justify the choice of a single FDAL A and substantiate that the development process for that member has sufficient independent validation/verification activities to ensure that potential development error(s) having a catastrophic effect have been removed or mitigated.

DAL assignment with architectuire considerations

- **The Development Assurance Level is assigned depending on the severity classification of Failure Conditions involved, considering the possible independence between development processes that can limit the consequences of development errors.**

ANAC

DAL assignment with architecture considerations

- **If the Safety Assessment shows that the aircraft or system architecture provides containment for the effects of development or design errors, so that the aircraft-level effects of such errors are sufficiently benign, then development assurance activities can be conducted at a reduced level of process rigor for the functions or items wholly within the architectural containment boundary.**

ANAC

DAL assignment with architecture consideration

- A systematic approach to assigning Development Assurance Levels, when considering system architectures, is to use the concept of Functional Failure Sets (FFS) and Independence.
- FUNCTIONAL FAILURE SET: A single Member or a specific group of Members that are considered to be independent from one another (not necessarily limited to one system) that lead(s) to a top level Failure Condition. Conceptually, for FDAL (and subsequently IDAL) assignment purposes, a FFS is equivalent to a Fault Tree minimal cut set (as defined in ARP4761), whose members represent the result of potential development errors rather than failures. A failure condition may have a single or multiple FFSs.
- MEMBER: An Item or Function that may contain an error causing its loss or anomalous behavior. [This definition is limited to the Functional Failure Set application herein.]
- Safety Assessment techniques are used to identify the FFSs.

ANAC

Independence Atributes

- **Independence atributes**
- **Independence between Functions or Items can protect against potential common mode Errors and is a fundamental attribute to consider when assigning Development Assurance Levels.**
- **The intent of Independence attributes is to have sufficient confidence that the likelihood of a common mode Error is minimized between two or more members at an extent commensurate with the severity of the Failure Condition Classification.**
- **For the purposes of assigning FDAL and IDAL, two types of independence attributes, Functional Independence and Item Development Independence are considered.**

Functional Independence

- **Functional Independence is an attribute where the Functions are different in order to minimize the likelihood of a common requirement Error.**
- **Functional Independence minimizes the likelihood of common sources of error associated with:**
  - **Common requirements errors**
  - **Common requirement interpretation errors**

ANAC

Functional Independence

- **Examples of Functional Independence where different requirements are employed to implement/achieve an aircraft or system level Function :**
- **Decelerate on the ground (wheel brakes, engine thrust reversers and ground spoilers),**
- **Control direction on ground (nose wheel steering, differential braking, and the rudder at high speed),**
- **Control aircraft in the air (flight control surfaces and vectored thrust),**
- **Navigate (GPS and Inertial Reference System),**
- **Provide AOA (vane and synthetic AOA computed from airspeed and inertial data),**
- **Provide Fuel Quantity (engine fuel flow rate and tank fuel probes).**

Item Development Independence

- **Item Development Independence is an attribute where the Items are different in order to minimize the likelihood of a common mode Error between the individually developed Items.**
- **Examples of Errors that may be mitigated by Item Development Independence:**
  - Software development errors
  - Hardware design errors
- **Examples of means to achieve Item Development Independence :**
  - Different technology such as hydraulic vs. electrical power
  - Different operating systems

DAL assignment with architecture considerations

- If a Catastrophic Failure Condition could result from a combination of possible development errors between two or more independently developed functions or items then, At least 1 development process is assigned Level A, or at least 2 independent development processes are assigned Level B, but none lower than the level associated with the most severe individual effects of an error in their development process for all applicable failure conditions and none lower than Level C.

- The Development Assurance process establishing that the two or more independently developed functions or items are in fact independent should remain level A.

DAL assignment with architecture considerations

- If a Hazardous Failure Condition could result from a combination of possible development errors between two or more independently developed functions or items then, At least 1 development process is assigned Level B, or at least 2 independent development processes are assigned Level C, but none lower than the level associated with the most severe individual effects of an error in their development process for all applicable failure conditions and none lower than Level D.

- The Development Assurance process establishing that the two or more independently developed functions or items are in fact independent should remain level B.

DAL assignment with architecture considerations

- If a Major Failure Condition could result from a combination of possible development errors between two or more independently developed functions or items then, At least 1 development process is assigned Level C, or at least 2 independent development processes are assigned Level D, but none lower than the level associated with the most severe individual effects of an error in their development process for all applicable failure conditions .

- The Development Assurance process establishing that the two or more independently developed functions or items are in fact independent should remain level C.

DAL assignment with architecture considerations

- If a Minor Failure Condition could result from a combination of possible development errors between two or more functions or items then, one development assurance process is assigned at least level D ,but none lower than the level associated with the most severe individual effects of an error in their development process for all applicable failure conditions .
- If a No Safety Effect Failure Condition could result from a combination of possible development errors between two or more functions or items then, the development assurance processes are assigned no lower than the level associated with the most severe individual effects of an error in their development process for all applicable failure conditions .

ANAC

DAL assignment with architecture considerations summary table

TOP-LEVEL FAILURE CONDITION CLASSIFICATION	DEVELOPMENT ASSURANCE LEVEL (NOTES 2 & 4)		
	FUNCTIONAL FAILURE SETS WITH A SINGLE MEMBER	FUNCTIONAL FAILURE SETS WITH MULTIPLE MEMBERS	
		OPTION 1 (NOTE 3)	OPTION 2
Column 1	Column 2	Column 3	Column 4
Catastrophic	FDAL A (NOTE 1)	FDAL A for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Members).	FDAL B for two of the Members leading to top-level Failure Condition. The other Member(s) at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level C for the additional Member(s)).
Hazardous/ Severe Major	FDAL B	FDAL B for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).	FDAL C for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions (but no lower than level D for the additional Members).
Major	FDAL C	FDAL C for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	FDAL D for two of the Members leading to top-level Failure Condition. The other Members at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.
Minor	FDAL D	FDAL D for one Member, additional Member(s) contributing to the top-level Failure Condition at the level associated with the most severe individual effects of an error in their development process for all applicable top-level Failure Conditions.	
No Safety Effect	FDAL E	FDAL E	

ANAC

DAL assignment with architecture considerations : notes

- **NOTE 1: When a FFS has a single Member and the mitigation strategy for systematic errors is to be FDAL A alone, then the applicant may be required to substantiate that the development process for that Member has sufficient independent validation/verification activities, techniques and completion criteria to ensure that potential development error(s) having a catastrophic effect have been removed or mitigated.**
- **NOTE 2: It is necessary to stay in the same row no matter the number of functional decompositions performed (e.g. for a Catastrophic Failure Condition any degree of decomposition from a top FDAL A FFS should include at least one FDAL A or two FDAL B Members).**
- **NOTE 3: If there is a large disparity on the numerical availability of the Members in the Functional Failure Set, the higher level FDAL should generally be assigned to the higher availability Member.**
- **NOTE 4: Some classes of 14CFR Part 23 /CS-23 aircraft have FDALs lower than shown in Summary Table . See the current FAA AC23.1309 and equivalent EASA policy for specific guidance.**

ANAC

FDAL and IDAL ASSIGNMENT CASES

- Case 1: Neither Functional nor Item Development Independence
- Case 2:Functonal Independence and Item Development Independence
- Case 3:Functional Independence is claimed but not Item development Independence.
- Case 4: No functional independence but Item development independence.

Neither Functional nor Item Development Independence

- **If there is no Functional Independence and no Item Development Independence, column 2 of Summary Table is used to assign the FDAL and IDAL.**

- **The FDAL and IDAL are the same and are equal to the top-level function FDAL.**

ANAC

Functional Independence and Item Development Independence

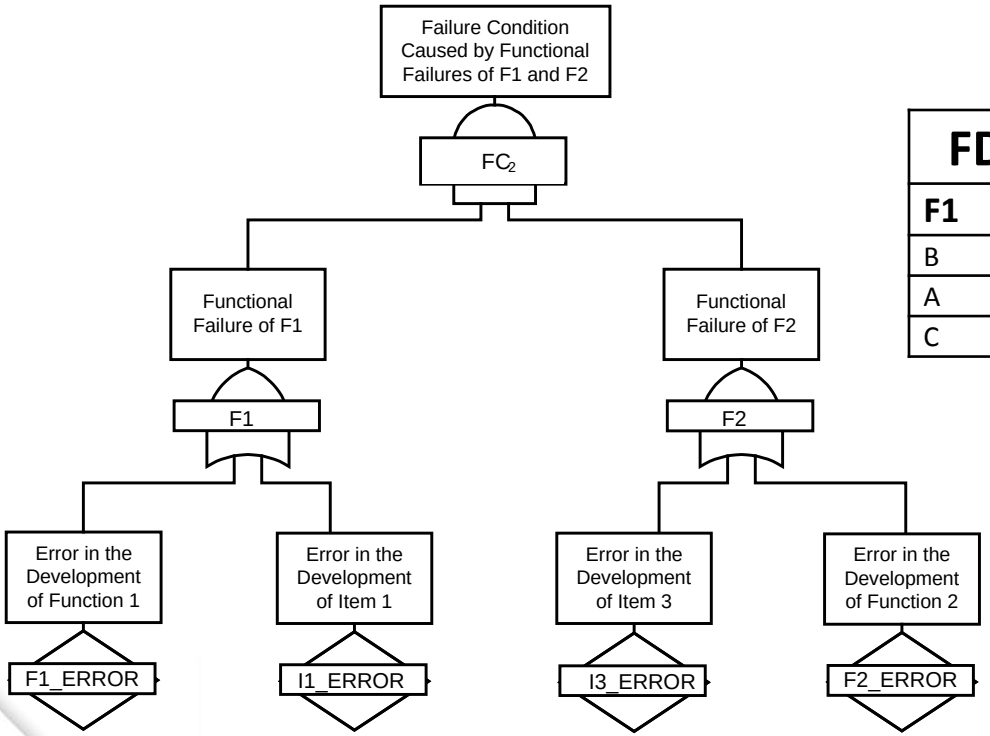
- **If both Functional and Item Development Independence are present, first assign the FDAL using Summary Table and then assign the IDAL using Summary Table (by substituting IDAL to FDAL).**
- **Option 1 or option 2 of the row related to the top-level Failure Condition classification (i.e. same row as FDAL assignment) can be used for the IDAL assignment.**
- **Review of the FFSs representing combinations of errors in both functions and items should be performed to ensure FDAL and IDAL assignments are compliant with the general principles.**

ANAC

Functional Independence and Item Development Independence

FUNCTIONAL FAILURE SETS

- F1 Error & F2 Error
- F1 Error & I3 Error
- I1 Error & I3 Error
- I1 Error & F2 Error



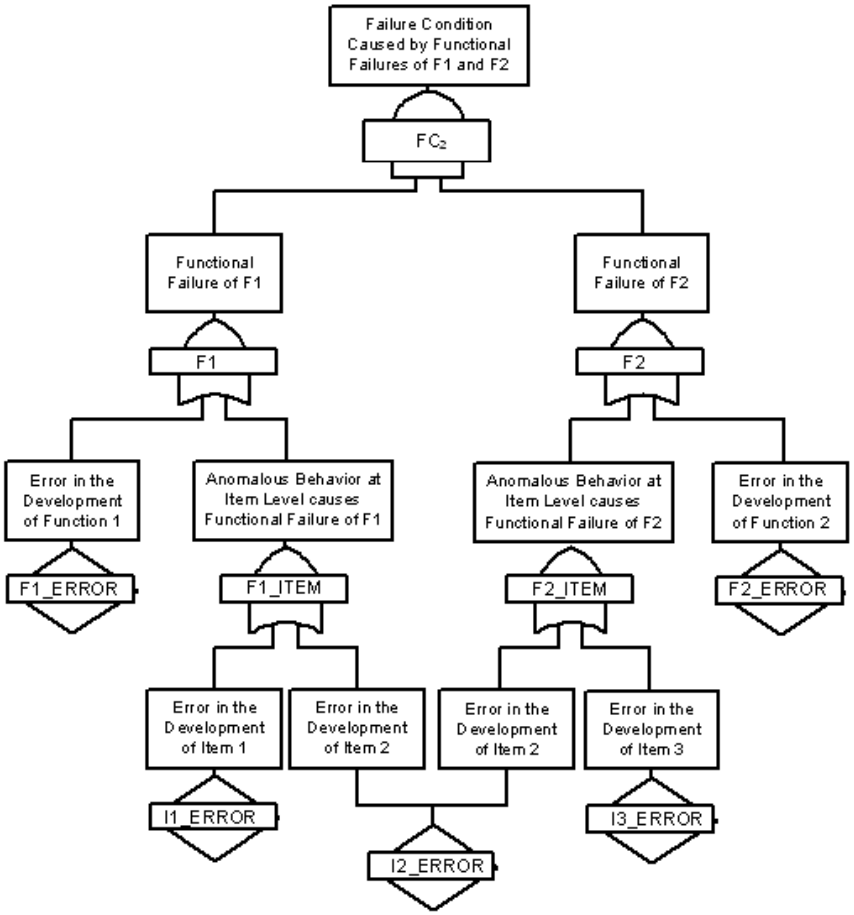
FDAL Assignment		IDAL Assignment	
F1	**F2**	**I1**	**I3**
B	B	B	B
A	C	A	C
C	A	C	A

Functional Independence is claimed but not Item Development Independence

- **If independent Functions are implemented using non-independent Items (or portions of the Items that are not independent), and if an error in the development of the non independent Items can lead to a common mode error between some or all of the Functions, then the IDAL of the "common" non independent Items needs to be assigned the level of the highest FDAL.**
- **The Functions implemented in the common design should be partitioned in order to confirm the Functional Independence claimed for FDAL assignment and to avoid an error in the development process of one Function affecting the other Functions through the common design.**
- **The Development Assurance Level of the partitioning Function should be assigned the FDAL commensurate with the most severe effect of an error in its development; this would be no lower than the highest FDAL of the implemented Functions.**

ANAC

Functional Independence is claimed but not Item Development Independence



FUNCTIONAL FAILURE SETS

- F1 Error & F2 Error
- F1 Error & I3 Error
- I1 Error & F2 Error
- I1 Error & I3 Error
- I2 Error

FDAL Assignment		IDAL Assignment		
F1	F2	I1	I2	I3
B	B	B	A	B
A	C	A	A	C
C	A	C	A	A

ANAC

No functional independence but Item development independence

- **The top-level function is created in one system function which is decomposed into multiple Items that are independent from one another.**
- **The system function FDAL is assigned the top function FDAL as per Table 2. The Item IDALs are assigned using either option 1 or option 2 in the row corresponding to the Top-Level Failure Condition Classification in Summary Table.**

ANAC

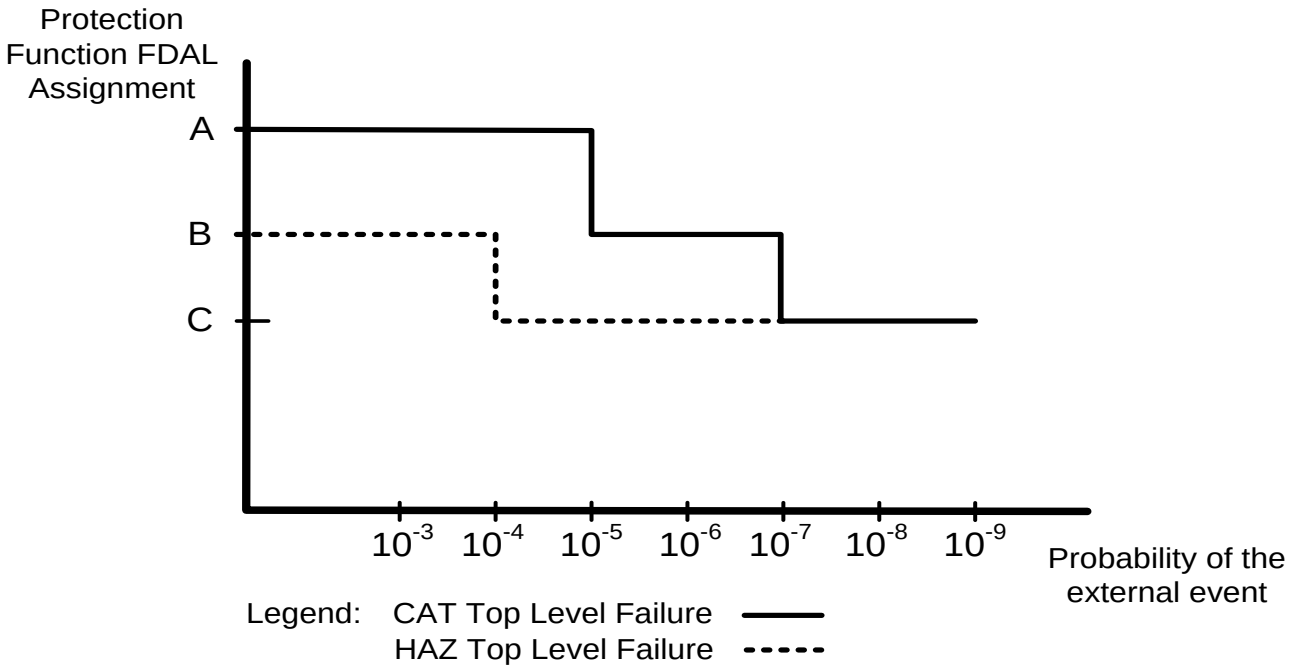
FDAL Assignment Taking Credit for External Events

- For systems that provide protection against an external event to the aircraft design, (e.g. cargo fire), the following guidelines may be applied in cases where no existing guidance material prescribing the associated FDAL exist.
- For Loss of Protection Function (availability failure), the FHA should consider the classification to reflect the reduction of safety margins (none, slight, significant or large) and impact on crew workload. Often the loss of protection alone is a latent failure and has no effect on the aircraft or crew capability to safely complete the mission. The level of reduction in safety margin can be evaluated considering the expected probability of the external event under protection.
- The FDAL of the protection Function can be assigned based on next Figure .

ANAC

FDAL assignment taking credit for external events

FDAL Assignment as Function of the Probability of an External Event



IDAL ASSIGNMENT ADDITIONAL CONSIDERATIONS

- **Non-complex Items (e.g. mechanical parts, relays, electro-mechanical devices, electro valves, servo valves, simple logic devices, etc.) if fully tested or fully analyzed relative to their requirements and identified Failure Conditions may be considered to provide a level of confidence equivalent to IDAL A, provided the design has been validated and verified. - This can be useful when considering their role in relation to other Items or functions in a system to assign the FDALs and IDALs for the functions and complex Items within that system.**

ANAC

THANKS!

ANAC

Agência Nacional de Aviação Civil - Brasil

Regulação
Fiscalização
Segurança Operacional
Aeronavegabilidade
Certificação
Capacitação
Prevenção de Acidentes
Relações Internacionais
Desenvolvimento
Padronização
Homologação
Orientações ao Usuário
Livre Concorrência