RELIABILITY AND REDUNDANCY ALLOCATION ANALYSIS APPLIED TO A NUCLEAR PROTECTION SYSTEM

Alexander Lucas Busse
João M. L. Moreira

INAC - 2019

Summary

➢ Main Objective

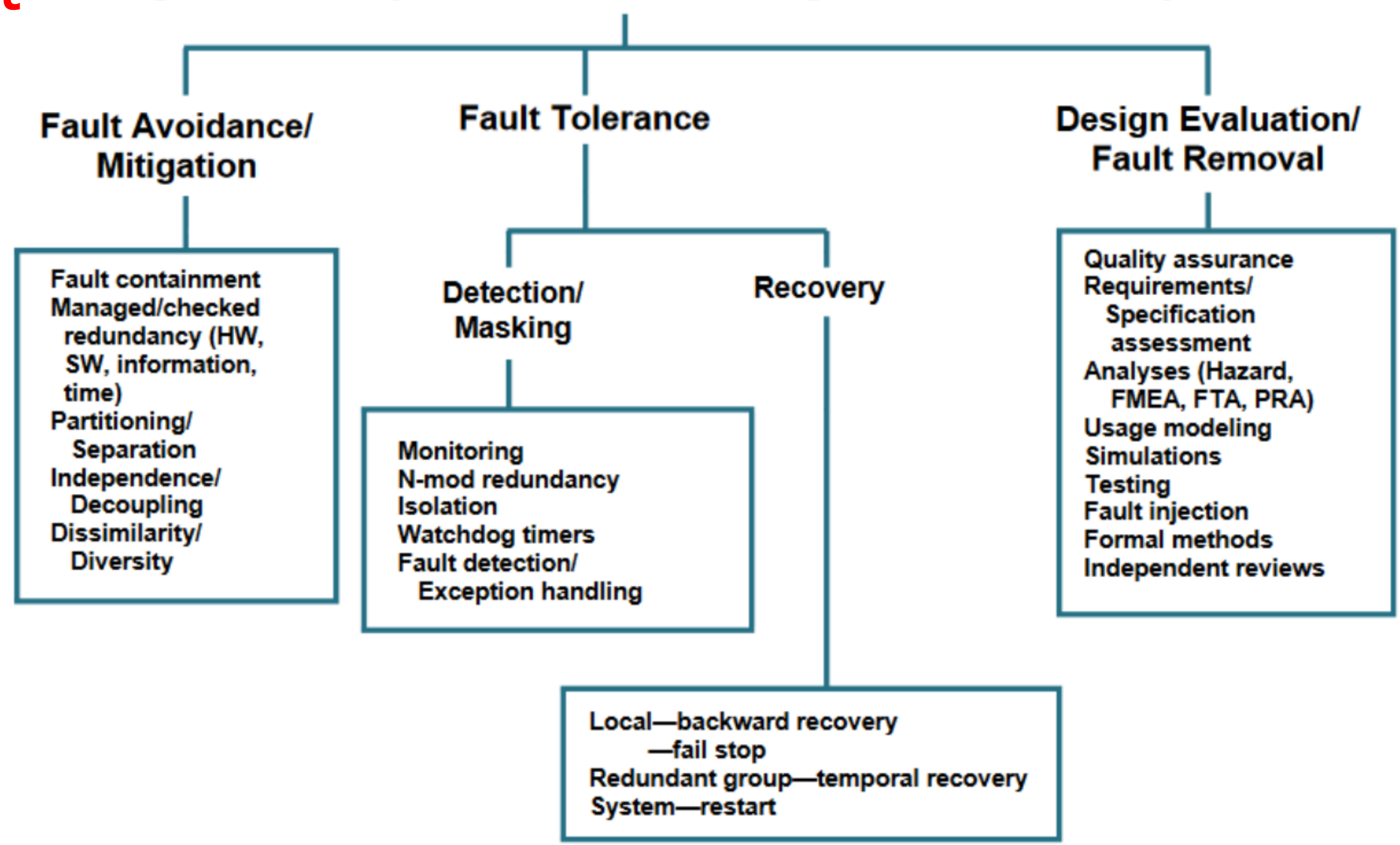
Understand the impacts of using a commercial digital protection system for a nuclear application

Considering:

1. **Nuclear Safety Aspects**
   - **1.1. Reliable Operation,**
   - **1.2. Fault Management.**
2. **Commercial Aspects**
   - **2.1. Financial Viability,**
   - **2.2. National Industry supply capacity.**

1. Context

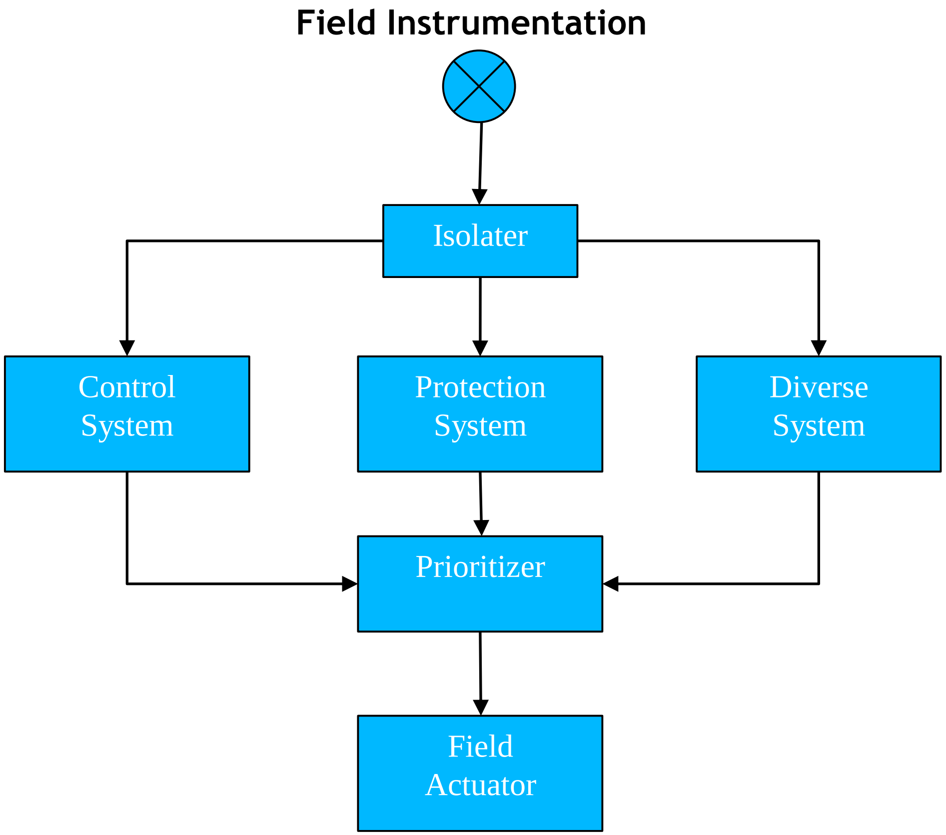
Digital I&C System Fault Management Techniques



NUREG-CR-7007, December 2008

1. Context - Reactor Protection System (RPS)

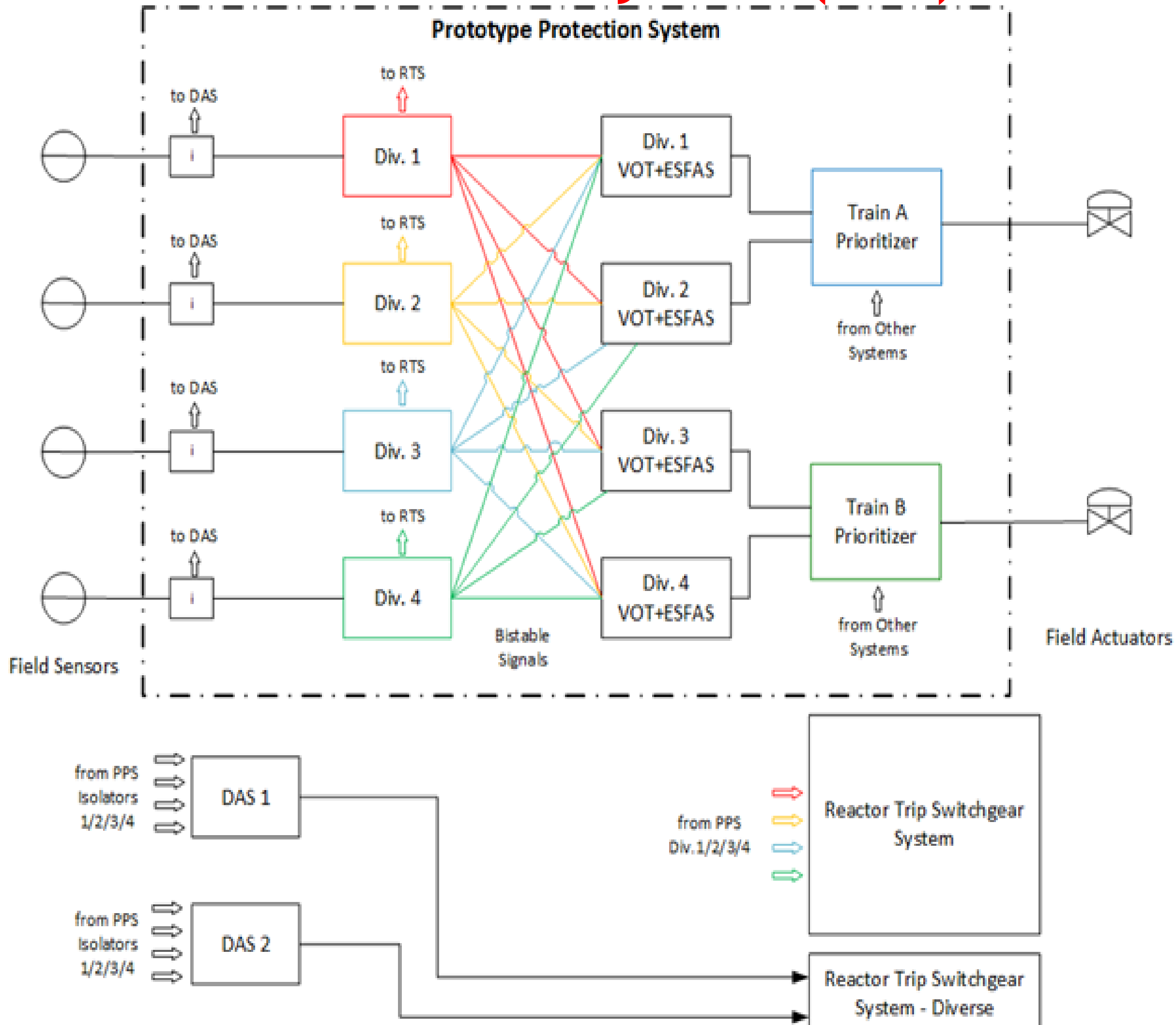
- ✓ RPS is the system that quickly initiates reactor shutdown when important plant parameter values exceed safety levels, these parameters are configurable and characteristic of the design of each plant,
- ✓ This system also initiates the action of Engineered Safety Features Actuation System (ESFAS).



Sensor sharing in Nuclear Power Plants

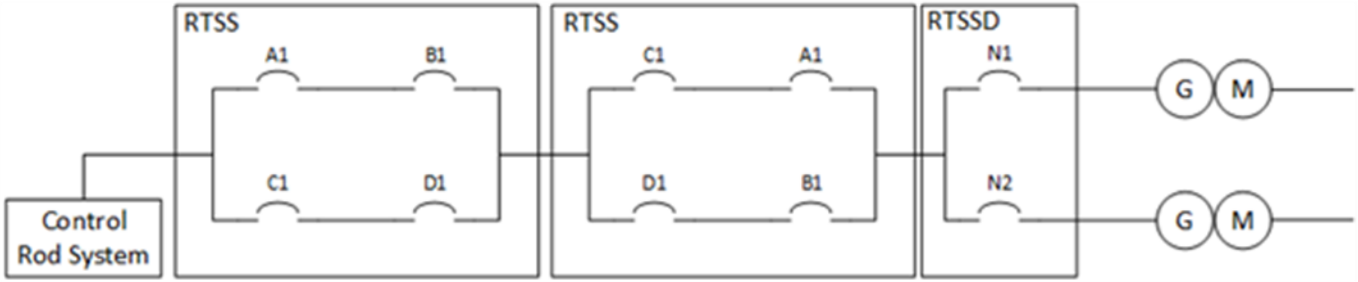
1. Context – Reactor Protection System (RPS)

Standard Architecture



1. Context - Reactor Protection System (RPS)

Standard Architecture



RTSS - *Reactor Trip Switchgear System*
RTSSD – *Reactor Trip Switchgear System Diverse*

Shutdown circuit breakers

1. Context - Reactor Protection System (RPS) - Certification

1. Architecture (how each block relates),
2. Hardware failure modes and failure rate,
3. Systematic failure modes (analysis of tolerance to systematic failures during the life cycle including human errors),
4. Reliability modeling (simulation techniques, RBD, FTA and Markov chain),
5. Reliability Assessment (after lifting the reliability characteristic curves, compare with the acceptance requirements for the architecture).

2. Methodology

- Redundancy and Reliability Allocation Problem (using Reliability Block Diagram methods and BlockSim software from Reliasoft)

- Modeling:

Case 1: The reference RPS

Case 2: RPS plus redundant processing division

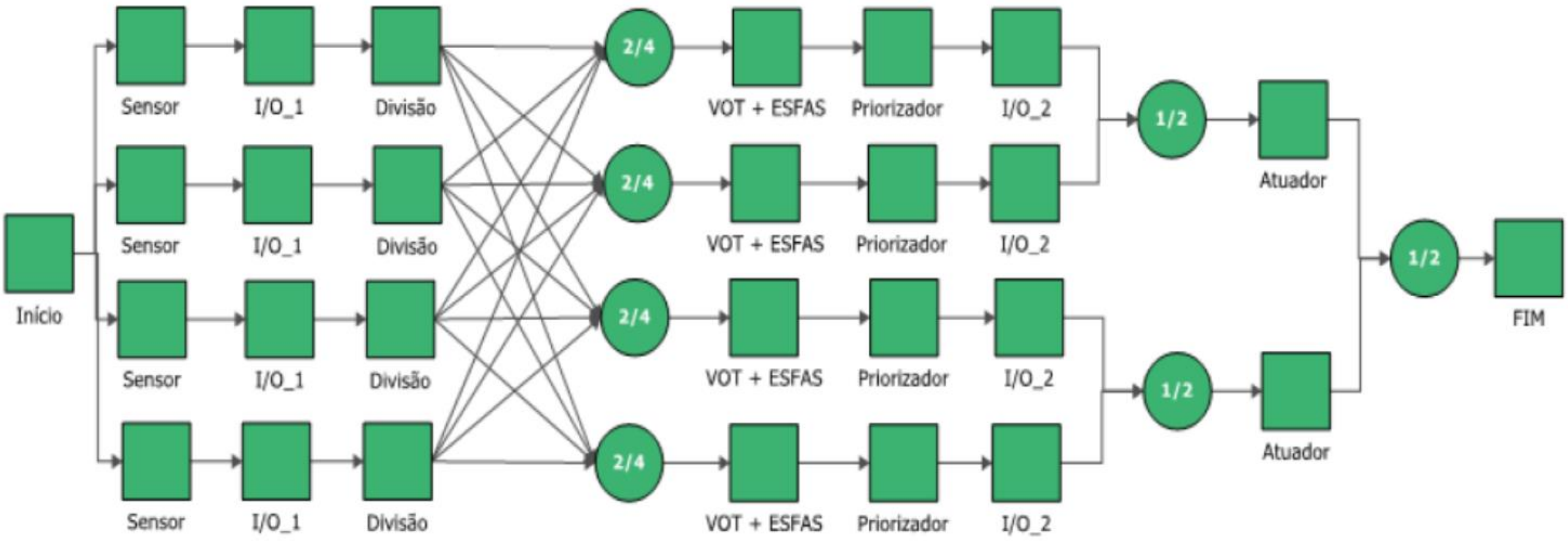
Case 3: RPS plus a complete redundant trip path

Subcases from case 2 and case 3:

(a) voting 2 of 5

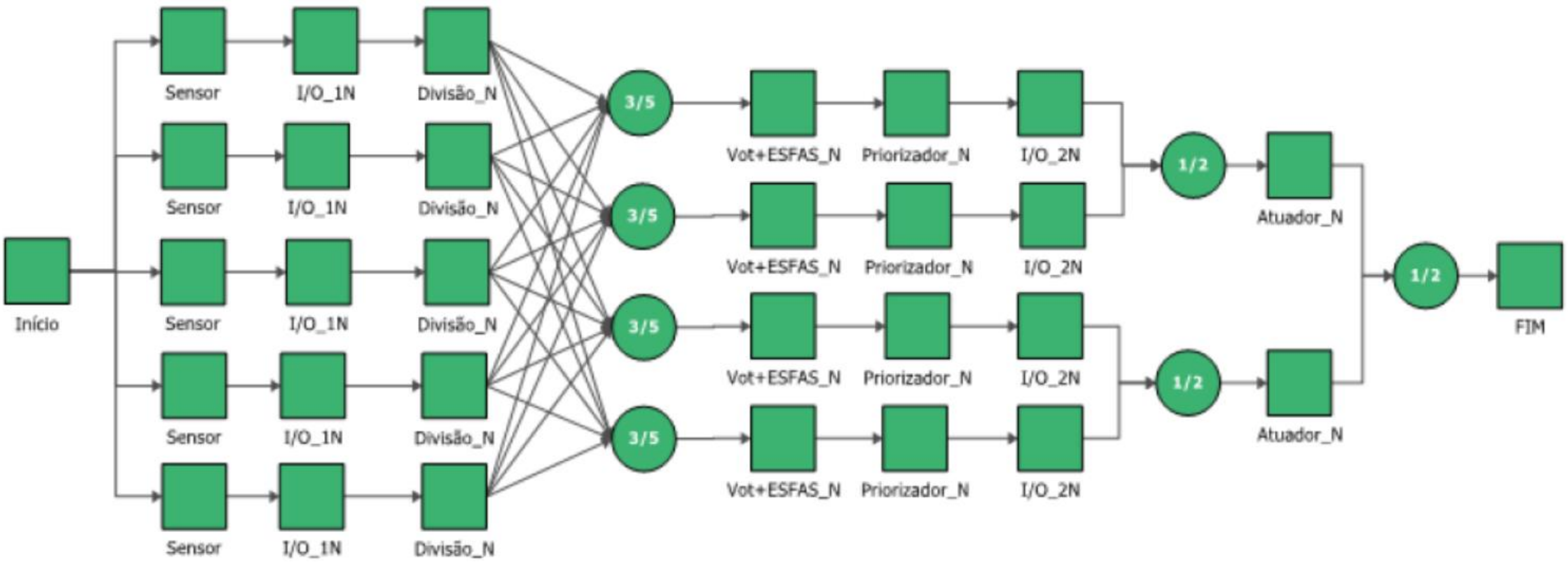
(b) voting 3 of 5

2. Methodology



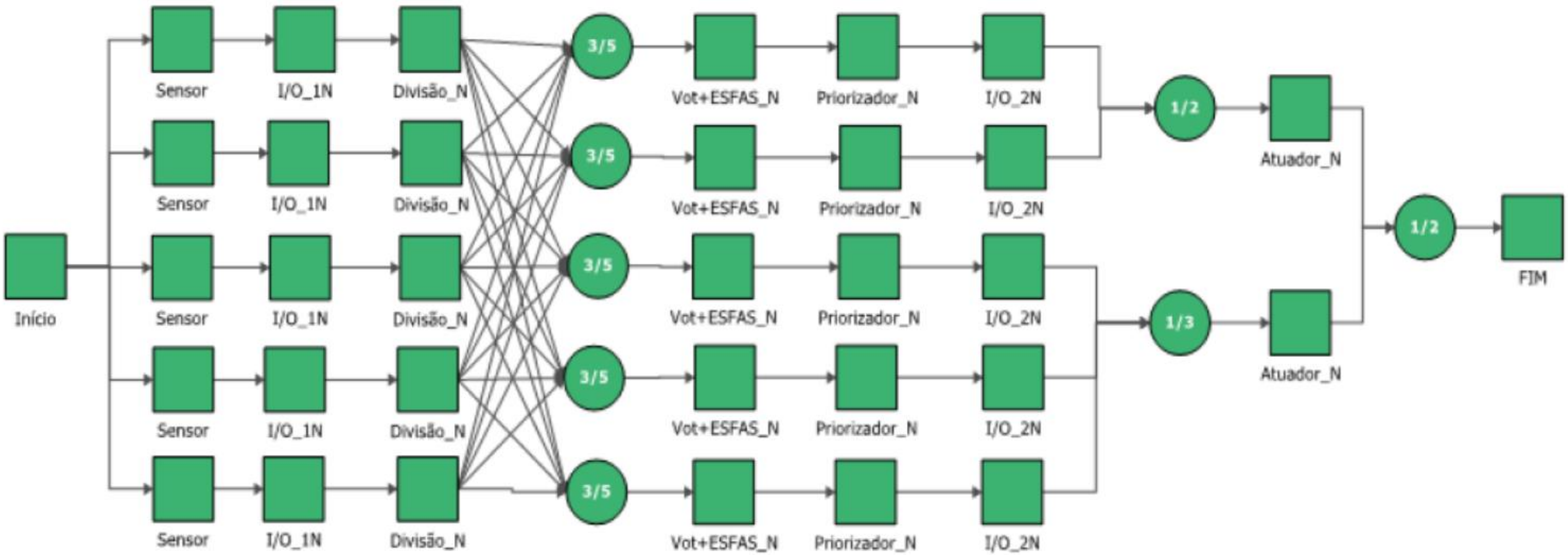
RBD model of the reference architecture

2. Methodology



RBD model plus redundant division

2. Methodology



RBD model plus a complete redundant trip path

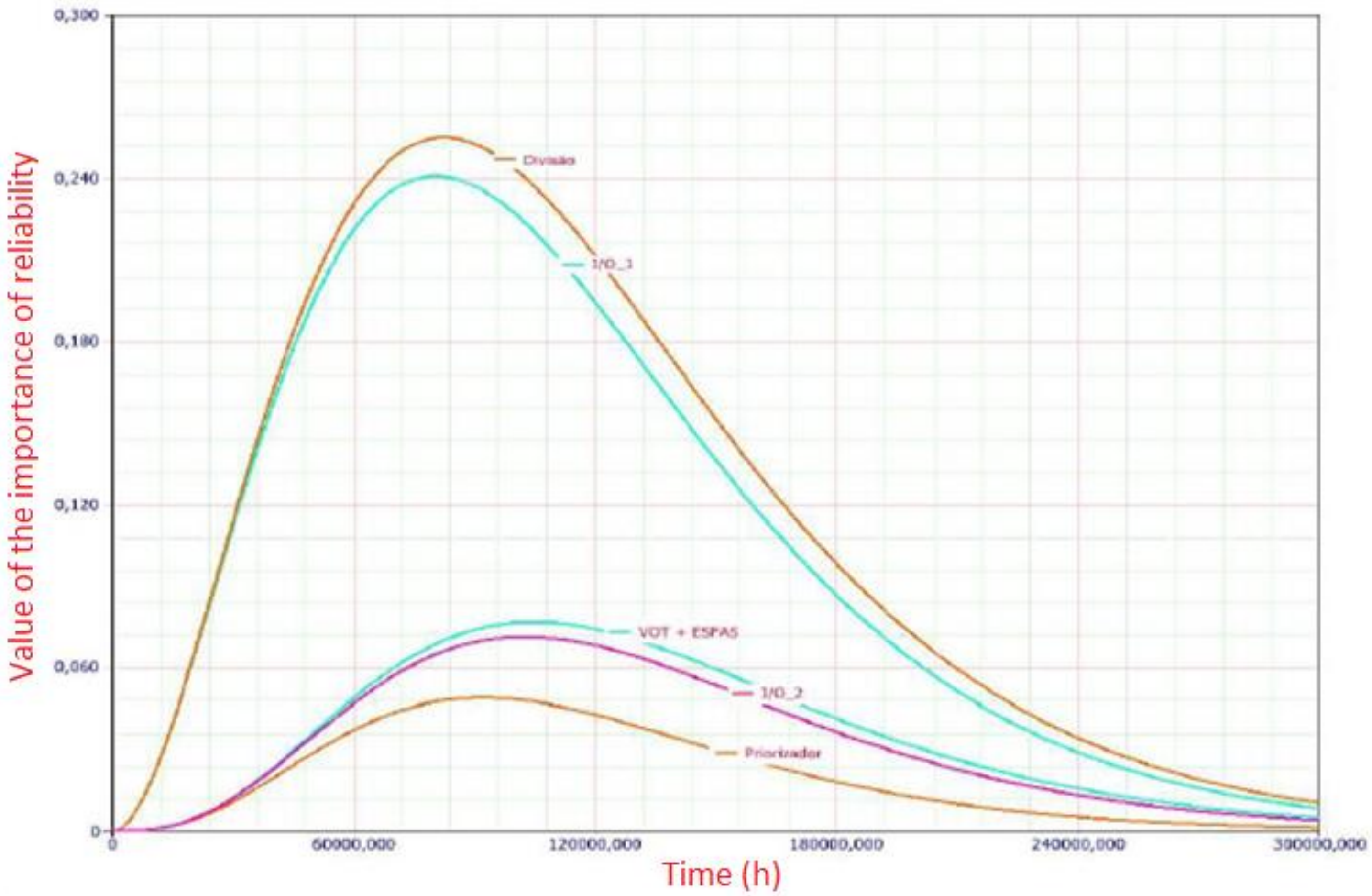
2. Methodology

Equipment	Failure Rate	Life Characteristic	Repair Time	Reference
Pressure Sensor	$1.1\ 10^{-6}$ /h	$9.0\ 10^{+5}$ /h	-	Sensor pressure
I/O	$4.2\ 10^{-6}$ /h	$238.0\ 10^{+3}$ /h	8 h*	ECEFS
Processing Division	$4.9\ 10^{-6}$ /h	$204.0\ 10^{+3}$ /h	8 h	UCEAF
VOT + ESFAS	$4.9\ 10^{-6}$ /h	$204.0\ 10^{+3}$ /h	8 h	UCEAF
Prioriser	$3.4\ 10^{-6}$ /h	$204.0\ 10^{+3}$ /h	3 h	RCEAF
Isolator	$3.7\ 10^{-6}$ /h	$270.0\ 10^{+3}$ /h	8 h*	UEYFO
Safety valve	$7.0\ 10^{-3}$ /d	142/d	-	SOCG

* Considered the value as processing division = 8 h

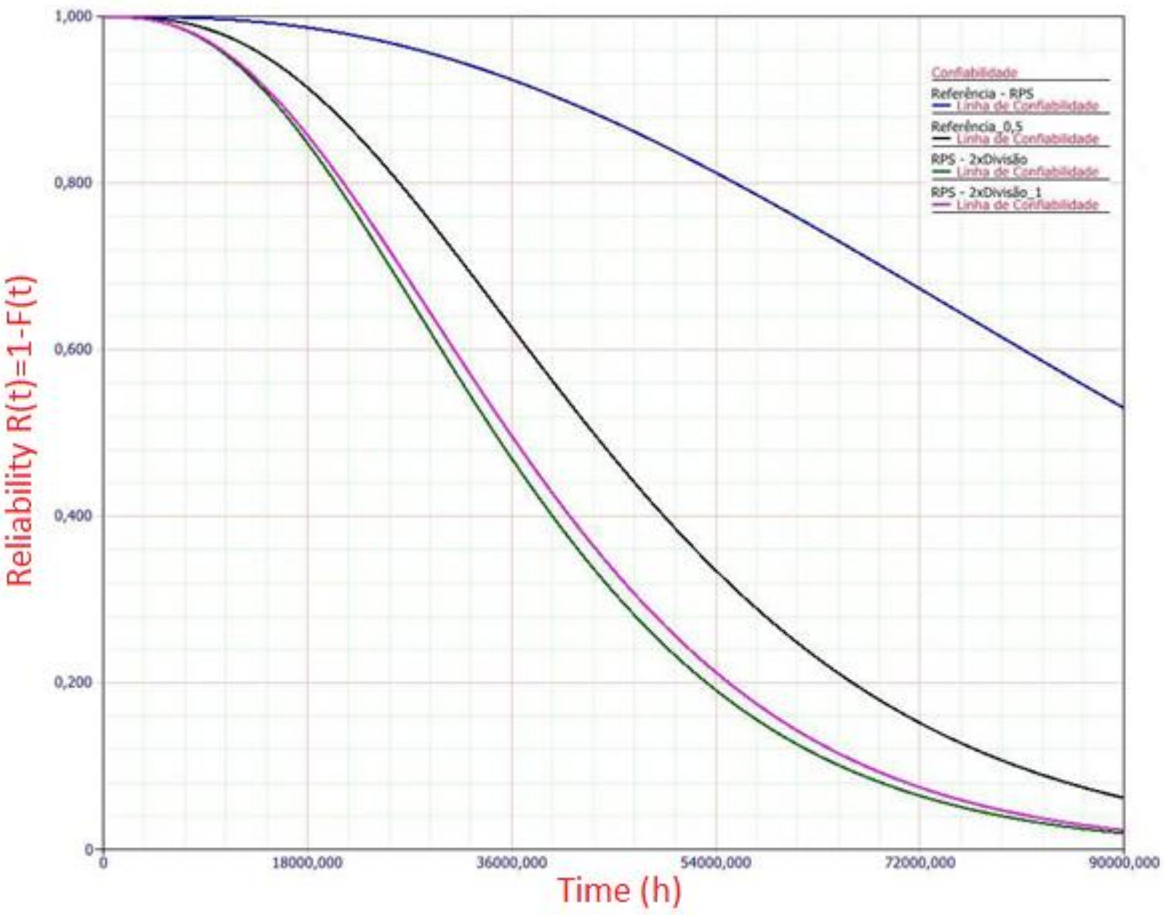
Note: Failure rate values for RPS reference components, for all other cases, the failure rates values, were divided by 2.

3. Results



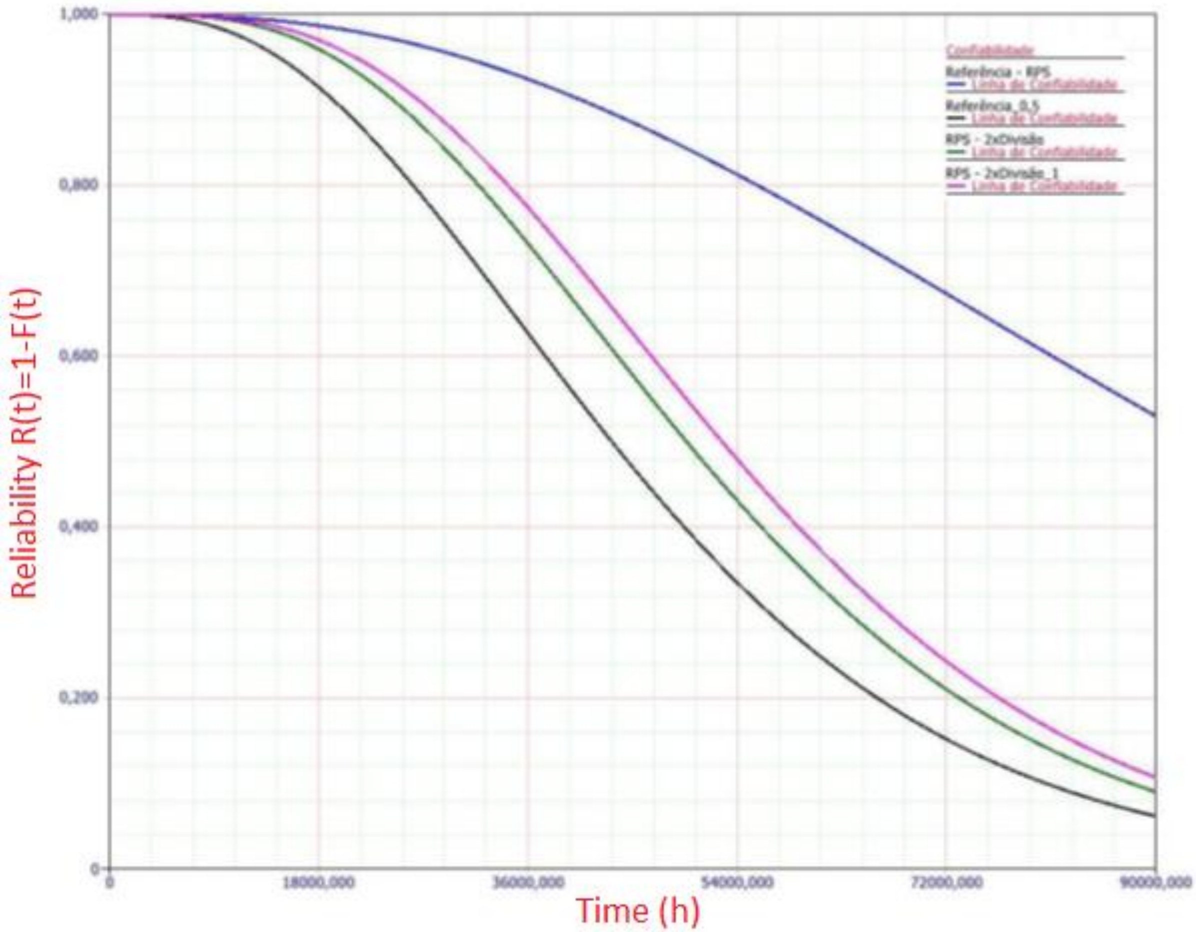
Importance of Reliability components vs time applied to RPS Reference

3. Results



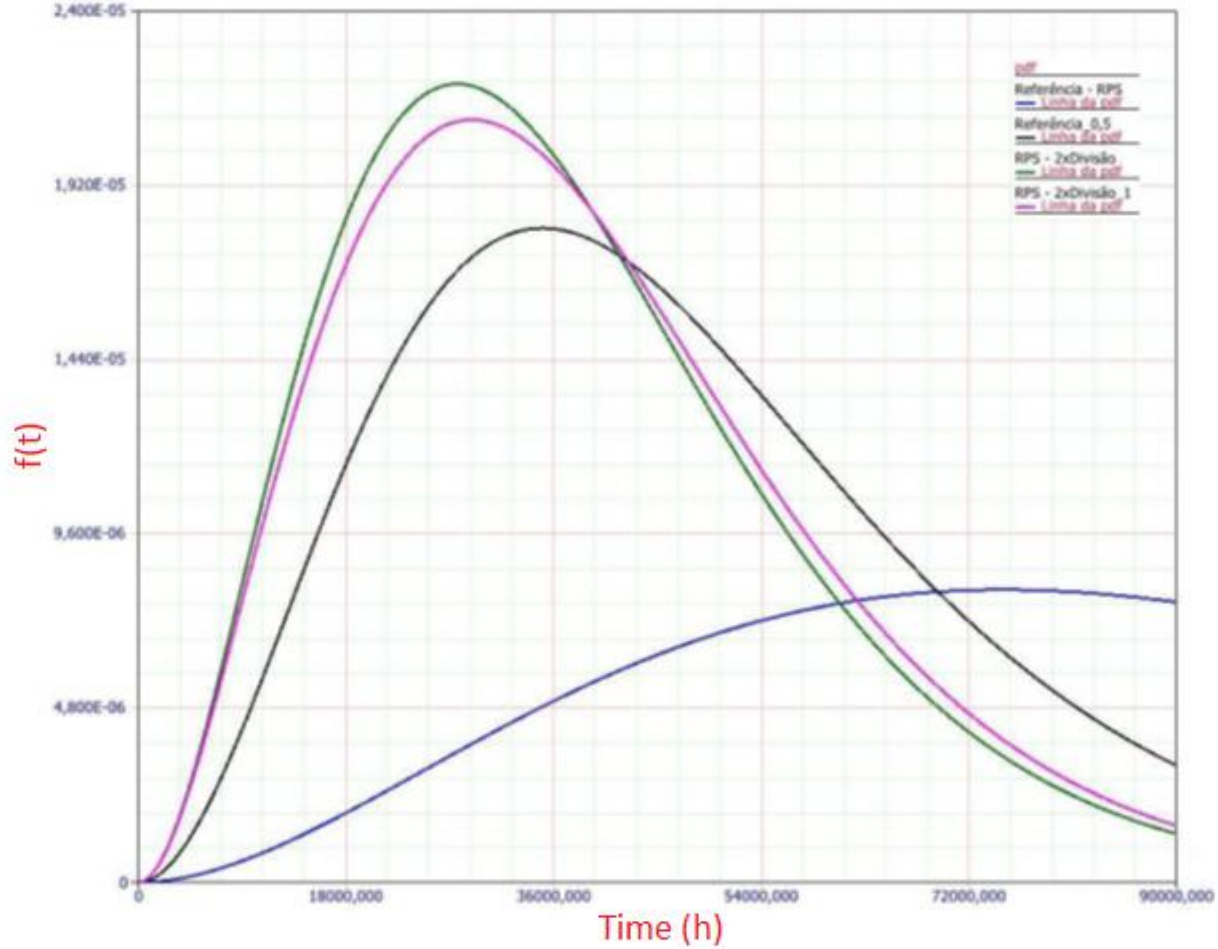
Importance of Reliability vs time applied to Reference (cases “a”)

3. Results



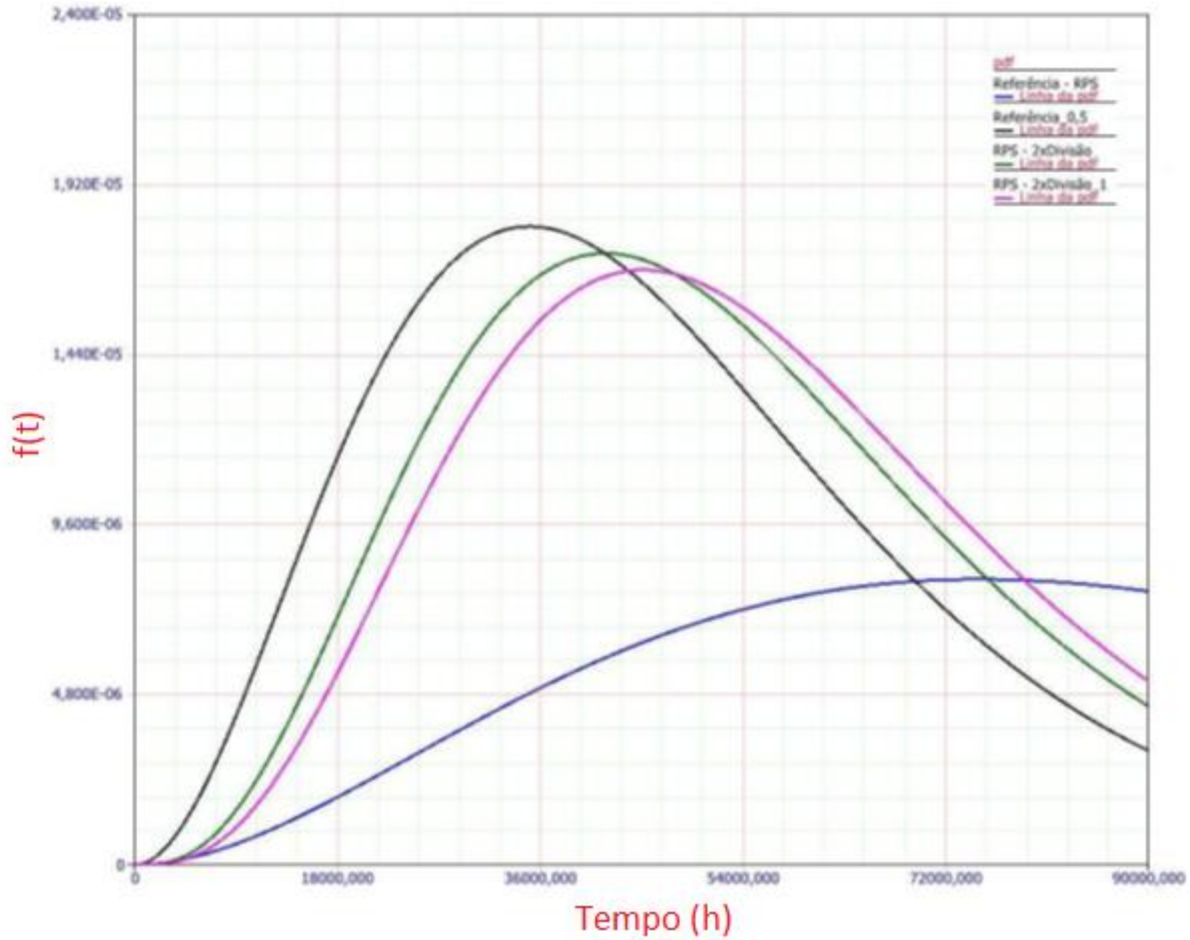
Importance of Reliability vs time applied to Reference (cases “b”)

3. Results



Probability density function vs time applied to Reference (cases “a”)

3. Results



Probability density function vs time applied to Reference (cases “b”)

3. Results

Models	R (1 year)	R (1.5 years)	R (10 years)
Case 1	0.9983	0.9945	0.5486
Case 2.a	0.9732	0.9261	0.0227
Case 2.b	0.9964	0.9854	0.1015
Case 3.a	0.9743	0.9302	0.0278
Case 3.b	0.9976	0.9898	0.1228

Reliability for all cases

4. Conclusions

1. Reliability values over 10 years of operation demonstrated that the difference between cumulative reliability between cases 2 and 3 with respect to reference (case 1) increased exponentially.
2. This divergence may be monitored through periodic self-test procedures, inspections, and preventive maintenance to detect simple failures.
3. The use of spare parts in cases 2 and 3 will be considerably larger than the reference.
4. For a more complete analysis of technical feasibility, we suggest that a RAM (Reliability, Availability and Maintainability) should be made.

5. Acknowledgements

Amazônia Azul Tecnologias de Defesa S.A.

Universidade Federal do ABC

alexlucasb@gmail.com.br

(11)-98649-3306