






Technologies for a safer world

KONATUS

AVALIAÇÃO DE RISCO
UMA COMPARAÇÃO INTERSETORIAL

Por Hygor Potter

NOV 2020

SUMÁRIO








INTRODUÇAO

KONATUS

SOBRE O TEMA

AUTORES

Dr. Guilherme Rocha

- ✓ *Professor do departamento de Eng. Mecânica e Aeronáutica do ITA*
- ✓ *Doutor em Eng. Eletrônica e Computação pelo ITA e Mestre e Graduado em Eng. Mecânica e Aeronáutica pelo ITA*
- ✓ *20+ anos na indústria aeronáutica: Engenharia de Sistemas, Suporte ao Cliente, Confiabilidade e Manutenção*

Salvador Ronconi

- ✓ *Mestre em Eng. Mecânica e Aeronáutica pelo ITA*
- ✓ *Graduado em Eng. Eletrônica pelo IME*
- ✓ *20+ anos na indústria aeronáutica: Engenharia de Sistemas, Suporte ao Cliente, Confiabilidade e Análise de Segurança*
- ✓ *Consultor nas áreas de Sistemas Críticos e Software*

? PALESTRANTE

Hygor Potter

- ✓ *Diretor Comercial & de Marketing da Konatus*
- ✓ *Graduação em Engenharia de Computação pelo ITA*
- ✓ *Especialista em Marketing na Western Asset (mercado financeiro)*
- ✓ *Gerente de Marketing na Captalys (fintech)*
- ✓ *Gerente de Vendas na LACE (eletrônica & tecnologia)*
- ✓ *15+ anos de experiência nos mercados de tecnologia e finanças*

KONATUS

GERENCIAMENTO DE RISCOS

Diferentes mercados, uma só preocupação

- Avaliação qualitativa e quantitativa de riscos: conceito geral
  - ✓ *Feita tanto na fase de projeto quanto na operação de sistemas*
  - ✓ *Pilar básico para assegurar operações com boas margens de segurança*

- Diferentes setores utilizam métodos, processos, ferramentas e taxonomias distintas para tratar a gestão de riscos

- Por meio de uma análise comparativa intersetorial, destacamos semelhanças e diferenças de abordagem
  - ✓ *Base: referências normativas mais utilizadas em cada setor*

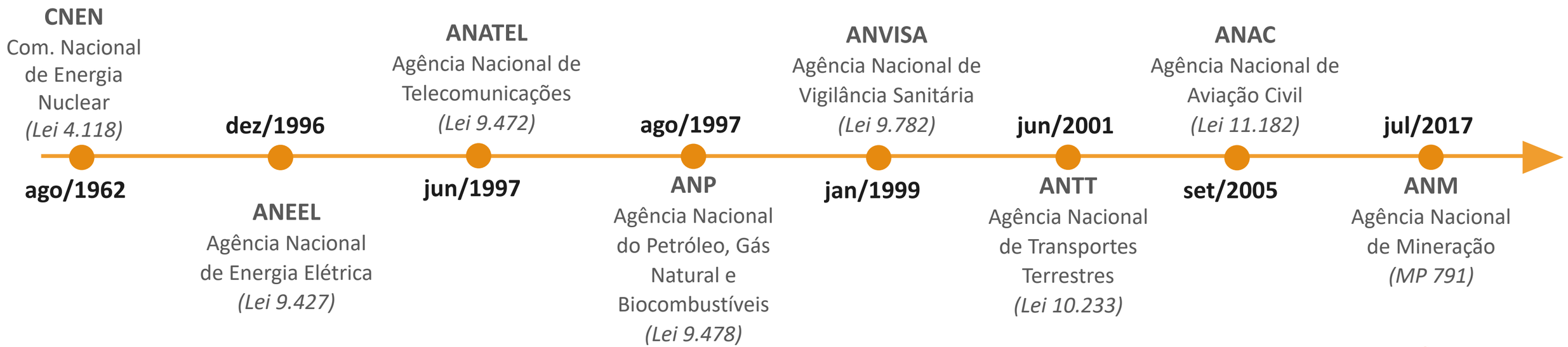
KONATUS

PANORAMA HISTÓRICO

Sistematização de processos no Brasil veio com a criação de órgãos e agências

- Grande contribuição de órgãos normativos e agências reguladoras
  - ✓ *Definição de base regulatória*
  - ✓ *Estabelecimento de meios de cumprimento aceitáveis para gerenciamento de riscos*

- Base regulatória inspirada em regras e normas adotadas por países desenvolvidos
  - ✓ *Adaptações ao cenário brasileiro*
  - ✓ *Participação ativa da comunidade prática via consultas públicas*



NORMAS SETORIAIS

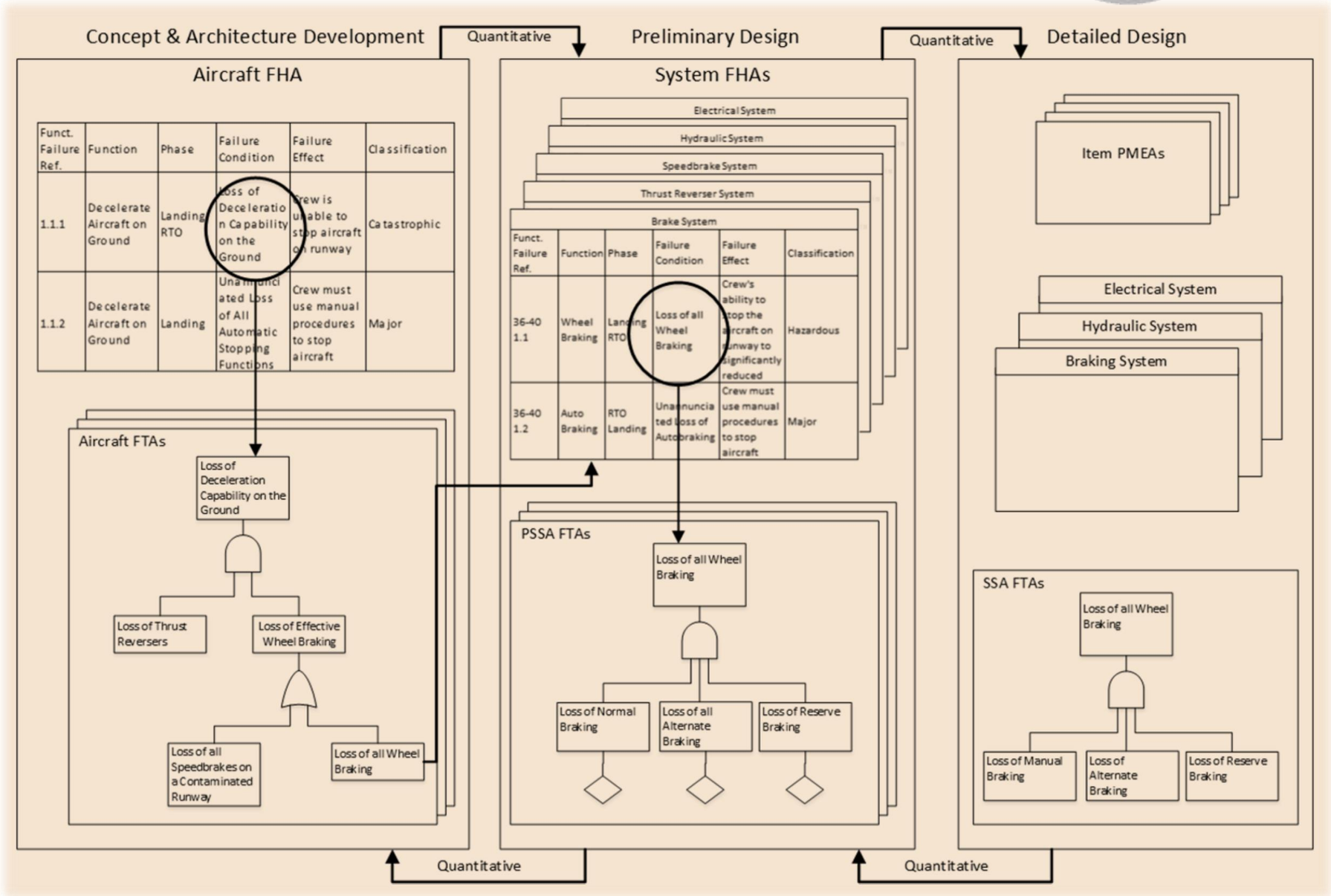
KONATUS

SETOR AERONÁUTICO

Principais normas e ferramentas

SAE-ARP-4761

- Processos e ferramentas de análise de segurança
- Fase de projeto de sistemas aeronáuticos
- Etapas
  - ✓ *FHA (Functional Hazards Assessment)*
  - ✓ *FMEA (Failure Mode and Effect Analysis)*
  - ✓ *FTA (Fault Tree Analysis)*
  - ✓ *CMA (Common Mode Analysis)*
  - ✓ *PRA (Particular Risk Analysis)*
  - ✓ *ZSA (Zonal Safety Analysis)*



Relação entre FHA, FTA e FMEA (SAE-ARP-4761)

SETOR AERONÁUTICO (II)

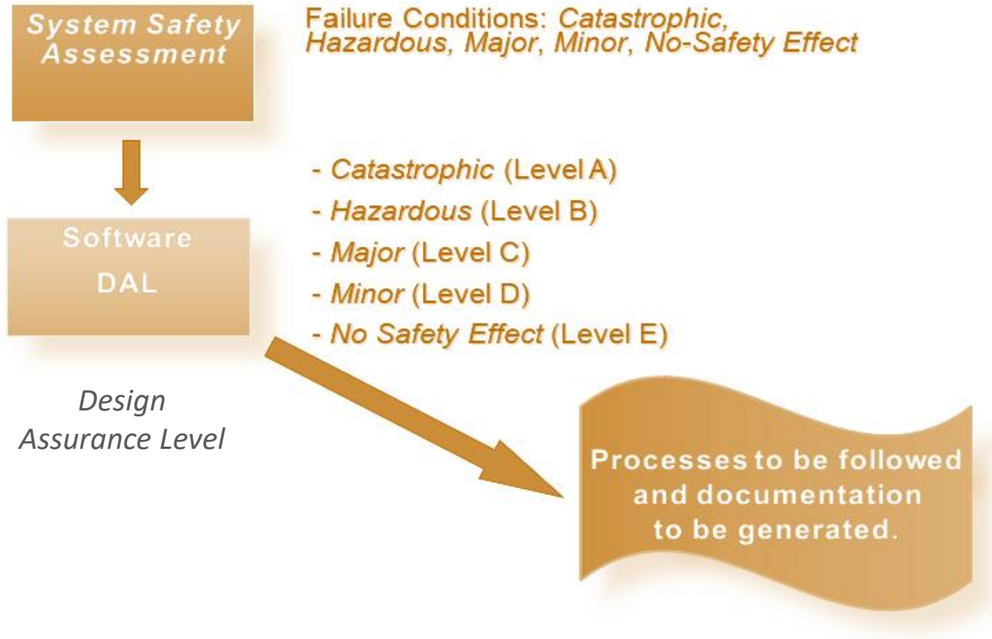
Principais normas e ferramentas

RTCA/DO-178C

- Objetivos processuais de desenvolvimento de software embarcado
  - ✓ *Tão mais rigorosos quanto mais crítica for a falha do referido software*
  - ✓ *Relação direta entre o rigor do desenvolvimento e a avaliação qualitativa de risco associada*

Histórico de revisões da norma RTCA/DO-178

Documento	Conteúdo	Data
DO-178	Definição da documentação mínima de certificação	1980
DO-178A	Aderência aos princípios de Engenharia de Software Introdução do conceito de Verificação e Validação	1985
DO-178B	Detalha os objetivos do processo de desenvolvimento (“O que”), mas não detalha o “Como” atingir tais objetivos.	1992
DO-178C	Inclusão de suplementos que abordam o “Como” *- DO-330/331/332/333*	2011



Nível de rigor de desenvolvimento de software (DAL)

- ✓ *Condição de falha do sistema*
- ✓ *Demanda por evidências de certificação*

KONATUS

SETOR AERONÁUTICO (III)

Principais normas e ferramentas

ICAO Anexo 19 (2013)

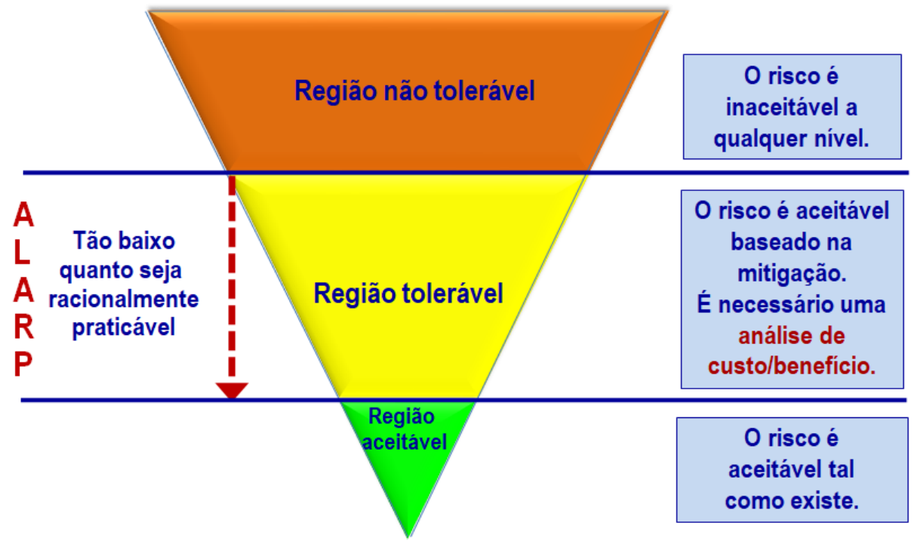
- Processo sistemático de gerenciamento de riscos
  - ✓ *Executado durante a operação de aeronaves*
  - ✓ *Definição de políticas de segurança*
  - ✓ *Gerenciamento de risco*
  - ✓ *Garantia do sistema*
  - ✓ *Promoção da segurança*

- Principal ferramenta: **matriz de avaliação de risco**
  - ✓ *Permite avaliar qualitativamente se um risco é aceitável, tolerável ou não tolerável*
  - ✓ *Uso de estimativas de severidade e probabilidade*

Matriz de avaliação do risco

Probabilidade	Severidade				
	Catastrófico A	Crítico B	Significativo C	Pequeno D	Insignificante E
Frequente 5	5A	5B	5C	5D	5E
Ocasional 4	4A	4B	4C	4D	4E
Remoto 3	3A	3B	3C	3D	3E
Improvável 2	2A	2B	2C	2D	2E
Muito improvável 1	1A	1B	1C	1D	1E

Processo de avaliação do risco - Anexo 19 da ICAO



KONATUS

PETRÓLEO & GÁS

Principais normas e ferramentas

N-2595 (Petrobras)

- Baseada na norma IEC 61511
- Estabelece condições mínimas requeridas para projeto, operação e manutenção de sistemas instrumentados de segurança utilizados na indústria de P&G – os chamados SIS

Taxonomia

- ✓ ***SIS*** *(Safety Instrumented System)*
- ✓ ***IPLFTA*** *(Independent Protection Layer): Fault Tree Analysis*
- ✓ *Falha (fault)*
- ✓ *Estado Seguro (safe state)*
- ✓ ***SIF*** *(Safety Instrumented Function)*
- ✓ *Falha sistemática (systematic failure)*
- ✓ *Redundância*
- ✓ *Risco & risco tolerável (tolerable risk)*

Processos & Ferramentas

- ✓ ***LOPA*** *(Layers of Protection Analysis)*
- ✓ ***PHA*** *(Process Hazard Analysis)*
- ✓ ***HAZOP*** *(Hazards and Operability Study)*
- ✓ ***SIL*** *(Safety Integrity Level): definição*

Etapas Processuais

- ✓ *Hazard Analysis*
- ✓ *Risk Evaluation*
- ✓ *Protection Layers*
- ✓ *SIS Design*
- ✓ *Factory Acceptance Test*

KONATUS

INDUSTRIAL & AUTOMOTIVO

Principais normas e ferramentas

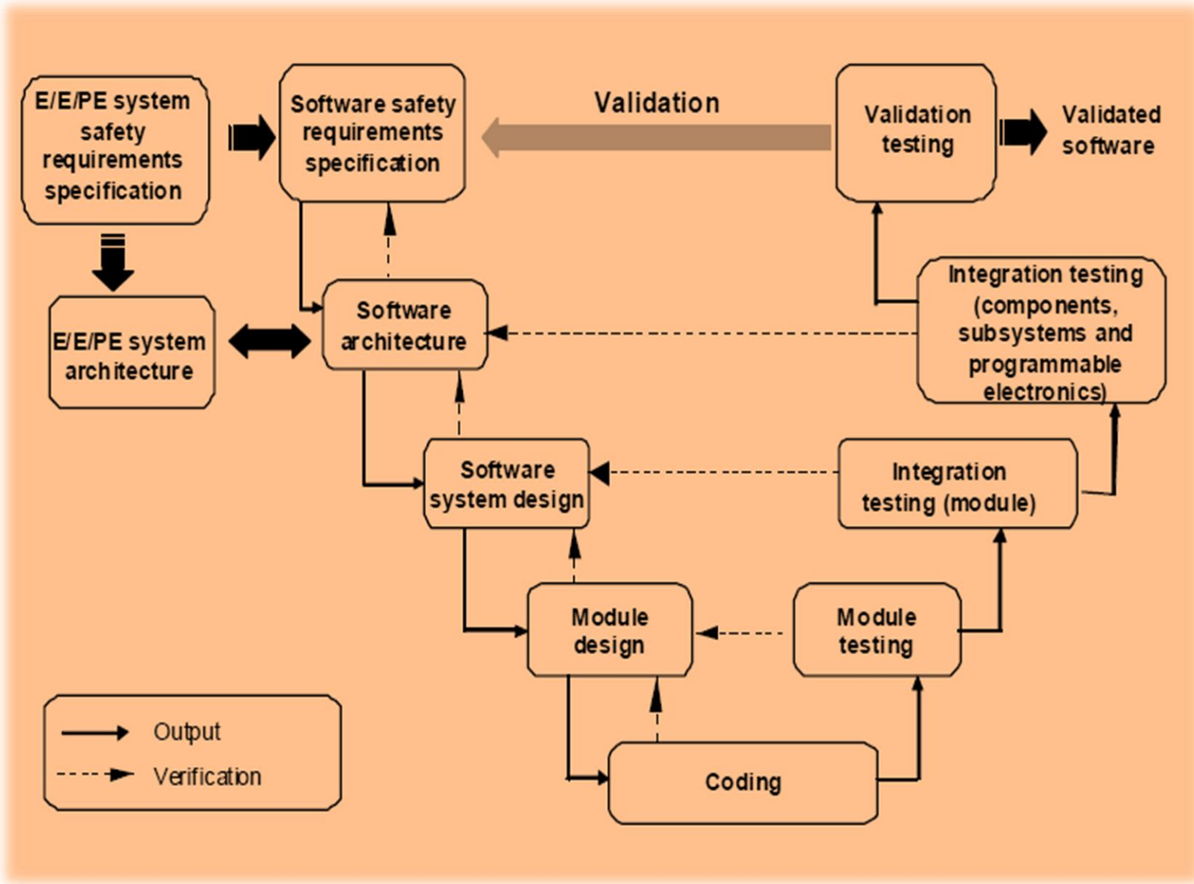
IEC 61508

- Processo de desenvolvimento para dispositivos eletroeletrônicos programáveis que possam colocar em risco a segurança do sistema
- ISO 26262: Adaptação da norma ao setor automotivo
- Quanto mais crítica a programação (software embarcado), maior o rigor processual demandado...
  - ✓ *Mais baixa deve ser a probabilidade média de falhas*
  - ✓ *Mais alto o fator de redução de risco (RRF – Risk Reduction Factor)*
  - ✓ *Maior o SIL (Safety Integrity Level)*

Processos Recomendados

1. *Software safety requirements specification*
2. *Validation plan for software aspects of system safety*
3. *Software design and development*
   - *software architecture*
   - *detailed design and development*
   - *code implementation*
   - *software module testing*
   - *software integration testing*
4. *Software operation and modification procedures*
5. *Software aspects of system safety validation*
6. *Software modification*
7. *Software verification*

Processo de desenvolvimento de software - norma IEC 61508



KONATUS

MINERAÇÃO

Principais normas e ferramentas

NR 22 (ANM & Min. Trabalho)

- Fiscalização de Segurança e Saúde Ocupacional na Mineração
  - ✓ *Primeira versão: jul/78; última atualização: abr/19*

- Disciplina os preceitos a serem observados na organização e no ambiente de trabalho
  - ✓ *Tornar compatível o planejamento e o desenvolvimento da atividade mineira*
  - ✓ *Busca permanente da segurança e saúde dos trabalhadores*
  - ✓ *Implantação de um **PGR específico***

- Aplicável a todos os ambientes
  - ✓ *Minerações subterrâneas e a céu aberto*
  - ✓ *Garimpos e atividades de beneficiamentos minerais*
  - ✓ *Realização de pesquisa mineral*

Cabe à empresa ou Permissionário de Lavra Garimpeira elaborar e implementar um Programa de Gerenciamento de Riscos - PGR, incluindo, no mínimo, aspectos relacionados a:

a) riscos físicos, químicos e biológicos;
b) atmosferas explosivas;
c) deficiências de oxigênio;
d) ventilação;
e) proteção respiratória;
f) investigação e análise de acidentes do trabalho;
g) ergonomia e organização do trabalho;
h) riscos decorrentes do trabalho em altura, em profundidade e em espaços confinados;
i) riscos decorrentes da utilização de energia elétrica, máquinas, equipamentos, veículos e trabalhos manuais;
j) equipamentos de proteção individual de uso obrigatório;
l) estabilidade do maciço;
m) plano de emergência e
n) outros resultantes de modificações e introduções de novas tecnologias.

O PGR deve incluir as seguintes etapas:

a) antecipação e identificação de fatores de risco, levando-se em conta, inclusive, as informações do Mapa de Risco, quando houver;
b) avaliação dos fatores de risco e da exposição dos trabalhadores;
c) estabelecimento de prioridades, metas e cronograma;
d) acompanhamento das medidas de controle implementadas;
e) monitorizarão da exposição aos fatores de riscos;
f) registro e manutenção dos dados por, no mínimo, vinte anos e
g) análise crítica do programa, pelo menos, uma vez ao ano, contemplando a evolução do cronograma, com registro das medidas de controle implantadas e programadas.

KONATUS

OUTROS SETORES

Principais normas e ferramentas

Saúde: IEC 62304

- Processo de desenvolvimento de software para equipamentos médicos críticos
  - ✓ *Diretamente relacionada com requisitos da ANVISA*
  - ✓ *Equipamentos médicos são classificados nas categorias I, II, III e IV, de acordo com o risco à saúde do paciente (I: mais severo)*

Espacial: NBR ISO 17666

- Princípios e requisitos para o gerenciamento do risco integrado em um programa espacial
- Esclarece o necessário para implementar política de gerenciamento do risco integrada a um projeto
  - ✓ *Processo geral de gerenciamento do risco subdividido em 4 passos básicos e 9 tarefas.*
  - ✓ *Aplicação pode ser adaptada às condições específicas de cada projeto*

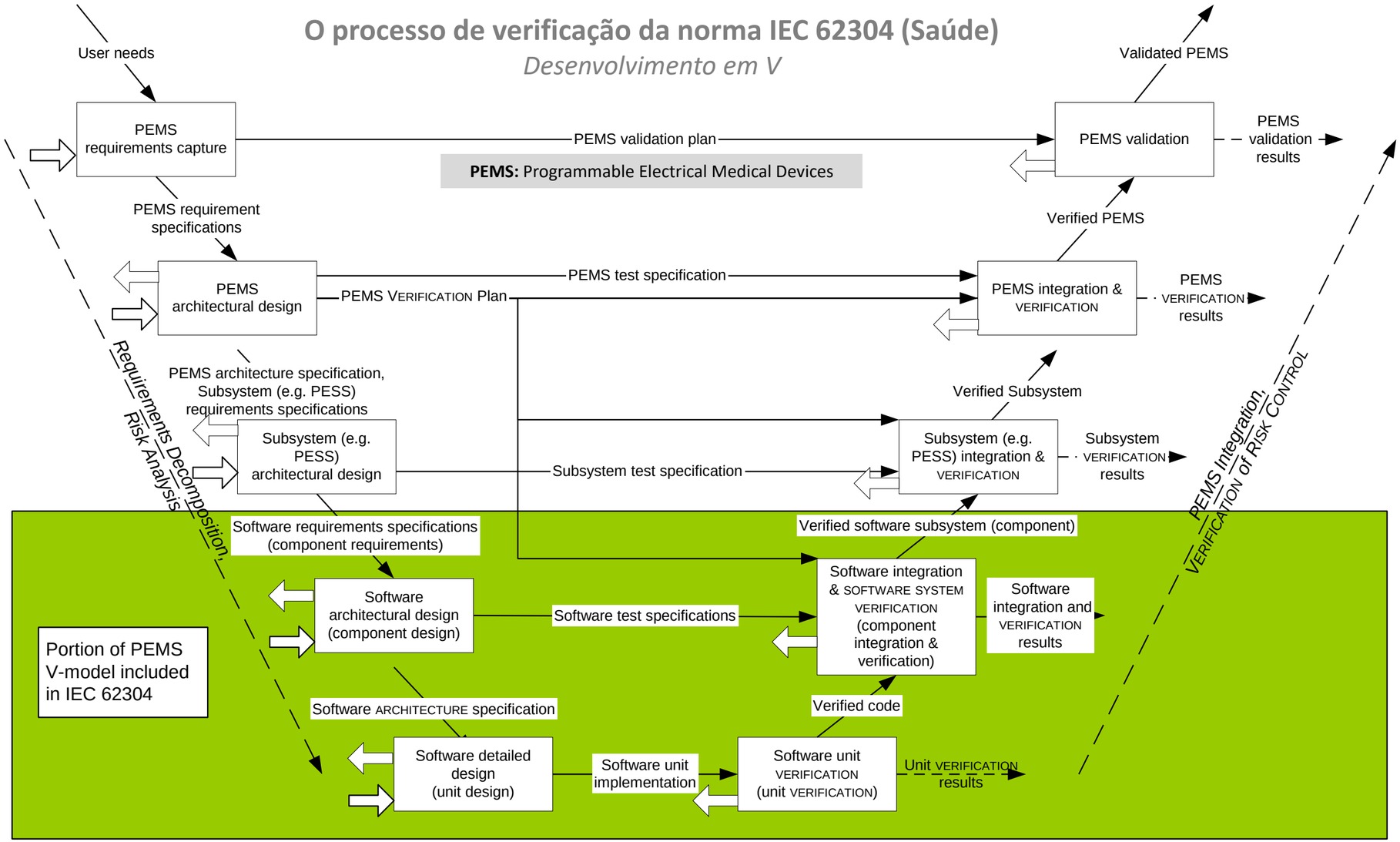
Nuclear: CNEN NE 1.26

- Requisitos mínimos para operação de usinas nucleoelétricas
  - ✓ *Condução sem risco indevido à saúde*
  - ✓ *Segurança da população e do meio ambiente*
- Organização operadora precisa desenvolver, aplicar e permanentemente aperfeiçoar um modelo de gerenciamento do risco
  - ✓ *Modelo deve estar associado às diversas configurações operacionais, sem estar prescrito*
- Os requisitos de projeto dessas instalações são definidos em conformidade com a IEC 61513

KONATUS

OUTROS SETORES (II)

Principais normas e ferramentas



DESDE 2015

Usado pela ANVISA como principal guia para adequação de projeto

KONATUS

CONCLUSOES

KONATUS

COMPARATIVO

Abordagem de ferramentas e processos para projeto & operação de sistemas críticos

SETOR	PROJETO		OPERAÇÃO	
	Ferramentas	*Processos*	*Ferramentas*	*Processos*
Aeronáutico	SAE-ARP-4761 (FMEA, FTA)	• SAE-ARP-4761 (FHA, CMA, PRA, ZSA) • RTCA/DO-178C (objetivos conforme o DAL)	ICAO Anexo 19 (matriz de avaliação do risco, suportada por monitoramento de dados)	ICAO Anexo 19 (ações mitigatórias e tolerabilidade ao risco)
Petróleo & Gás	N-2595 (determinação do SIL)	N-2595 (LOPA, PHA, HAZOP)	N-2595 (HAZOP, risk evaluation)	N-2595 (ações mitigatórias e tolerabilidade ao risco)
Industrial & Automotivo	IEC 61508 / ISO 26262 (compatibilização SIL-RRF)	IEC 61508 / ISO 26262 (objetivos conforme o SIL)	-	-
Mineração	-	-	NR 22 (mapa de risco, avaliação dos fatores de risco)	NR 22 (PGR)
Saúde	-	IEC 62304 (objetivos conforme a categoria)	ISO 14971 (matriz de avaliação do risco)	ISO 14971 (ações mitigatórias e tolerabilidade ao risco)
Espacial	-	NBR ISO 17666 (gerenciamento de risco integrado no projeto)	-	-
Nuclear	-	IEC 61513 (requisitos de projeto instalativo)	-	CNEN NE 1.26 (gerenciamento de risco)

KONATUS

COMPARATIVO (II)

Quanto à avaliação de riscos, verificam-se muitas similaridades intersetoriais...

- Taxonomia comum entre os diversos setores, com poucas carências de harmonização

SETOR	PROJETO		OPERAÇÃO	
	Ferramentas	Processos	Ferramentas	Processos
Aeronáutico	SAE-ARP-4761 (FMEA, FTA)	• SAE-ARP-4761 (FHA, CMA, PRA, ZSA) • RTCA/DO-178C (objetivos conforme o DAL)	ICAO Anexo 19 (matriz de avaliação do risco, suportada por monitoramento de dados)	ICAO Anexo 19 (ações mitigatórias e tolerabilidade ao risco)
Petróleo & Gás	N-2595 (determinação do SIL)	N-2595 (LOPA, PHA, HAZOP)	N-2595 (HAZOP, risk evaluation)	N-2595 (ações mitigatórias e tolerabilidade ao risco)
Industrial & Automotivo	IEC 61508 / ISO 26262 (compatibilização SIL-RRF)	IEC 61508 / ISO 26262 (objetivos conforme o SIL)	-	-
Mineração	-	-	NR 22 (mapa de risco, avaliação dos fatores de risco)	NR 22 (PGR)
Saúde	-	IEC 62304 (objetivos conforme a categoria)	ISO 14971 (matriz de avaliação do risco)	ISO 14971 (ações mitigatórias e tolerabilidade ao risco)
Espacial	-	NBR ISO 17666 (gerenciamento de risco integrado no projeto)	-	-
Nuclear	-	IEC 61513 (requisitos de projeto instalativo)	-	CNEN NE 1.26 (gerenciamento de risco)

COMPARATIVO (III)

...mas também notam-se contrastes, com um setor em vantagem

- Taxonomia comum entre os diversos setores, com poucas carências de harmonização
- Desbalanceamento quanto ao uso de técnicas e ferramentas de análise
  - ✓ ***Setor aeronáutico: estágio mais avançado***
  - ✓ *Emprego das melhores práticas tanto qualitativas quanto quantitativas de gerenciamento de riscos*

SETOR	PROJETO		OPERAÇÃO	
	Ferramentas	Processos	Ferramentas	Processos
Aeronáutico	SAE-ARP-4761 (FMEA, FTA)	• SAE-ARP-4761 (FHA, CMA, PRA, ZSA) • RTCA/DO-178C (objetivos conforme o DAL)	ICAO Anexo 19 (matriz de avaliação do risco, suportada por monitoramento de dados)	ICAO Anexo 19 (ações mitigatórias e tolerabilidade ao risco)
Petróleo & Gás	N-2595 (determinação do SIL)	N-2595 (LOPA, PHA, HAZOP)	N-2595 (HAZOP, risk evaluation)	N-2595 (ações mitigatórias e tolerabilidade ao risco)
Industrial & Automotivo	IEC 61508 / ISO 26262 (compatibilização SIL-RRF)	IEC 61508 / ISO 26262 (objetivos conforme o SIL)	-	-
Mineração	-	-	NR 22 (mapa de risco, avaliação dos fatores de risco)	NR 22 (PGR)
Saúde	-	IEC 62304 (objetivos conforme a categoria)	ISO 14971 (matriz de avaliação do risco)	ISO 14971 (ações mitigatórias e tolerabilidade ao risco)
Espacial	-	NBR ISO 17666 (gerenciamento de risco integrado no projeto)	-	-
Nuclear	-	IEC 61513 (requisitos de projeto instalativo)	-	CNEN NE 1.26 (gerenciamento de risco)

CONSIDERAÇÕES FINAIS

Oportunidades de melhoria passam por maior intercâmbio

- Enorme potencial de avanço no estudo de métodos e ferramentas para avaliação *quali & quant* de riscos
  - ✓ ***Compartilhamento de experiências entre profissionais de diferentes setores***
  - ✓ *Estímulo ao desenvolvimento de cultura de segurança e normatização*
  - ✓ *Treinamento e capacitação de pessoas*
  - ✓ *Fortalecimento da comunidade que estuda e trabalha com sistemas críticos à segurança*
  - ✓ *Maior interação entre indústria e comunidade acadêmica*

KONATUS

REFERÊNCIAS

[1] SAE, SAE-ARP-4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, SAE, US (1996);

[2] RTCA, RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification, RTCA, US (2011);

[3] ICAO, ANNEX 19 Safety Management, ICAO, US (2013);

[4] PETROBRAS, N-2595 REV C. Critérios de Projeto e Manutenção para Sistemas Instrumentados de Segurança em Unidades Industriais, PETROBRAS, BRASIL (2012);

[5] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61511 Functional safety - Safety instrumented systems for the process industry sector, IEC, SUÍÇA (2016);

[6] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), IEC, SUÍÇA (2010);

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 26262 Road vehicles – Functional safety, ISO, SUÍÇA (2011);

[8] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 62304 Medical device software – software life cycle processes, IEC, SUÍÇA (2015);

[9] COMISSÃO NACIONAL DE ENERGIA NUCLEAR, CNEN NE 1.26 Segurança na operação de usinas nucleoelétricas, CNEN, BRASIL (1997);

[10] INTERNATIONAL ELECTROTECHNICAL COMISSION, IEC 61513 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC, SUÍÇA (2011);

[11] ABNT, NBR ISO 17666 Sistemas Espaciais – Gerenciamento do risco, ABNT, BRASIL (2012);

[12] MINISTÉRIO DO TRABALHO E EMPREGO, NR 22 Saúde e Segurança Ocupacional na Mineração, MTE, BRASIL (2019).

KONATUS








Conatus [koh-**ney**-*tuh* s]

(latim) *substantivo, plural* **co·na·tus**

1. esforço ou empenho.
2. força ou tendência simulando um esforço humano.
3. (Segundo a filosofia de Espinosa) inclinação inata de uma coisa para continuar a existir e se aprimorar, podendo ser a mente, a matéria ou uma combinação de ambos.

Qualquer tendência, impulso ou esforço direcionado de forma natural. É uma das três partes da mente, junto com o afeto e a cognição. Em resumo, a parte cognitiva do cérebro mede a inteligência, a afetiva lida com emoções e **a conativa concilia esses pensamentos e sentimentos no intuito de nos orientar como agir com relação a eles.**

Fonte: Merriam-Webster, Wikipédia

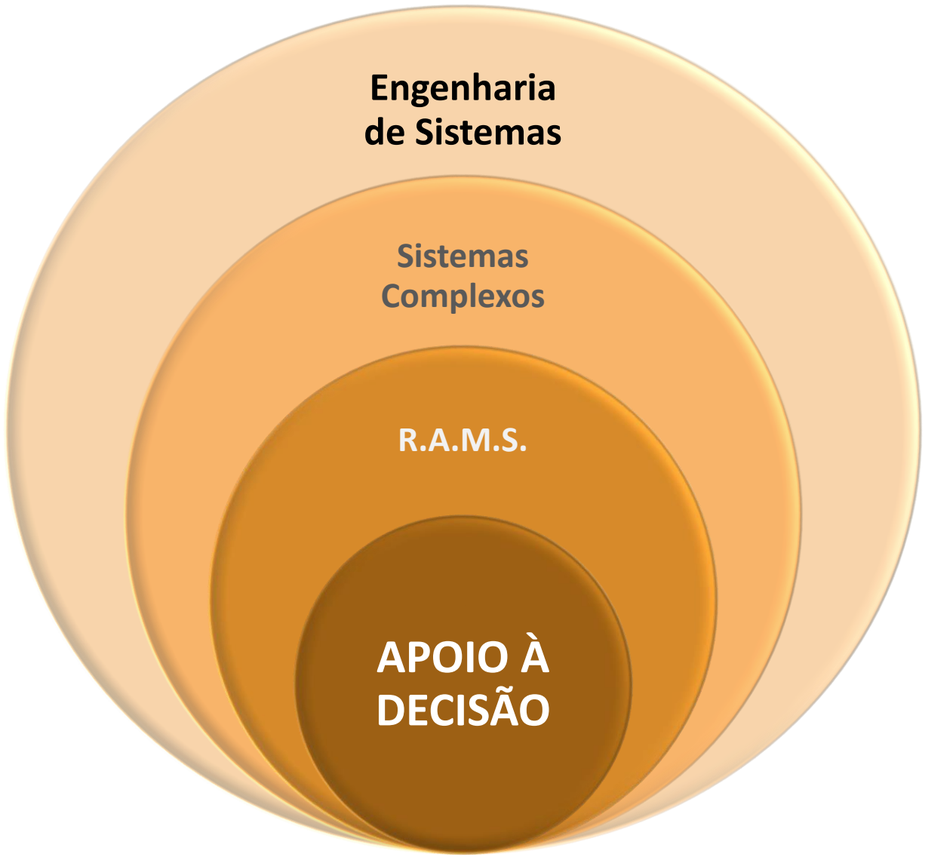
SOBRE A KONATUS

KONATUS

QUEM SOMOS

O jeito Konatus de agregar valor

POSICIONAMENTO ESTRATÉGICO



ESCOPO

- **Gestão de ativos**
- **Gestão operacional**
- **Avaliação de indicadores de R.A.M.S.**

Tecnologias essenciais

- ✓ Integração de sistemas
- ✓ Plataformas web & mobile
- ✓ Processamento de dados
- ✓ Data science
- ✓ Prognóstico & diagnóstico

Soluções

- ✓ Licenciamento de software
- ✓ Desenvolvimento de SW customizado
- ✓ Consultoria & treinamento

KONATUS

EXPERTISE EM R.A.M.S.

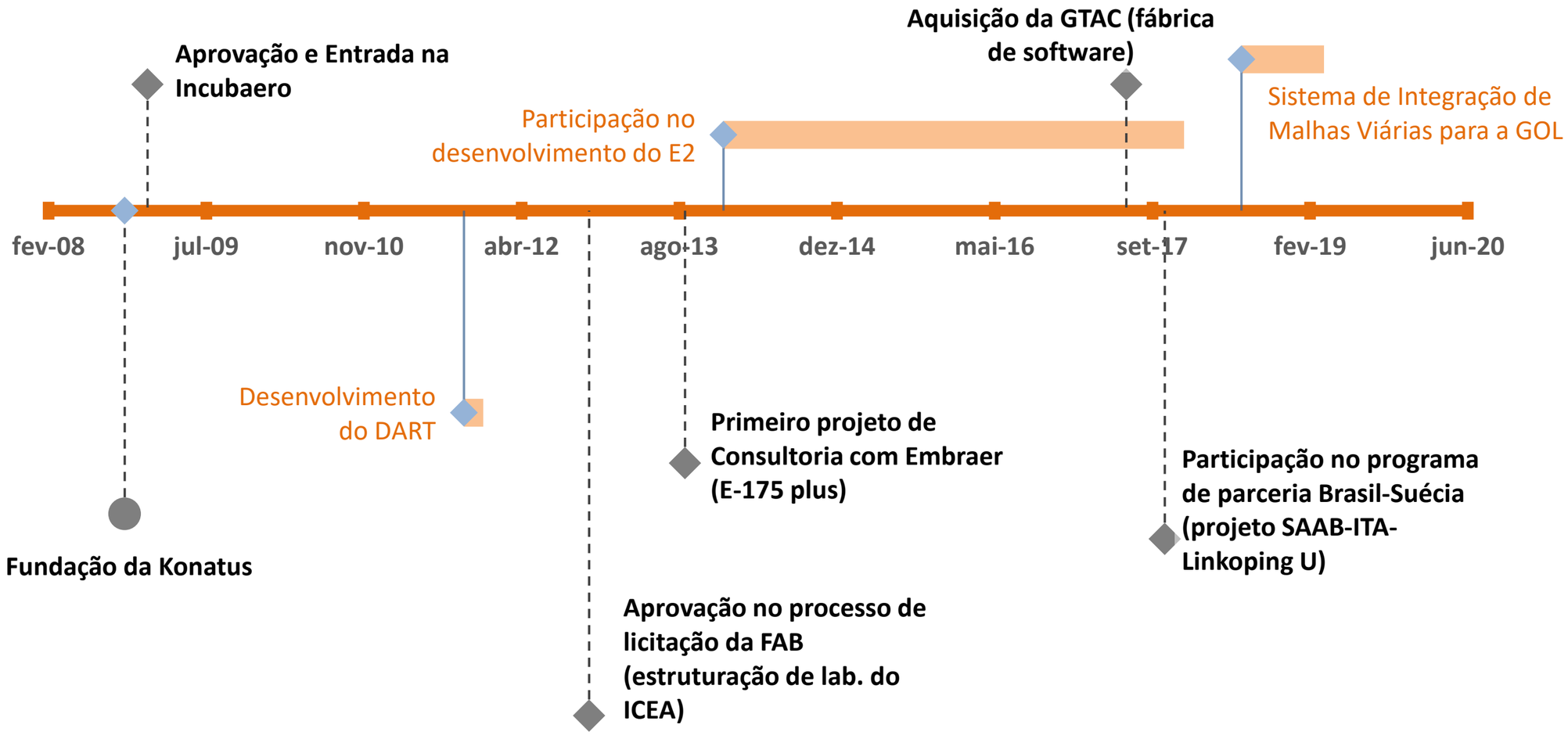
Equipes experientes com competências sob demanda para cada projeto

- Soluções em Confiabilidade, Disponibilidade, Manutenibilidade e Segurança (R.A.M.S.)
- Principais setores atendidos
  - ✓ *Aeronáutico*
  - ✓ *Defesa*
  - ✓ *Automobilístico*
  - ✓ *Médico*

- Acesso a rede de profissionais renomados altamente especializados
- Modelo ágil de contratação por projeto
  - ✓ *Flexibilidade e rapidez de atendimento*
  - ✓ *Custo competitivo*

LINHA DO TEMPO

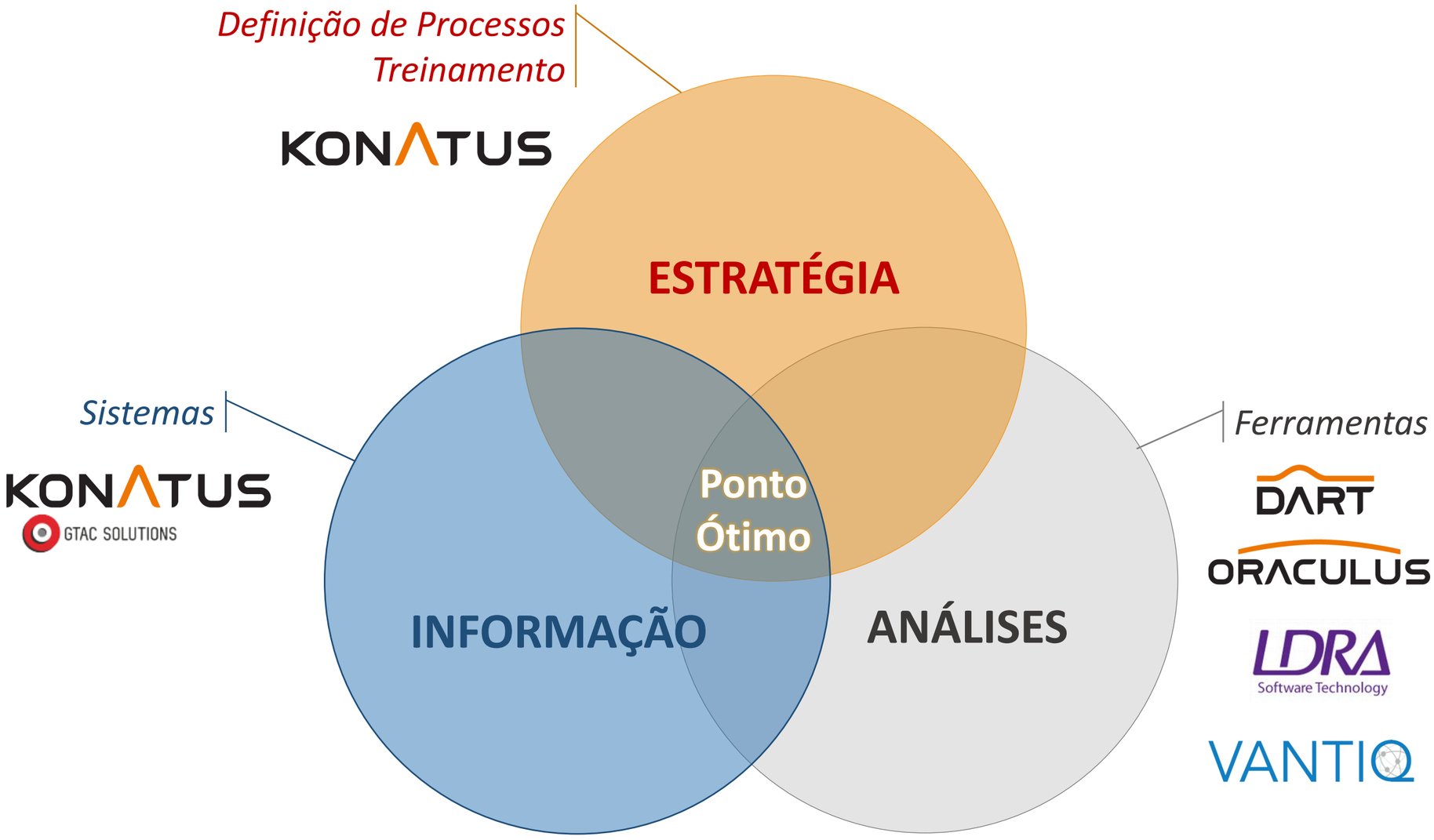
Do meio aeronáutico para o mundo



KONATUS

SOLUÇÕES PARA APOIO À DECISÃO

Busca incessante pela ideal conciliação dos 3 fatores principais de gestão



**Adaptado do web site da Systecon*

KONATUS

CLIENTES

Trabalhamos com algumas das maiores empresas do mundo

Desenvolvimento de sistema de integração de todos os projetos do evento, com planejamento e monitoramento das obras

WWW.KONATUS.COM.BR
+5512 3307 0019
Av. São João, 2375 – sala 2301
São José dos Campos-SP
contato@konatus.com.br

Technologies for a safer world

KONATUS

OBRIGADO!

(PERGUNTAS ?)

CONTAMOS COM SUA PRESENÇA

VI SAFETY CRITICAL SEMINAR

15/dez – 9h às 16h

Edição 2020 totalmente online (webinar)

Inscrições gratuitas em
konatus.com.br/scs2020

Hygor Potter
Diretor de Vendas & Marketing
+5511 97549 1395
hygor.potter@konatus.com.br