



*Verificação e Validação de
Software Projeto Qualidade do
Software Embarcado em
Aplicações Espaciais*

Conteúdo

- **Contextualização**
- **Processo de Desenvolvimento de Software INPE**
- **ECSS e ciclo de vida de missões espaciais**
- **Objetivo do projeto**
- **Software Piloto**
- **Metodologia de Execução**
- **Adequação das Normas ECSS ao projeto**
- **Modelo Fábrica de Software DBA**
- **Processo de Verificação e Validação Independente**
- **Modelos Serviços/ Casos de Testes/**

Contextualização - Internacional

- Crescente preocupação das agências espaciais mundiais a partir dos anos 90 com a qualidade de projetos
 - satélites
 - veículos lançadores
 - operação de missões em soloatinge a **qualidade do software em sistemas críticos**
- Evolução dos sistemas computacionais aumenta as funcionalidades implementadas por software - **maior complexidade dos componentes de software**
- Grandes investimentos do setor industrial na **melhoria dos processos de desenvolvimento de software**

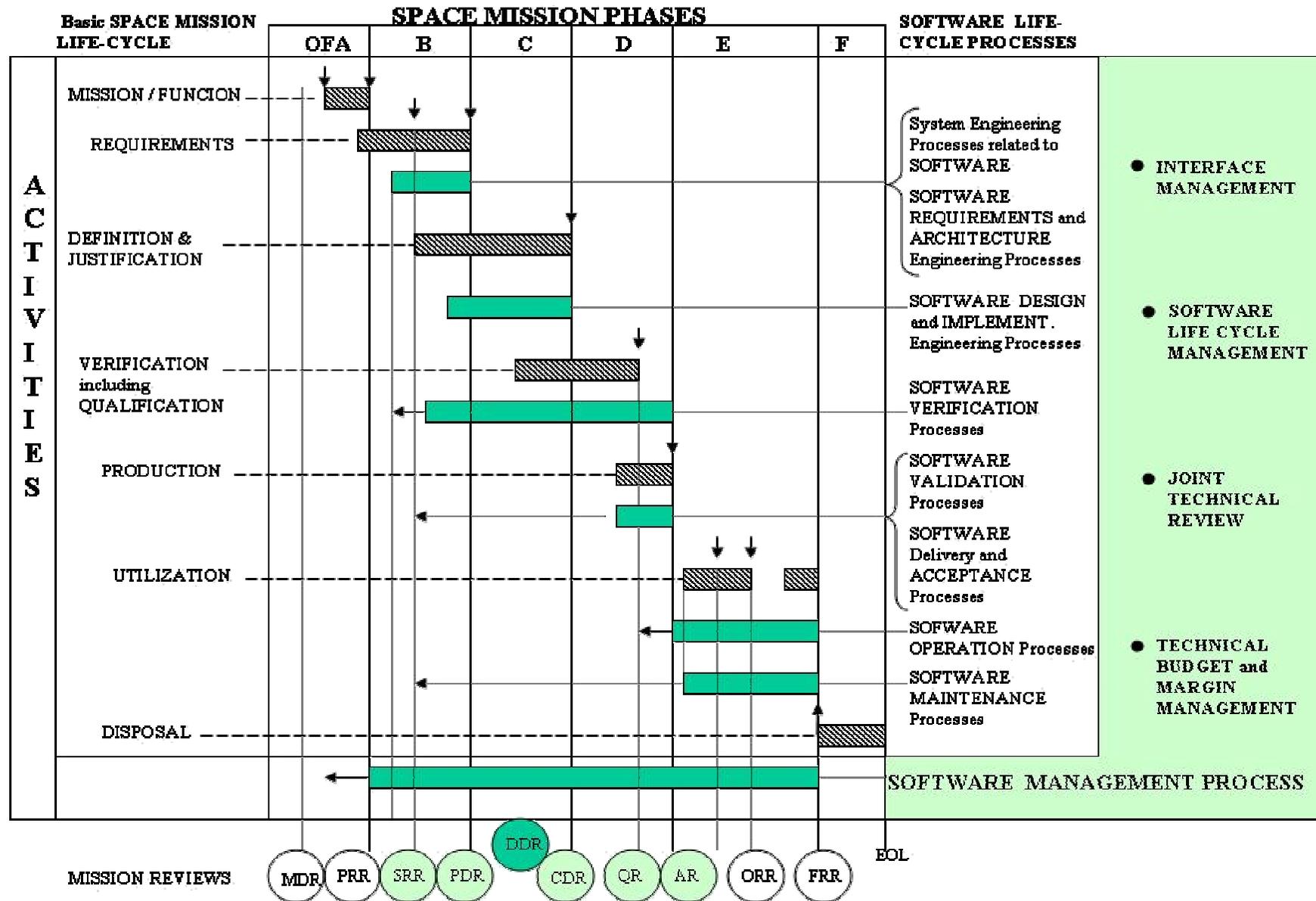
Contextualização - Nacional

- Necessidade de envolver a indústria brasileira de software no fornecimento de subsistemas embarcados em missões de satélites
- Interesse em avaliar a aderência dos processos seguidos pela indústria aos requisitos recomendados pelas normas da área espacial ECSS adotadas no INPE



Software em Missões Espaciais

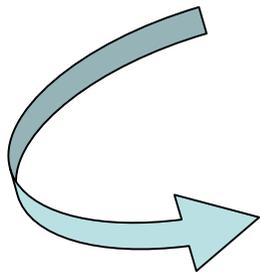
Normas ECSS



Objetivos do Projeto QSEE

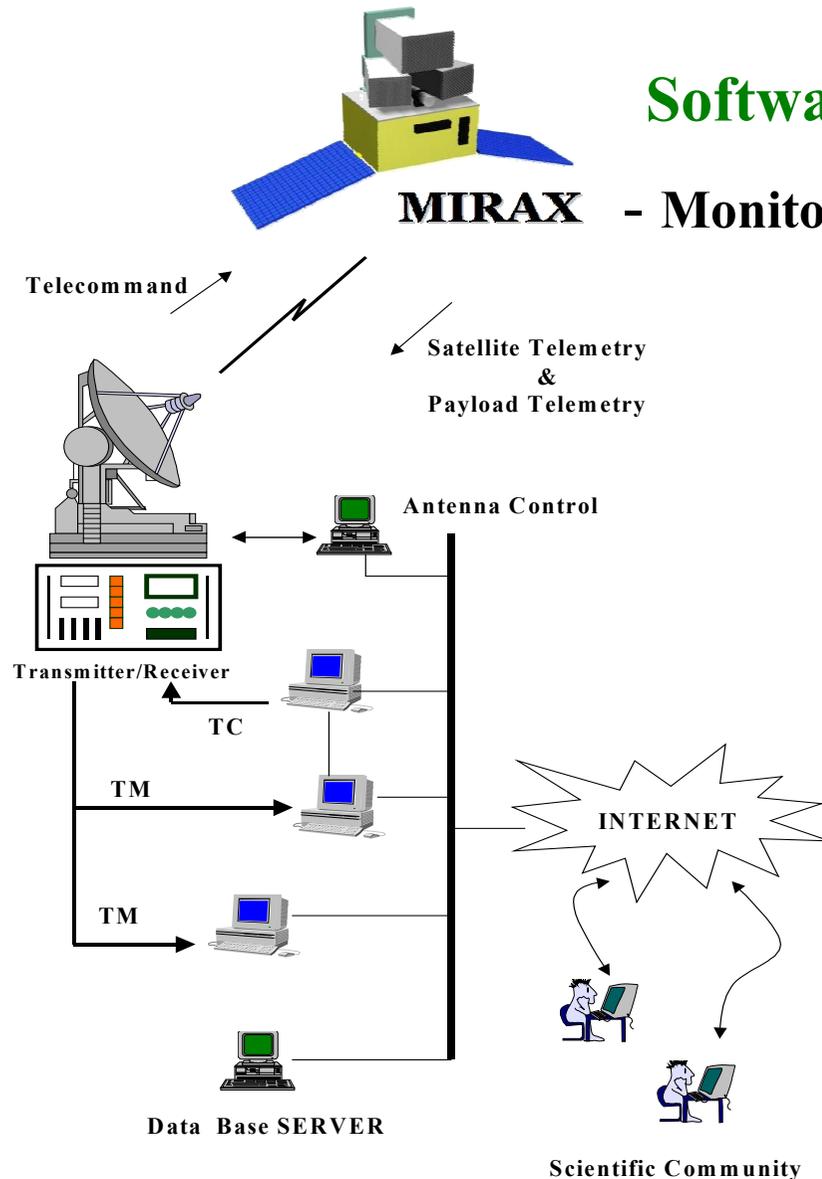


- Avaliar um modelo de Fábrica de Software nacional no desenvolvimento de software embarcado para o INPE
- Uso das normas ECSS para facilitar a relação Cliente/fornecedor
- Consolidar um processo de aceitação de software para o INPE apoiado na abordagem de Verificação e Validação Independente de Software



Experiência no fornecimento de software embarcado pela indústria nacional seguindo as normas ECSS

Software Piloto SWPDC



MIRAX - Monitor e Imageador de Raios X

Software da carga útil do satélite científico

Satélite de Astronomia para Imageamento contínuo (mínimo 9 meses) de Raios X de uma vasta região em torno do plano Galáctico central para fenômenos transientes

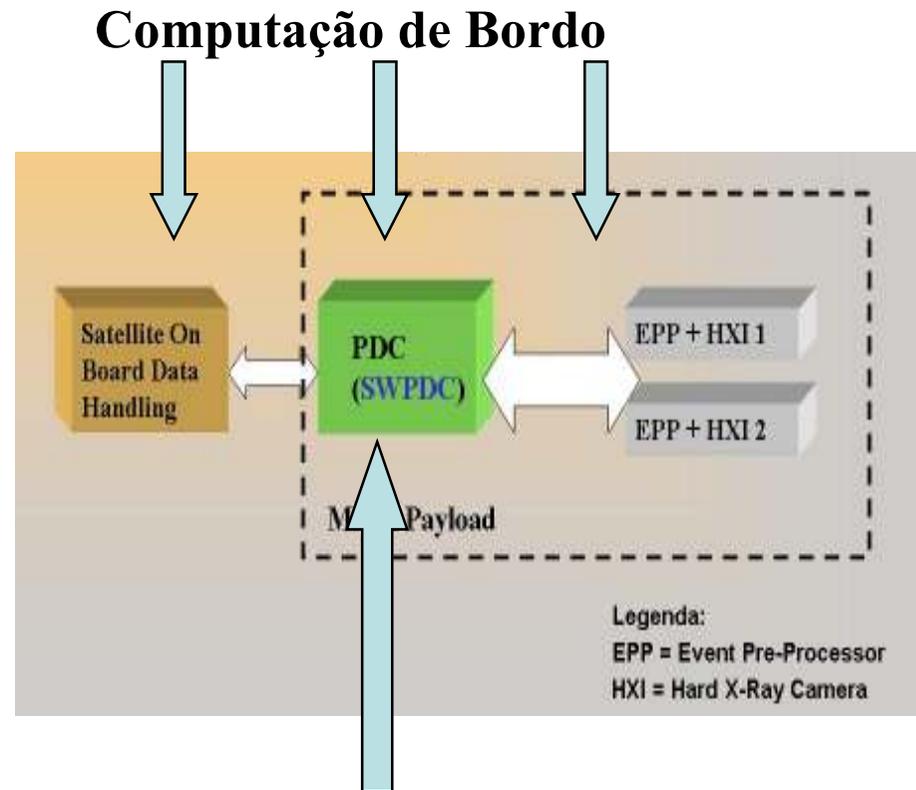
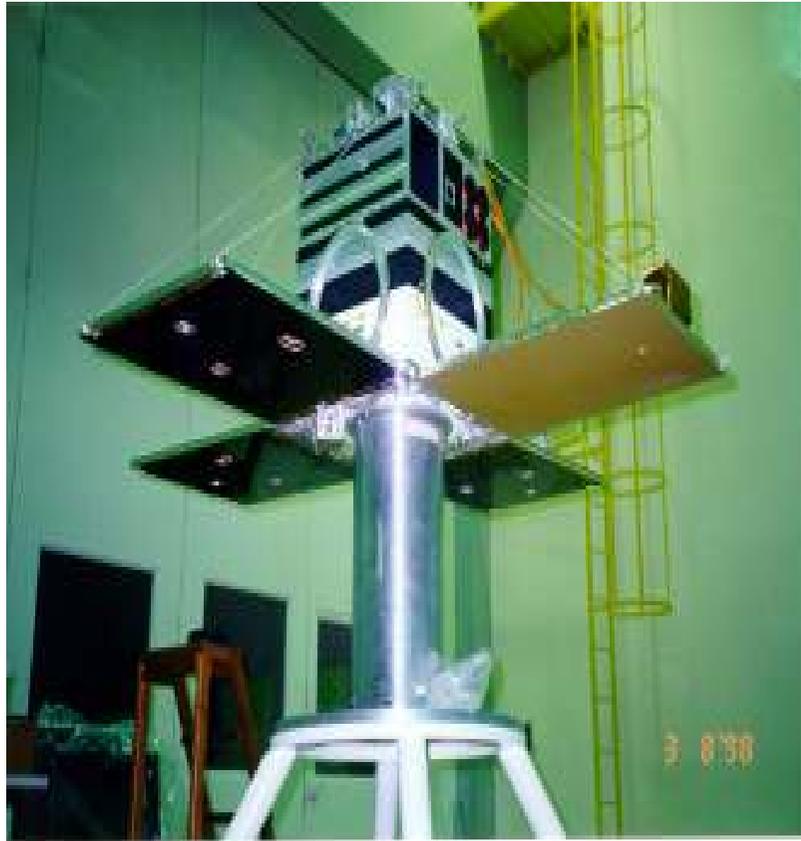
CARGA ÚTIL

Instrumento Imageador de Raios X

- Computador PDC - **SWPDC**
- Computador - Eventos das Câmeras - EPPs
- 2 Câmeras de Raios X - HXI

<http://www.cea.inpe.br/qsee/>

Software Piloto SWPDC



Software Piloto do QSEE



Cliente

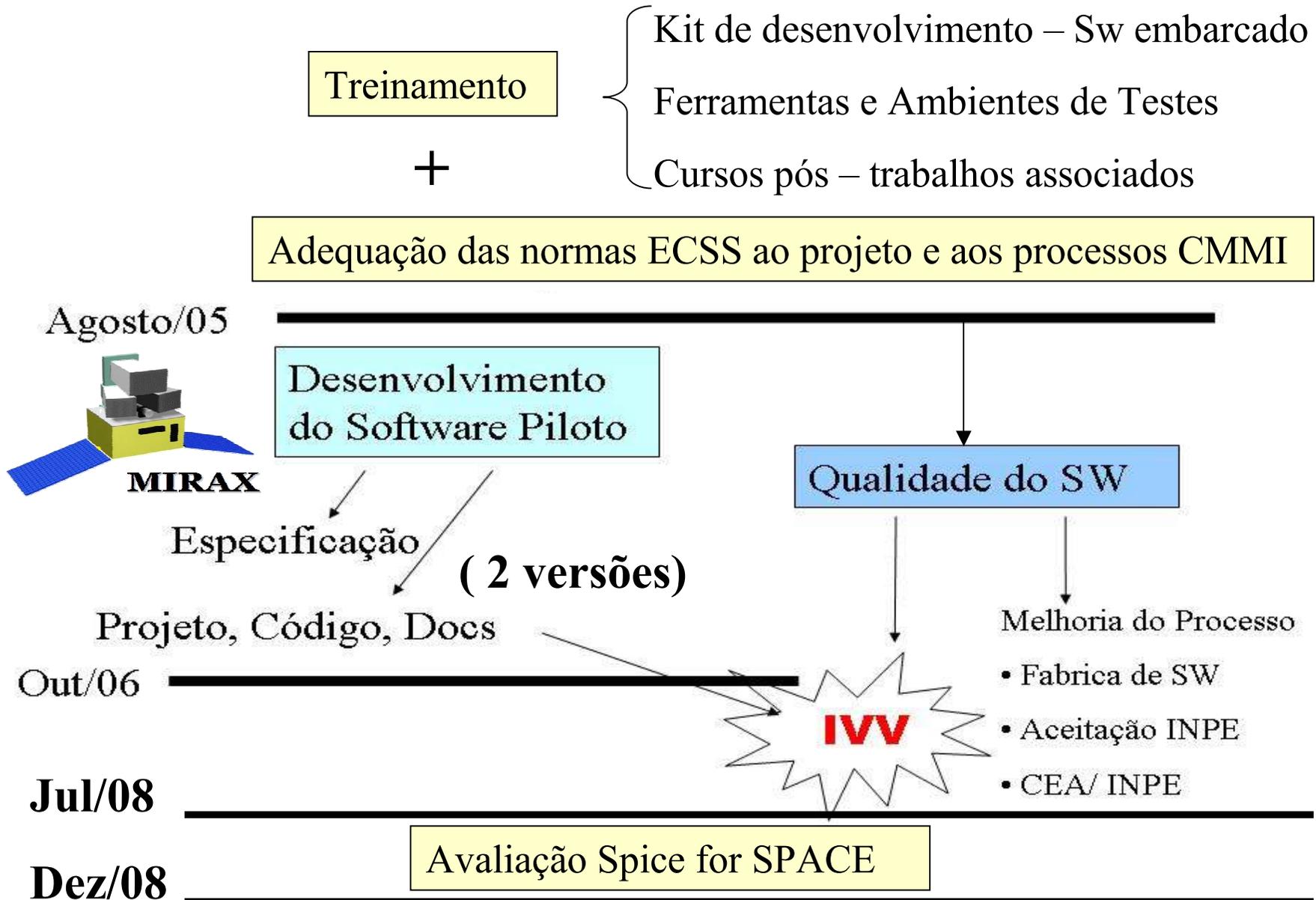
Especificação

2 versões

Fornecedores



Metodologia de Execução



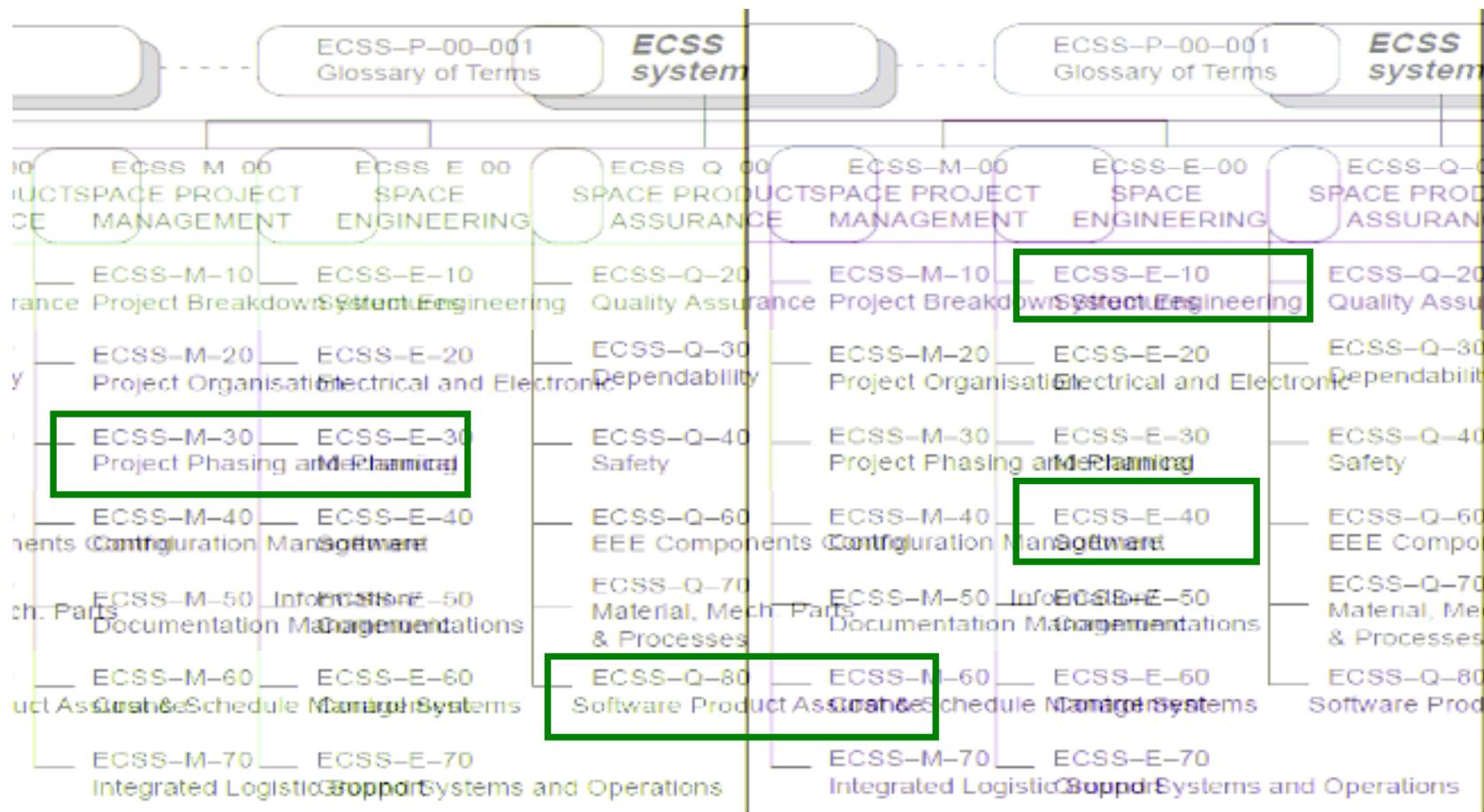
Adequação das Normas ECSS



Foco no relacionamento INPE x Fábrica de Software

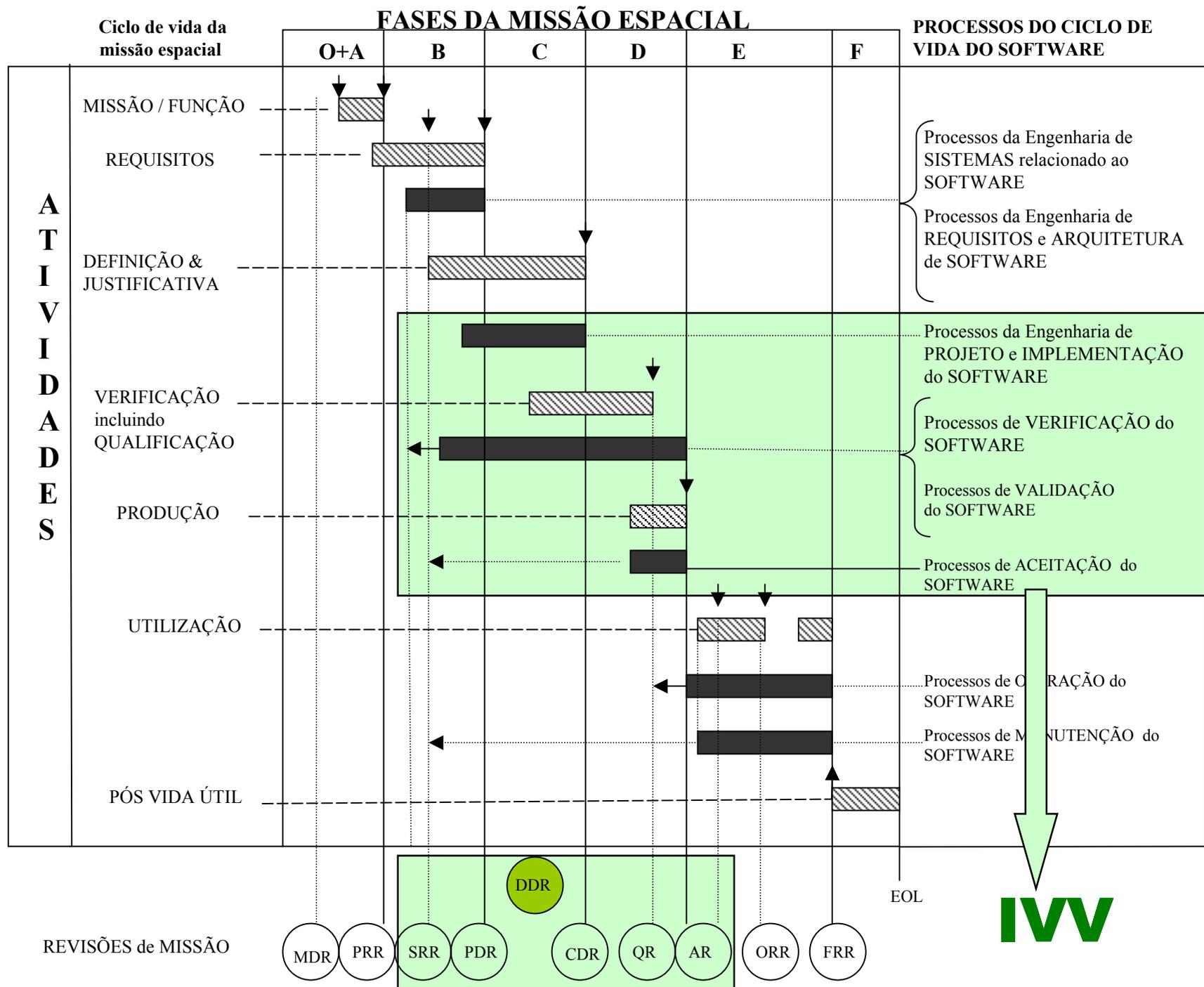
Cliente- Fornecedor

ECSS Structure:

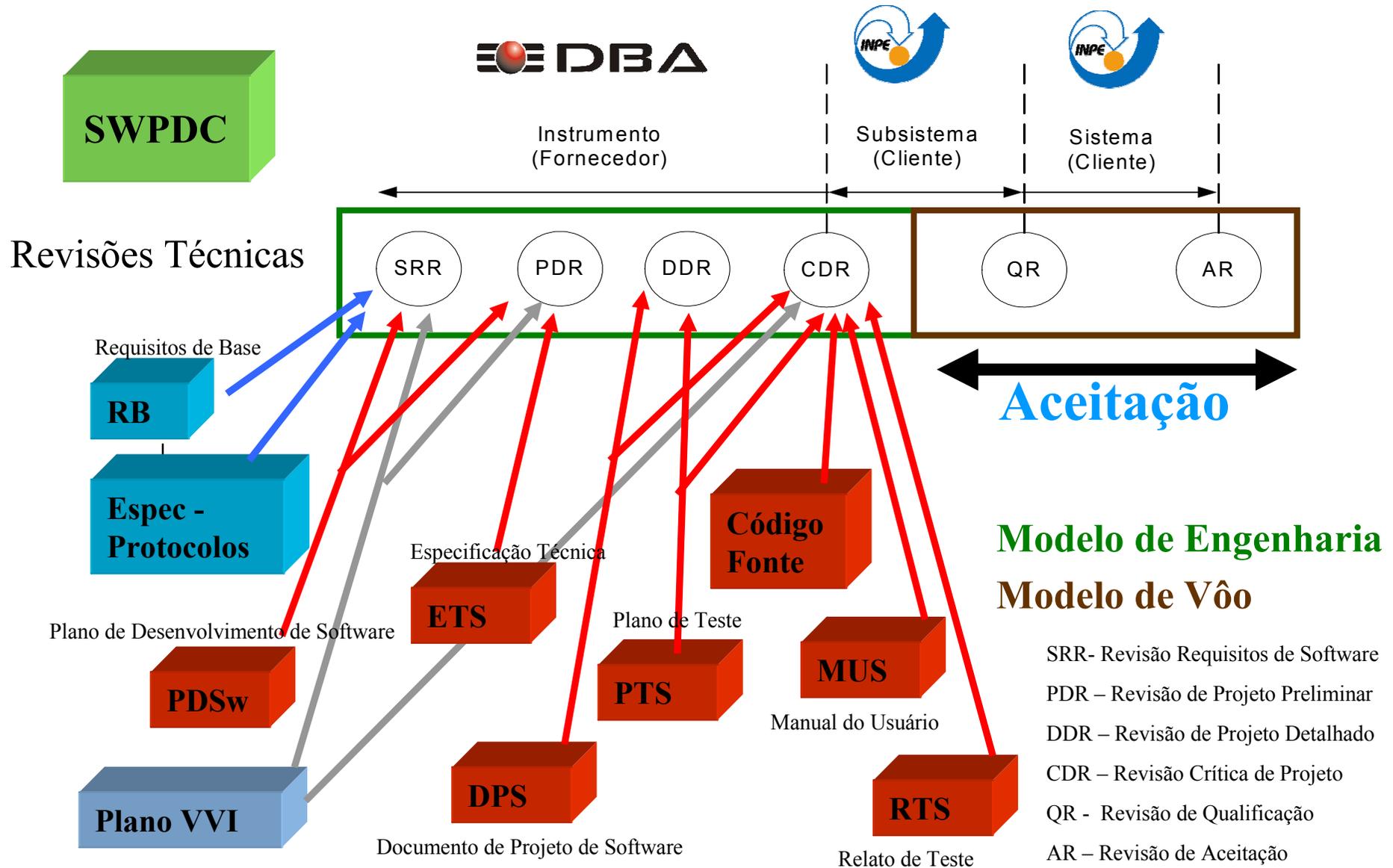


ECSS Requirements related to software product assurance **PLANNING**

Requirement	Description	Tailored Form	Tool	Document
Contractual Aspects	Supplier and Customer define a contract	Established when project QSEE was approved by governmental financial support (FINEP)	-	Agreements on Project Proposal
Software Product Assurance Planning and Control	Supplier provides a plan complying requirements and being approved by customer	SPA items included in DBA Software Development Plan document, reviewed and approved in SSR	Compliance matrix	SDPlan
Software Product Assurance Reporting	Supplier provides mechanisms for assessment of the current quality of the product	Reviews data package and tool allowing the customer to follow each Production Order (OP) into the FSW	Reports from a proprietary tool (SAF)	SDPlan
Non-conformances	Software Reviewer Board and baseline established by supplier/ customer	Formal Reviews point out the discrepancies (RIDs) and project control meetings	-	RB
Software Problem	Supplier defines and implements procedures for logging, analysis and corrections of software problems	Software Problems identified in the FSW have well established internal procedure. RNCs are problems identified on acceptance testing.	DBA FSW work-flow involves QA team	SDPlan



Desenvolvimento do Software + IVV



Processo da Qualidade do Software Embarcado no INPE



- Especificação do SW
- Definição das interfaces
- Análise de requisitos

Software é visto como subsistema



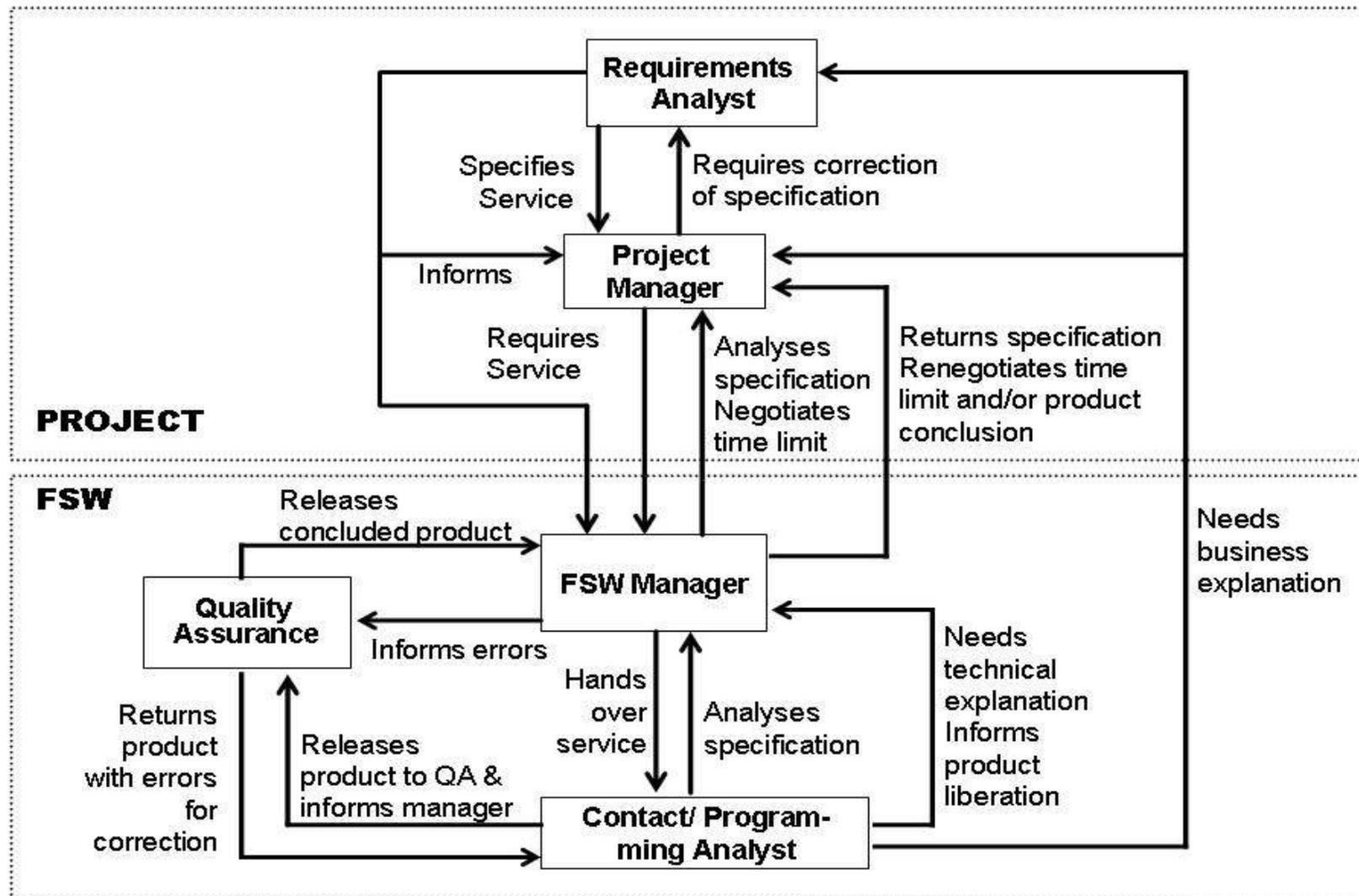
- Projeto Preliminar
- Prototipação



- Projeto Detalhado
- Implementação e Testes

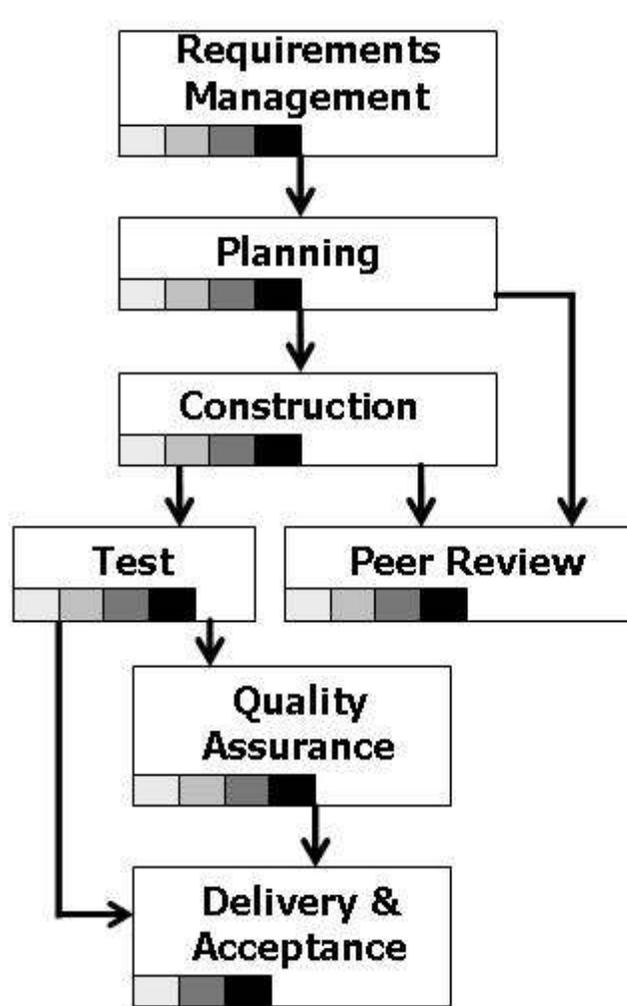


Modelo Fábrica de Software da DBA - CMMI 3

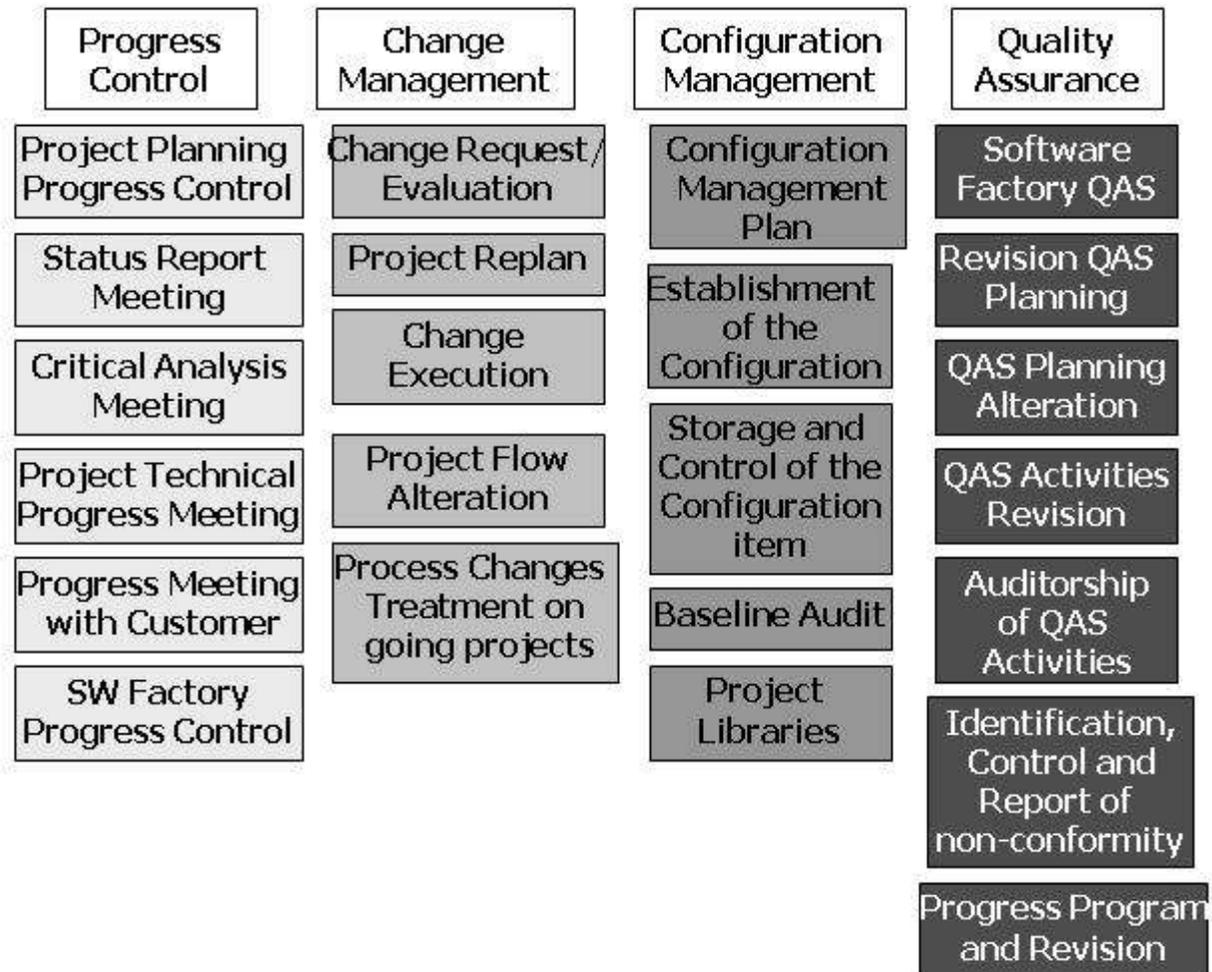


Modelo Fábrica de Software da DBA

SW Development Processes Macro-Flow



Related sub-processes



Hoje MPS_br A preparando CMMI 5

Software Piloto SWPDC



Laboratório de Desenvolvimento da Ciências Espaciais e Atmosféricas/INPE

Experiência no desenvolvimento de software crítico para sistemas espaciais

- Engenheiro Pleno (líder)
- 2 Desenvolvedores Sw



Fábrica de Software



Fases do ciclo de vida do software

- Analista Pleno (líder)
- 2 Desenvolvedores Sw

áreas chave de processos CMMI níveis 2 e 3

- EQA

Processo de Verificação e Validação Independente

Requisitos Base 

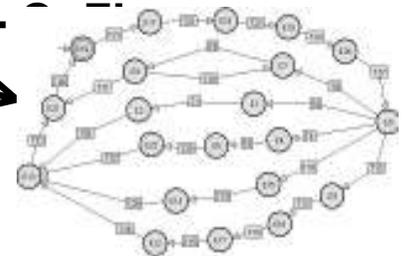
+ Especificação Técnica 



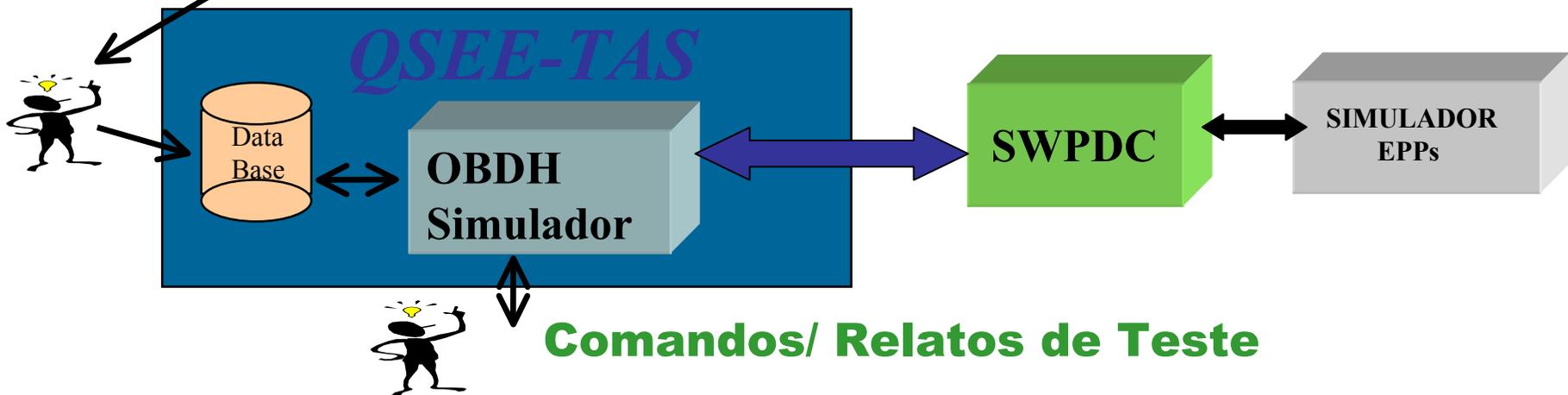
IVV



- Metodologia de especificação dos testes –
- Participação nas revisões de projeto



- Refinamento da Modelagem usando o Manual do Usuário
- Ferramenta de Geração Automática de Testes – CONDADO
- Script Casos de Teste



Aceitação do Software SWPDC



Operação do Software é validada



Em cada estágio de integração o software será incrementalmente encapsulado e validado sob diferentes pontos de vista de testadores (modelos comportamentais do software)

Processo de Aceitação do SW apoiado em IVV

A formal testing to determine whether or not a systems satisfies acceptance criteria based on the software problems reports resulting from verification and validation activities [IEEE-Std1059-1993]

Neste projeto os critérios de aceitação estão baseados nas falhas reveladas pelos serviços modelados pela equipe IVV

Aceitação do Software SWPDC



Operação do Software é validada



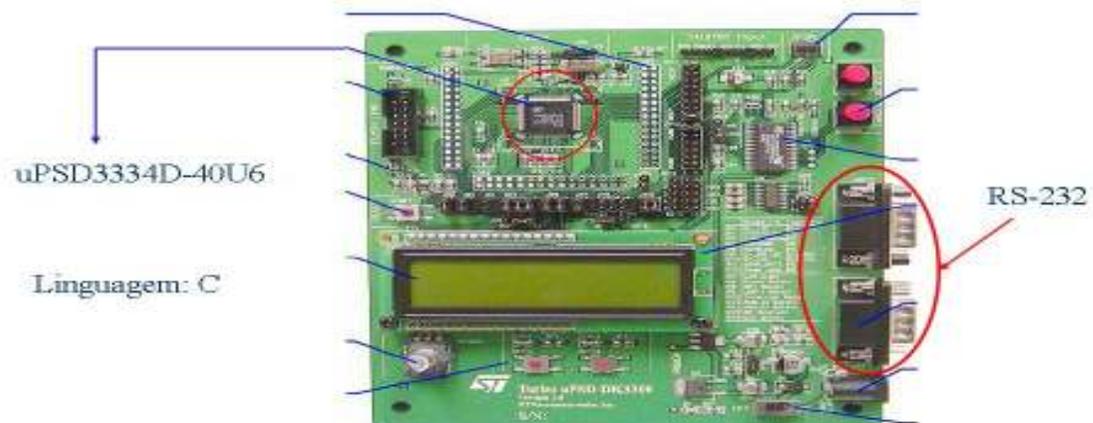
Instrumento

PDC – “Modelo de Engenharia”

Código- Fonte

Parâmetros	DBA
Files:	107
Functions:	81
Lines:	10409
Lines Blank:	2236
Lines Code:	3869
Lines Comment:	4475
Declarative Statements:	531
Executable Statements:	2383
Ratio Comment/Code:	1.16
Binary file Size (kB)	26.2

- Processador uPSD3334D-40U6: microcontrolador baseado no 8051/8032 da Intel, com uma estrutura de memória flexível, lógica programável e periféricos internos.



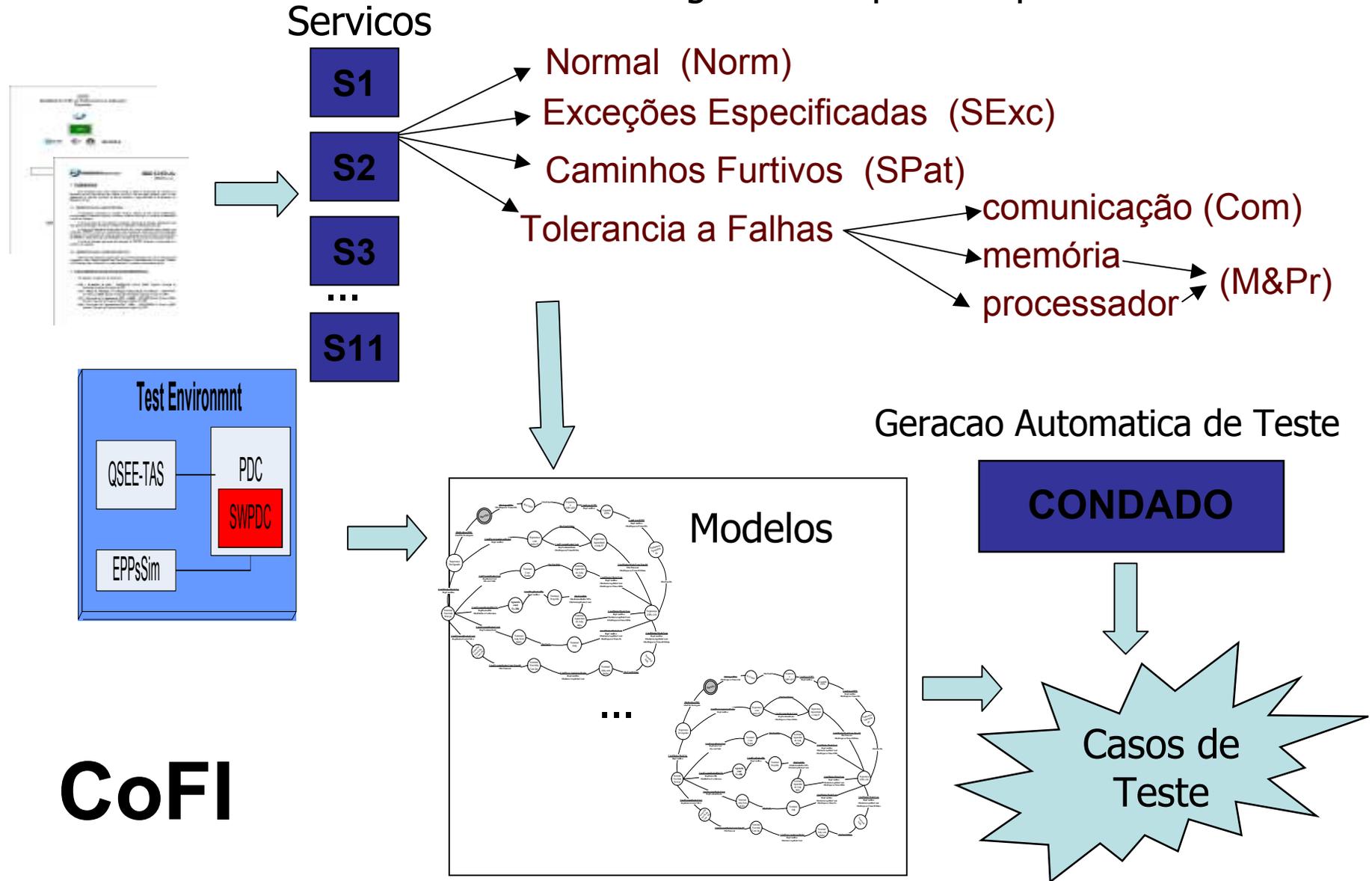
Funcionalidades

- Manipulação de Comandos do OBDH
- Coleta e Formatação de Dados (Científicos, Diagnóstico, Teste, Housekeeping e Descarga de Memória)
- Transmissão de Dados de Telemetria
- Suporte a Carregamento de Programas, em tempo real, Memória do PDC
- Gerenciamento de Memória
- Mecanismos de Detecção. Confinamento e Recuperação de Erros

SERVIÇOS

Modelos dos Serviços e de Falhas

Cenários organizados por comportamento do SW



Número de Modelos dos Serviços

Services		Models					Total
		Norm	SExc	SPat	Com	M&Pr	
S1	Initialization	2	1	1	1	1	6
S2	Scientific data	2	2	1	1	1	7
S3	Housekeeping	3	3	3	1	1	11
S4	Test data	2	4	4	1	1	12
S5	Diagnostics	2	4	4	2	2	14
S6	Memory dump	5	3	5	2	1	16
S7	Change operation	1	0	0	0	1	2
S8	Load & execute mode program	1	5	4	3	2	15
S9	OBDM msg syntax	1	0	0	1	0	2
S10	EPP msg syntax	1	0	0	1	0	2
S11	Special commands	4	0	0	2	4	10
Total		24	24	22	13	14	97

770 Casos de Testes

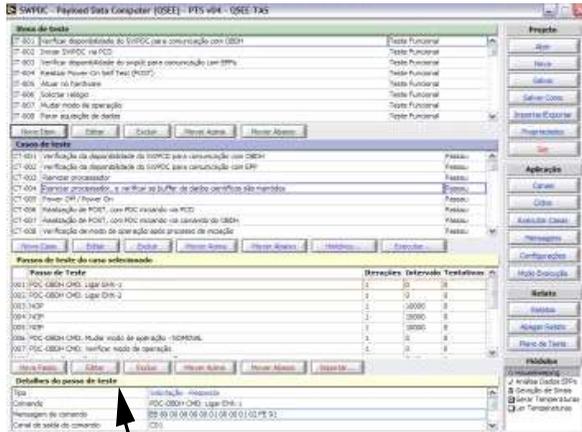


**CONDADO –
Geração Automática de Teste**

QSEE-TAS

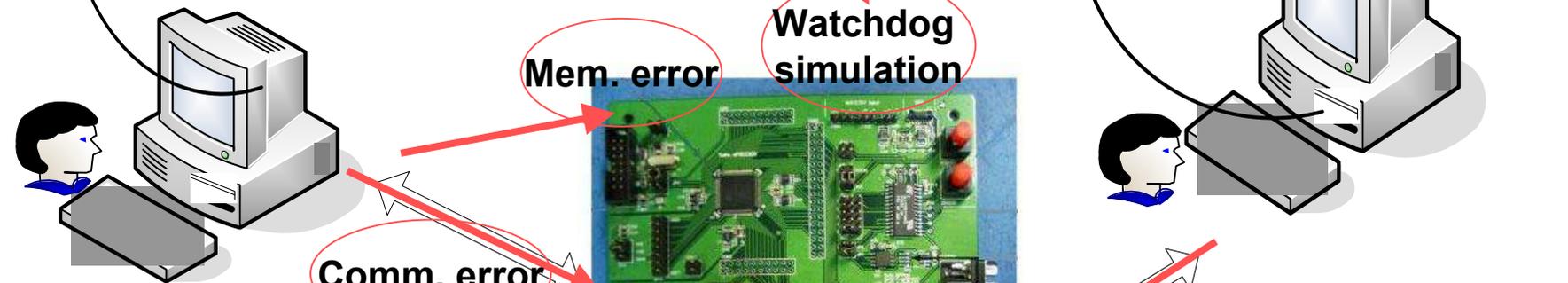
Ambiente de Teste

EPPs Simulator



```

Projeto QSEE - Qualidade de Software Embarcado em Aplicac
MIRAX Hard X-Ray Event Pre-processor Emulator
EPP-Hx Emulator 2.3 - Apr 17 2007 : Lightweight
(C) 2005-2008 - MST/INPE-DAS
[00000000000000586]:configuration status: [fk: none, ff: 0
00 us timeout]
[0000000000001877]:Loading samples of event packs from: e
[00000000001538950]:READY
  
```



OBDH simulator

EPPs simulator

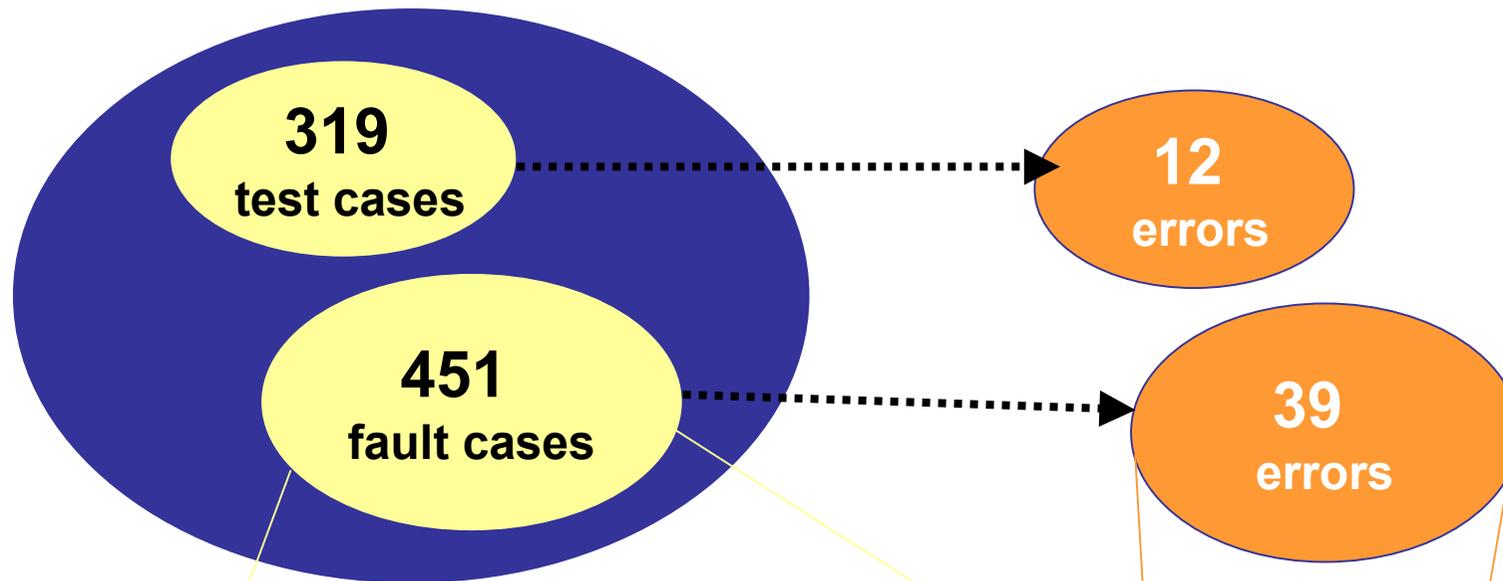
- comunicacao
- controle_de_dados
- controle_de_execucao
- infra-estrutura
- PSDSoft
- servicos_periodicos
- swpdc_main
- bootloader.c
- bootloader.h
- cao_de_guarda.c
- cao_de_guarda.h
- global.h
- I_Atenuacao_HW.h
- I_Cao_de_Guarda.h
- I_Coleta_Relatos.h
- I_Comunicacao_EPPs.h
- I_Control_Erros.h
- I_Control_Execucao.h
- I_Dados_Coletados.h
- I_Gera_Relato.h
- I_Memoria.h
- I_Preparacao_Dados.h
- I_Relogoio.h
- I_Verificacao_HW.h
- startup.asi
- string_swpdc.c
- string_swpdc.h
- swpdc.dbi
- SWPDC.PRJ
- swpdc.WMC
- upsd_init.c

SWPDC embedded in the PDC board

51 Falhas



Resultado dos Testes



Fault Type	Fault injection experiments	Detected Errors
Communication	283	31
Processor	80	5
Memory	88	3
Total	451	39

Conclusão

- **As revisões exigidas pelo cliente INPE e documentos associados não acarretaram alterações no processo de **verificação** da FSw**
 - Requisitos na ETS foram bem detalhados em casos de uso UML e demais artefatos utilizados no PSw
 - Revisões por pares implantadas no fornecedor foram mantidas
- **A **validação** do SWPDC na FSw seguiu a abordagem rotineira**
 - Teste unitário e integrado
 - Planejamento dos testes,
 - Elaboração de casos de testes,
 - Preparação do ambiente e
 - Execução dos testes

Conclusão

- A abordagem **IVV** adotada pelo cliente INPE permitiu
 - Exercitar o envolvimento da terceira parte (INPE + IC/Unicamp) para apoiar o cliente no recebimento e aceitação do software desenvolvido pela FSw
 - Evoluir a concepção e elaboração dos casos de testes em alto nível de abstração em paralelo ao desenvolvimento do software pela FSw
 - Preparar/ adequar o ambiente para execução dos testes no domínio do cliente, diferente do contexto em que o SWPDC foi desenvolvido e testado na FSw

Conclusão

- **Equipe da Garantia da Qualidade da FSw identificou facilmente as especificidades requeridas pelo cliente – maturidade CMMI 3**
- **Treinamento da equipe DBA no INPE por seis meses (2 analistas pleno com mestrado) facilitou a instanciação dos processos da FSw para produção de software embarcado em aplicações espaciais – domínio não familiar a FSw.**
- **Experiência da FSw em produtos de software para celular ajudou na correlação Modelo de engenharia / ambiente alvo**

Lições aprendidas



- **O fornecedor deve entender, antes do início do projeto**
 - **A complexidade e ciclo de vida da missão/ sistema em que o objeto de fornecimento irá operar**
 - **Ambientes, ferramentas e processos pelos quais o produto fornecido será submetido para ser aceito**

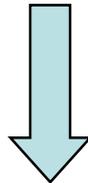


Planejamento das atividades e recursos consistente com a realidade de execução



Lições aprendidas

- **Necessidade de detalhar o documento RB**
 - **Aspectos operacionais do software embarcado devem constar do documento RB para auxiliar a execução das atividades IVV**

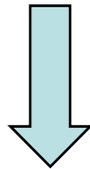


Uma equipe não envolvida com a solução tem que utilizar informações de comportamento e requisitos de operação bem especificados pelo cliente para planejar e aplicar testes operacionais

Melhorias na Fabrica de Software

Checklist mais detalhado do que o padrão existente de itens a serem verificados na linguagem C, processo de Revisão por Pares

Revisão de Requisitos de Software foi incorporada ao ciclo de desenvolvimento utilizado pela FSw precedendo as Fases de Contratação e Levantamento de Requisitos



Evita interpretações equivocadas do fornecedor mitigando riscos de eventuais problemas na entrega do produto e conseqüente retrabalho

Produção Acadêmica

- 2 artigos em Conferência Internacional – 2006
- 2 artigos em Workshop Internacional – 2006
- 2 artigos em Simpósio Nacional – 2006
- 3 artigos em Conferência Internacional - 2007
- 2 artigos em Conferência Internacional - 2008

Método Desenvolvido

- Processo de Aceitação de Software para o INPE usando a abordagem VVI

Recursos Humanos Capacitados

- 3 estagiários nível de mestrado concluído
- 2 estagiários nível de graduação concluído

Premiações

- Ciclo 2007 – PBQP Software - Dorgival Brandao Junior

Agradecimentos

- **FINEP – pelo suporte financeiro concedido ao projeto QSEE – Ações Transversais/ Software.**
- **CNPq – bolsa DTI de apoio ao projeto.**
- **FUNDEP – pela apoio administrativo à execução do projeto.**

<http://www.cea.inpe.br/qsee/>

Perguntas ?

Obrigada!

SERIE DE SEMINARIOS EM COMPUTACAO

INSTITUTO DE COMPUTACAO - UNICAMP

Data: 19 DE SETEMBRO de 2008, sexta.

Hora: 10-12:00

Local: sala 85, IC-2.

Palestrante: Maria de Fátima Mattiello-Francisco - Instituto Nacional de Pesquisas Espaciais (INPE)

Título: "Verificação e Validação de Software: Projeto Qualidade do Software Embarcado em Aplicações Espaciais"

Resumo: Apresentar os desafios e a experiência adquirida em Verificação e Validação de Software Embarcado em instrumento científico a bordo de satélites no contexto do Projeto Qualidade do Software Espacial em Aplicações Espaciais – QSEE. Caracterizado como um projeto de transferência tecnológica para a indústria de software brasileira, ele explora o modelo Fábrica de Software no desenvolvimento de sistemas de software críticos da área espacial.

Biografia: Maria de Fátima Mattiello-