2o Seminário Internacional de Segurança Ferroviária

ARYLDO G. RUSSO JR. – Director &
***Senior Safety Assessor* – CERTIFER**

Certificação Ferroviaria
Experts en Railway Certification

Pontos fortes

Lider na França, Top 3 worldwide

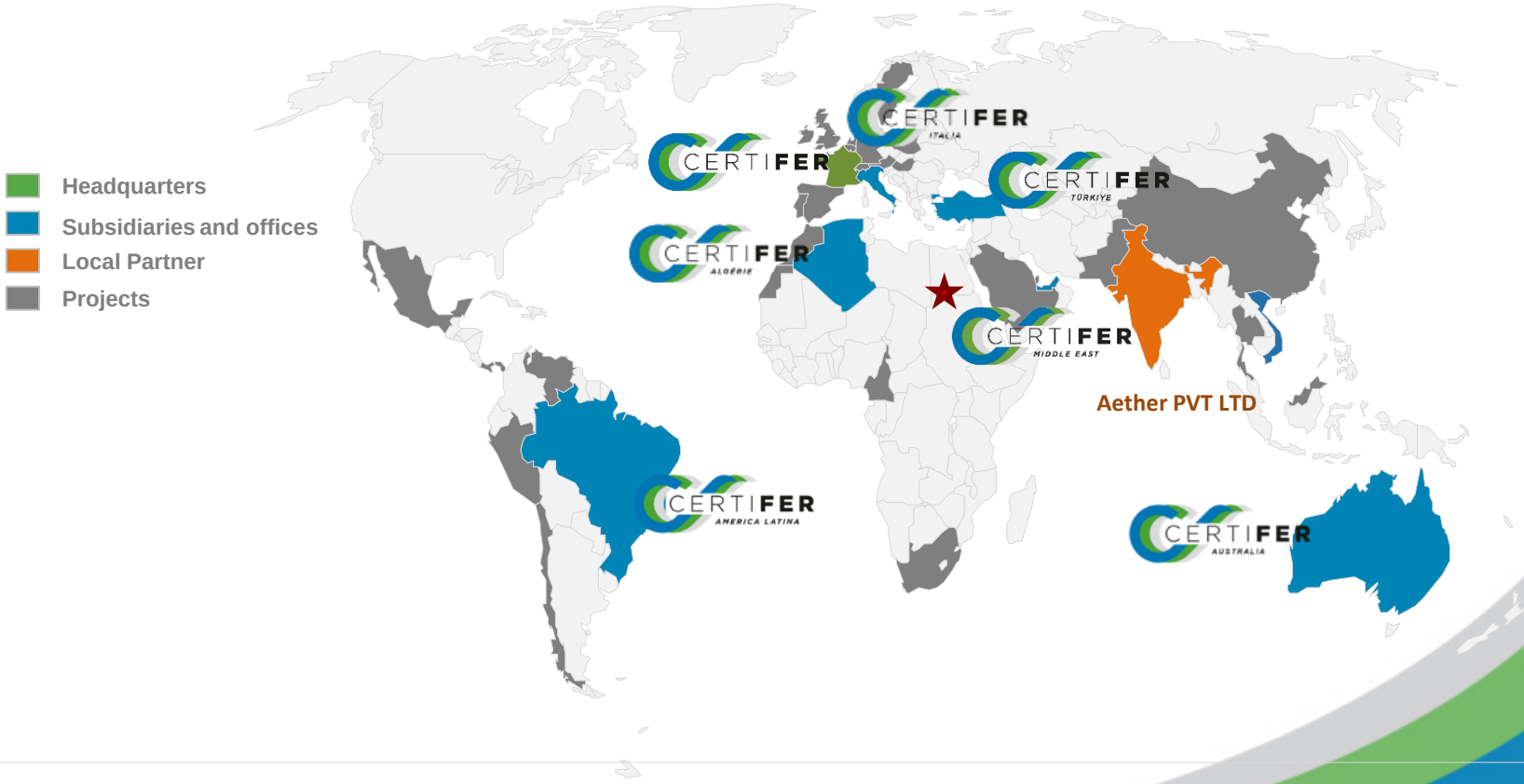
O fornecimento de certificação no setor ferroviário é nosso principal negócio.

20 anos de experiencia

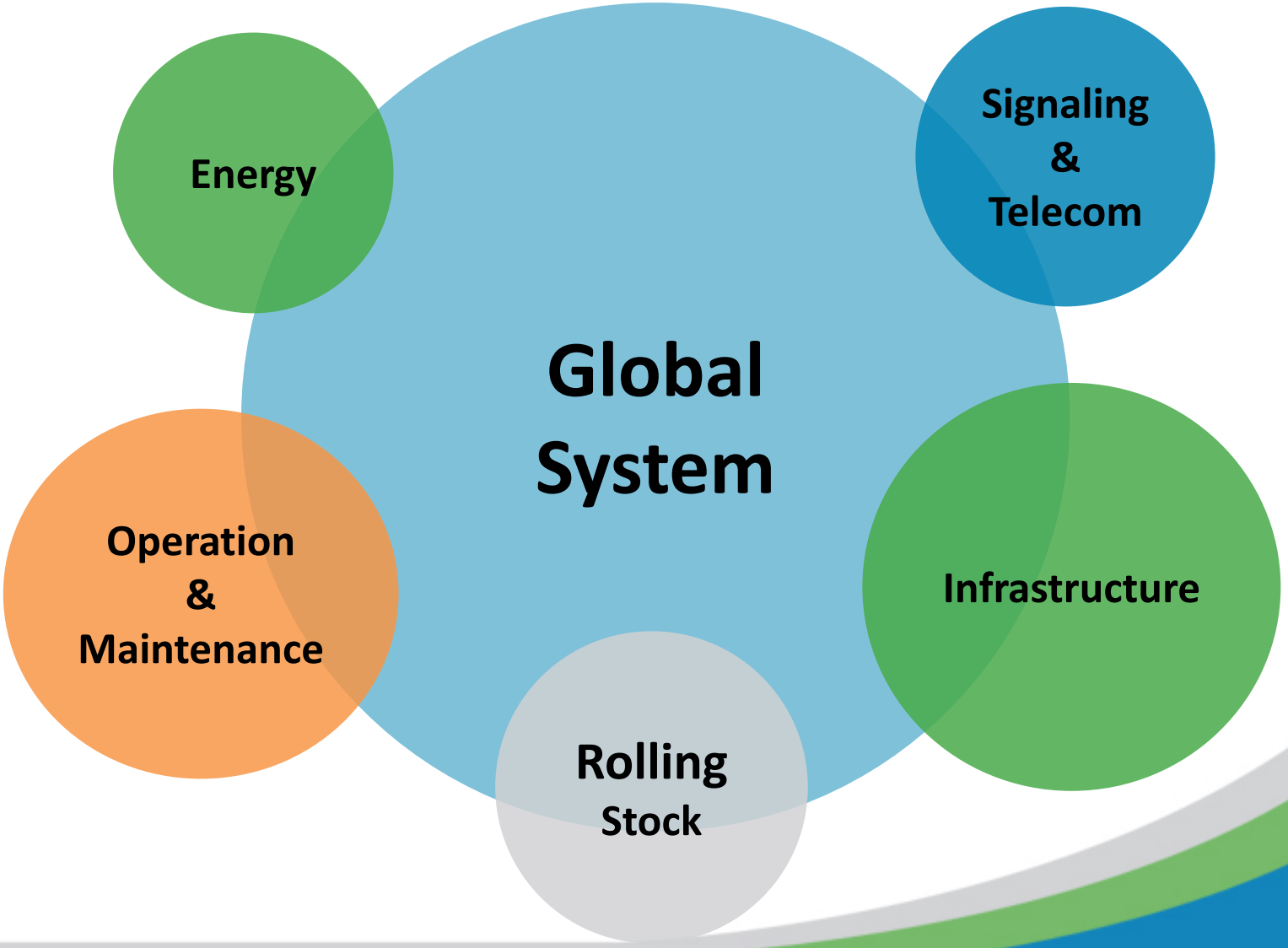
Acreditações nacionais e internacionais

Mais de **350 experts** provenientes de todos os setores metroferroviários no mundo todo

CERTIFER está atuando em mais de 40 países



Global Services



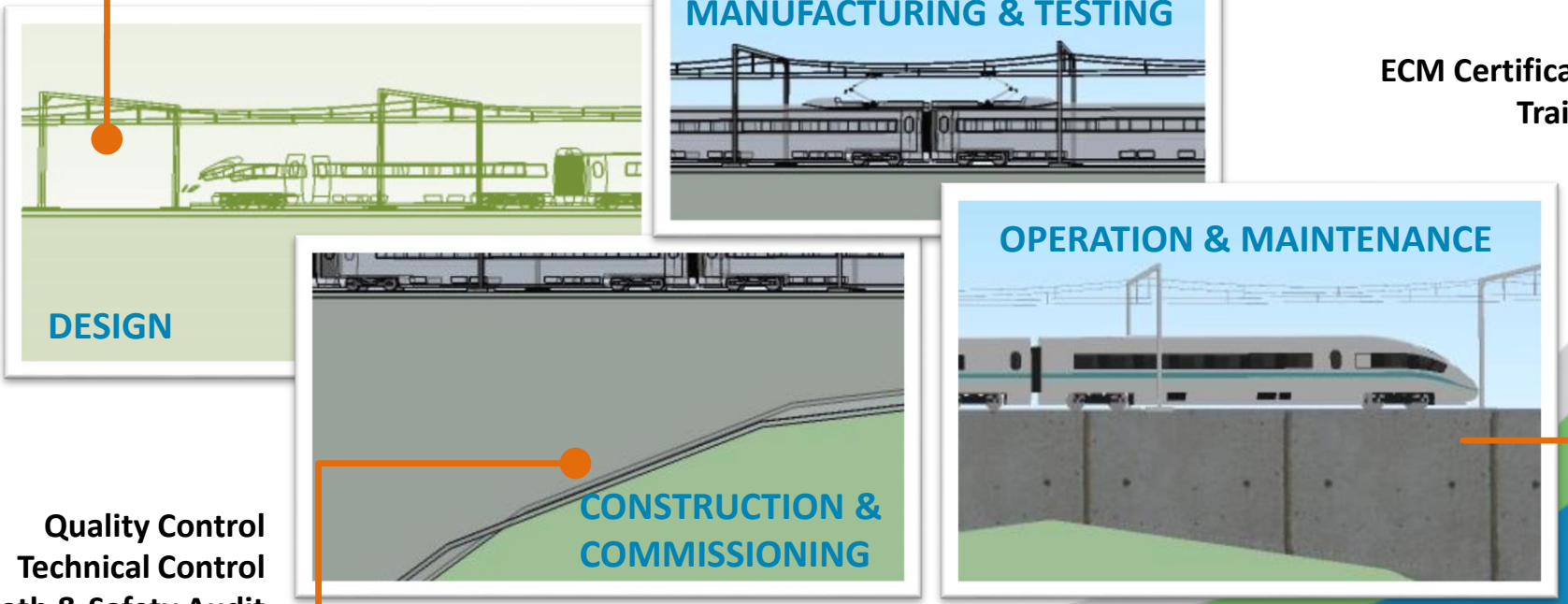
Nossas atividades

Independent Safety Assessment (ISA)
TSI interoperability certification
National Regulation Assessment
SIL certification
Reliability, Availability, Maintainability, Safety (RAMS) Studies
TPED/RID Certification

Quality Audit
Product certification
Third Party Quality Agency

ECM Certification
Training

Quality Control
Technical Control
Heath & Safety Audit



- **PARTE 1 - O processo de certificação de acordo com as Normas internacionais IEC**

- **PARTE 2 - Os níveis hierárquicos e a aceitação cruzada no processo de certificação de Segurança**

Parte 1

- Introdução aos tipos de missões
- Avaliação Independente de Segurança (Missão ISA)
- Processo ISA
- Independência e Imparcialidade

Presentation Outline

Introdução aos tipos de missão

Some independent services

- ISA: Avalia se os riscos relevantes foram reduzidos a um nível aceitável, e se evidências suficientemente fortes foram apresentadas para demonstrar que os objetivos de segurança foram cumpridos.
- NoBo: De acordo com a diretiva de interoperabilidade, verifica que um subsistema cumpre os requisitos essenciais
- DeBo: De acordo com a diretiva de interoperabilidade, verifica que um subsistema cumpre com as regras nacionais
- Outras como ICP, ICE, CSM, etc…

Presentation Outline

Avaliação Independente de Segurança (Missão ISA)

ISA Mission

- Deve iniciar junto com o início do projeto
- Deve seguir o ciclo de vida do processo
- Deve utilizer diferentes abordagens, tais como:
  - Avaliação do processo / Auditorias
  - Avaliação da documentação
  - Avaliação do processo de V&V, Testes e Inspeções locais de conformidade
  - Avaliação dos Safety Cases, entre outras

ISA Mission

- O objetivo principal é ganhar confiança de que o Sistema tenha estabelecido:
  - Os requisitos corretos de segurança
  - Que as funções implementadas correspondem precisamente ao que foi especificado.
  - Que todos os requisitos exportados a manutenção e/ou operação sejam implementáveis.

ISA Mission

- Obrigação da utilização de uma entidade ISA:
  - Quando demandada por lei ou agência regulatória
  - Quando demandada pela Grant Authority (casos das PPPs)
  - Quando apresentado como requisito nas especificações do cliente Implicita ou explicitamente, por exemplo:
  - “4.1.8 SISTEMAS CRÍTICOS

Todos os sistemas críticos devem ter o nível de segurança adequado, devendo ser certificado por instituição com notória especialidade, conforme norma **CENELEC EN50126**. Nessa classe
de sistemas encontram-se:

- Sistema de sinalização e controle automático dos trens - CBTC;
- Sistema de freios dos trens;
- Sistema de portas automáticas dos trens e plataformas;
- Sistema de suspensão dos trens, responsável pela estabilidade de rolamento nas vias.

Presentation Outline

Processo ISA

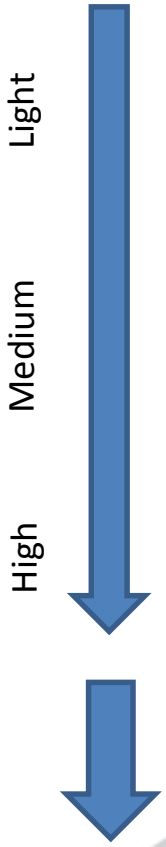
Various Depths of Assessment

Verificação da existência (ou planos de criação) dos documentos/processos previstos pelas regras vigentes (Por exemplo, normas)

Verificar se o conteúdo dos documentos são corretos em relação aos parametros definidos nestas regras

Verificar se as técnicas e ferramentas devinidas por estas regras para serem utilizadas foram corretamente aplicadas

Verificar se as características técnicas da aplicação estão de acordo com os requisitos



Process Assessment

Mainly for RAMS

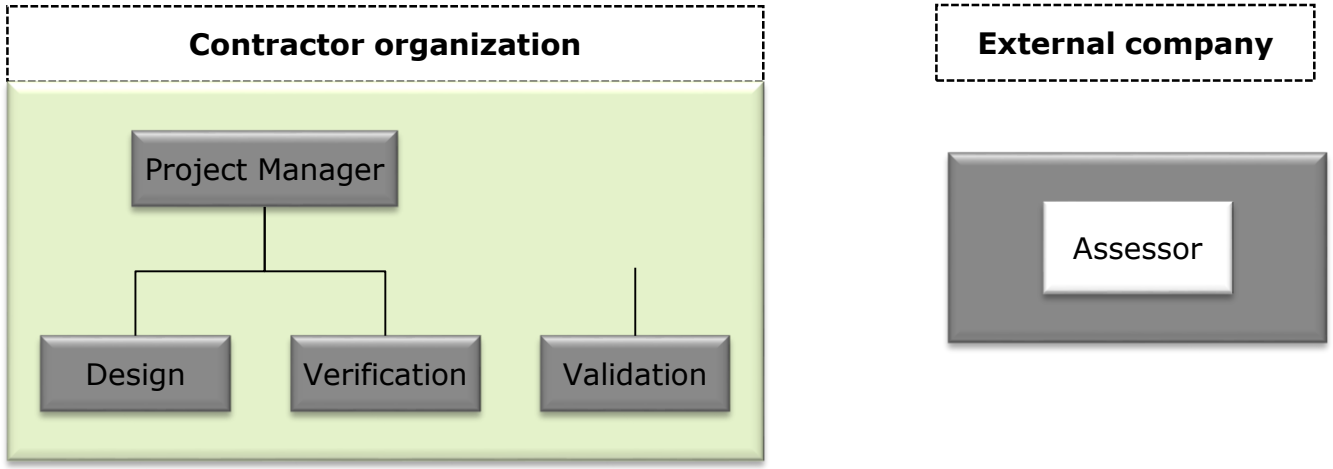
Product assessment

Presentation Outline

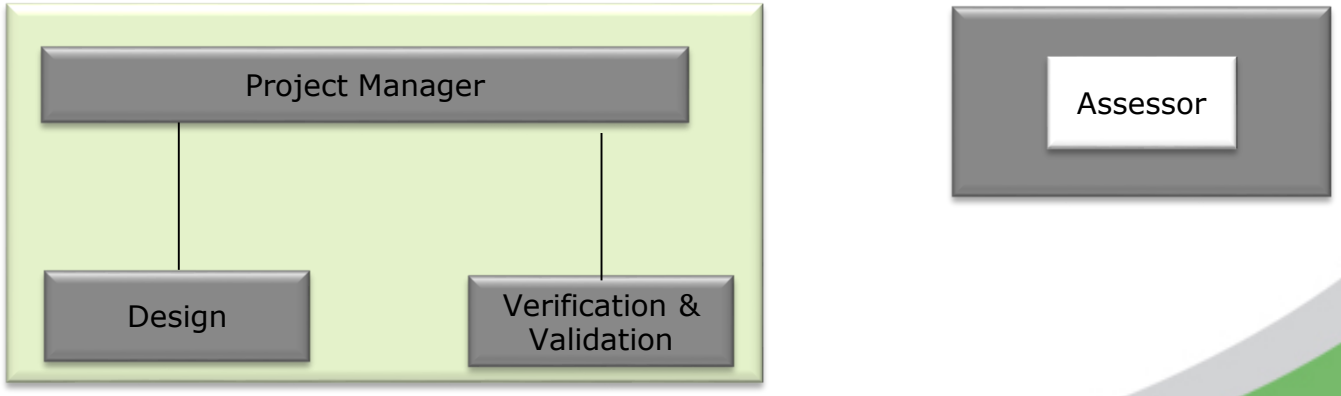
Independência e Imparcialidade

Independence w.r.t. the CENELEC/NoBo

SIL3/4



SIL1/2



Accreditation and Independence

- Para garantir a Independência/Imparciabilidade, o ISA deve ser acreditado pela norma ISO17020(Inspeção) e/ou ISO17065(Certificação). Esta acreditação confirmará que a entidade (ISA) NÃO SERÁ/NÃO DEVERÁ:

a) Responsável pela concepção, manufatura, distribuição e/ou manutenção do *PRODUTO CERTIFICADO*

b) Responsável pela concepção, utilização, operação ou manutenção do *PROCESSO CERTIFICADO*,

c) Responsável pela concepção, utilização, fornecimento ou responsável pelo serviço comercial do *SERVIÇO CERTIFICADO*,

d) *Propor ou fornecer atividades de consultoria*

- **PARTE 2 - Os níveis hierárquicos e a aceitação cruzada no processo de certificação de Segurança**

Parte 2

- Desenvolvimento estruturado
- Reutilização sem modificações – Aceitação Cruzada
- Reutilização com modificações – CSM e diretivas

Presentation Outline

Desenvolvimento estruturado

Structured Development and Cross Acceptance

Porque:

- Diminui a complexidade dos sistemas;
- Facilita a integração dos produtos;
- Multiplicidade de aplicações;
- Evita recertificações / novas avaliações.

Structured Development and Cross Acceptance

How and the impact on the certification

Produto Genérico

- Mesmo produto -> múltiplas aplicações
- Um Safety Case chamado (GPSC) focado na segurança do produto

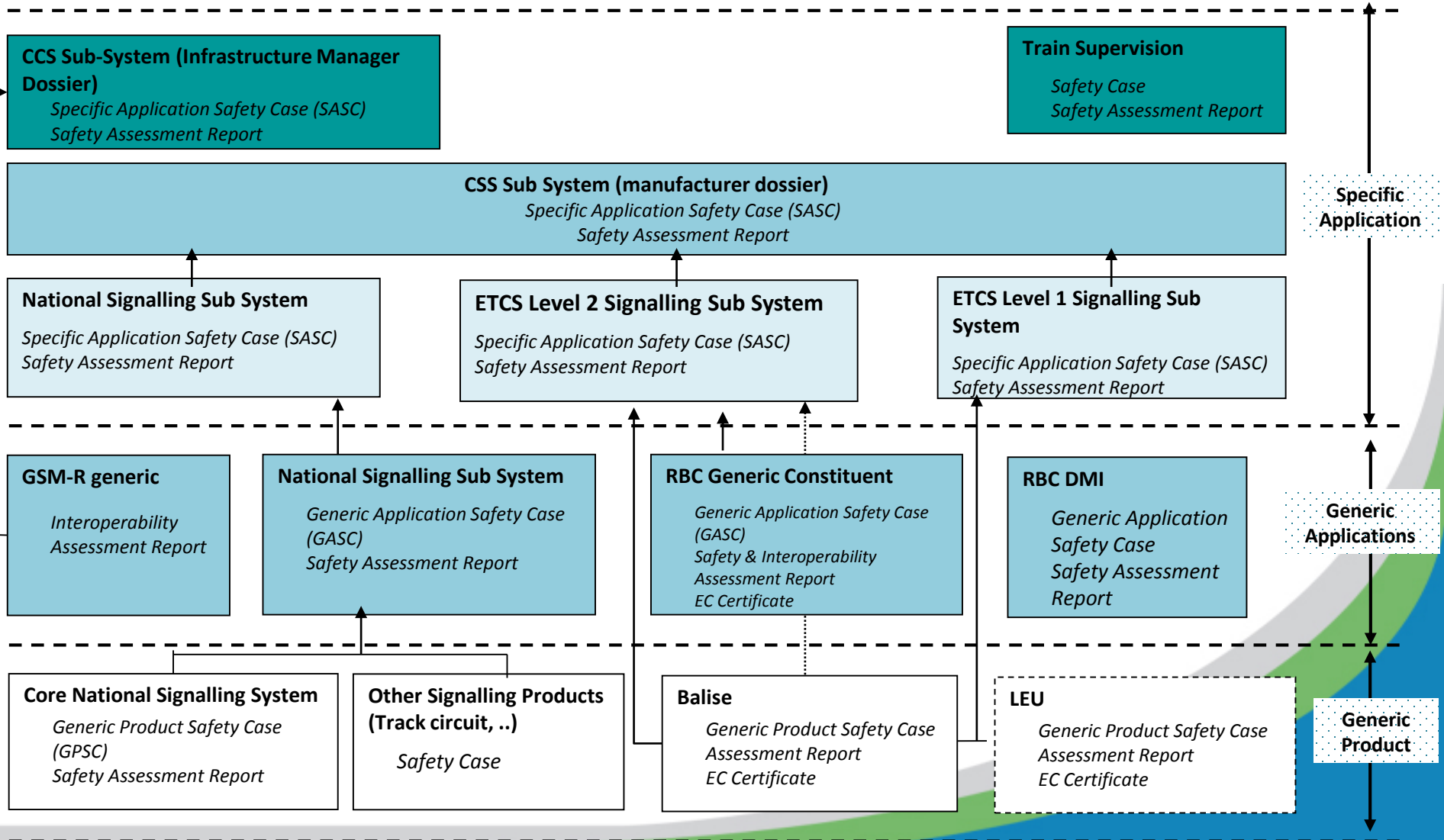
Aplicação Genérica

- Produto genérico adaptado (hardware e/ou software) para um tipo específico de sistema (por exemplo, processador vital para ser utilizado pelo ATP)
- Aceitação cruzada do GPSC
- Um Safety Case chamado (GASC) focado no processo de adaptação (development)

Aplicação Específica

- Aplicação Genérica adaptada (usualmente parametragem de software)para um projeto em específico (Por exemplo, ATP de bordo para ser utilizado no trem Z da linha X do Metro Y)
- Aceitação cruzada do GASC
- Instanciação (Design) para um projeto específico com base na topologia e parâmetros específicos

Structured Development: Example



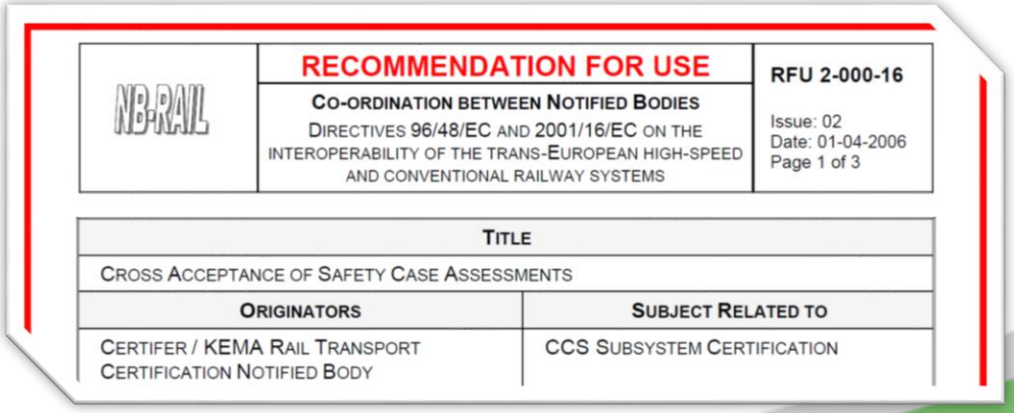
Reutilização sem modificações – Aceitação Cruzada

Application of Cross Acceptance

Criterio para aceitação de uma entidade ISA

O critério mínimo a ser avaliado para a aceitação dos resultados apresentados por uma entidade ISA, em relação a independência, competência e qualidade deve se basear em 3 elementos:

a. Acceptance of the ISA competency
b. Acceptance of the ISA entity
c. Acceptance of the safety assessment results



NB-RAIL

RECOMMENDATION FOR USE

CO-ORDINATION BETWEEN NOTIFIED BODIES

DIRECTIVES 96/48/EC AND 2001/16/EC ON THE INTEROPERABILITY OF THE TRANS-EUROPEAN HIGH-SPEED AND CONVENTIONAL RAILWAY SYSTEMS

RFU 2-000-16

Issue: 02
Date: 01-04-2006
Page 1 of 3

TITLE	
CROSS ACCEPTANCE OF SAFETY CASE ASSESSMENTS	
ORIGINATORS	**SUBJECT RELATED TO**
CERTIFER / KEMA RAIL TRANSPORT CERTIFICATION NOTIFIED BODY	CCS SUBSYSTEM CERTIFICATION

Reutilização com modificações – CSM e diretivas

Método comum de segurança

Método de determinação da profundidade de avaliação

Regulamentado na Europa pelo decreto 1136/2015 da comissão Européia de 13 / 7 / 2015

Règlement 402/2013

1)Règlement européen → exécution obligatoire

2) Méthode = outil. Attention ne remplace pas la nécessité de connaître et comprendre le ferroviaire

3) Sécurité : concerne la sécurité du système ferroviaire et en particulier la sécurité des opérations ferroviaires

4) Commune : Harmonisation au niveau européen → comparabilité, traitement égal des acteurs.

Campos de aplicação

- Deve ser aplicado sempre que houver uma modificação considerada **significativa** do sistema ferroviário **(article 4)**

- A modificação pode ser de natureza técnica, operacional ou organizacional (está tendo reflexo sobre a operação ou a manutenção)

Modificação significativa (article 4)

Se a modificação proposta está ligada a segurança, o proponente, suportado por um conselho de um especialista, determina a importancia desta modificação com base nos critérios abaixo:

Consequencia de uma falha

Inovação

Comprexidade

Acompanhamento

Reversibilidade

Adicionalidade

Changement significatif (article 4)

1) Changement n’est pas considéré comme significatif

➔ le proposant applique sa propre méthode de sécurité

2) Changement est considéré comme significatif

➔ le proposant doit appliquer le règlement MSC

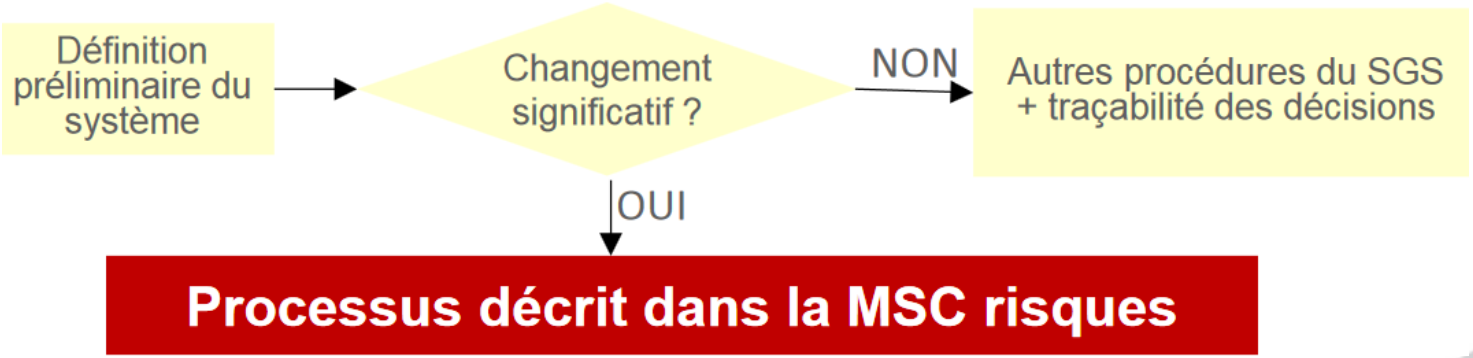
Changement significatif (article 4)

Qui détermine si un changement est significatif ?

1) Le proposant. Pas l'ANS
2) L'autorité nationale si règle nationale notifiée

Comment déterminer ?

- Sur avis d'experts
- Application des 6 critères de la MSC : les conséquences, innovation, complexité, insuffisance de contrôle, réversibilité, additionnalité



Changement significatif (article 4)

Evolution « peu importante » → Evolution « importante »				
Item A La conséquence d'une défaillance	Pas de conséquence à dire d'expert. ☐	La conséquence d'une défaillance n'est pas un évènement critique ☐	La conséquence d'une défaillance est un évènement critique avec boucle de rattrapage. ☒	La conséquence d'une défaillance est un évènement critique sans boucle de rattrapage. ☐
Item B L'innovation utilisée dans la mise en œuvre du changement	La modification respecte le cadre du prescrit existant sur le périmètre de l'évolution. ☐	La modification s'écarte du prescrit mais un système de référence existe au sein de l'entreprise. ☐	La modification s'écarte du prescrit et il n'existe pas de système de référence au sein de l'entreprise. ☐	La modification s'écarte du prescrit et une autorisation externe à l'EF SNCF doit être obtenue. ☒
Item C La complexité du changement.	Entité interne à l'EF SNCF			Entité externe à l'EF SNCF
	Le promoteur a autorité sur l'ensemble du périmètre impacté par le changement. Ou le changement ne nécessite pas la création ou la modification de processus. ☐	Le promoteur n'a pas l'autorité sur l'ensemble du périmètre impacté par le changement. Mais le changement ne concerne que l'entité dont le promoteur dépend. Ou le changement nécessite la création ou la modification de processus maîtrisés par l'entité dont le promoteur dépend. ☐	Le promoteur n'a pas l'autorité sur l'ensemble du périmètre impacté par le changement. Et le changement concerne les interfaces à l'extérieur de l'entité dont le promoteur dépend. Ou le changement nécessite la création ou la modification de processus maîtrisés par l'EF SNCF. ☐	Le promoteur n'a pas l'ensemble du périmètre impacté sous son autorité. Et le changement concerne les interfaces avec l'extérieur de l'EF SNCF. Ou le changement nécessite la création ou la modification de processus en interface avec l'extérieur de l'EF SNCF. ☒
Item D Le suivi	Entité interne à l'EF SNCF			Entité externe à l'EF SNCF
	Le promoteur assure le suivi de la modification et ce suivi est réalisé dans son entité. ☐	Le promoteur assure le suivi de la modification et ce suivi est réalisé par l'entité dont le promoteur dépend. ☐	Le suivi de la modification est assuré par le promoteur moyennant la mise en place d'une organisation en interface avec des entités de l'EF SNCF. ☐	Le suivi de la modification est assuré par le promoteur moyennant la mise en place d'une organisation en interface avec des entités hors de l'EF SNCF. ☒
Item E La réversibilité (après changement)	Un retour en arrière total est possible à périmètre constant de la situation initiale. ☒	Un retour en arrière partiel est réalisable vers la situation initiale et sans dégradation du niveau de sécurité initial. ☐	Un retour en arrière partiel est réalisable vers la situation initiale et avec dégradation du niveau de sécurité initial. ☐	Le retour en arrière est impossible dans le cadre du projet. ☐
Item F L'additionnalité	Aucune évolution dans les 2 dernières années ☒	1 évolution non-significative dans les 2 dernières années. ☐	Plusieurs évolutions non-significatives dans les 2 dernières années ou 1 évolution dans la dernière année. ☐	Au moins 1 évolution significative dans les 2 dernières années. ☐

CERTIFER

Annexe 1 : Processo de gestão de risco e avaliação independente

0 : Mudança significativa

1 : Definição do Sistema

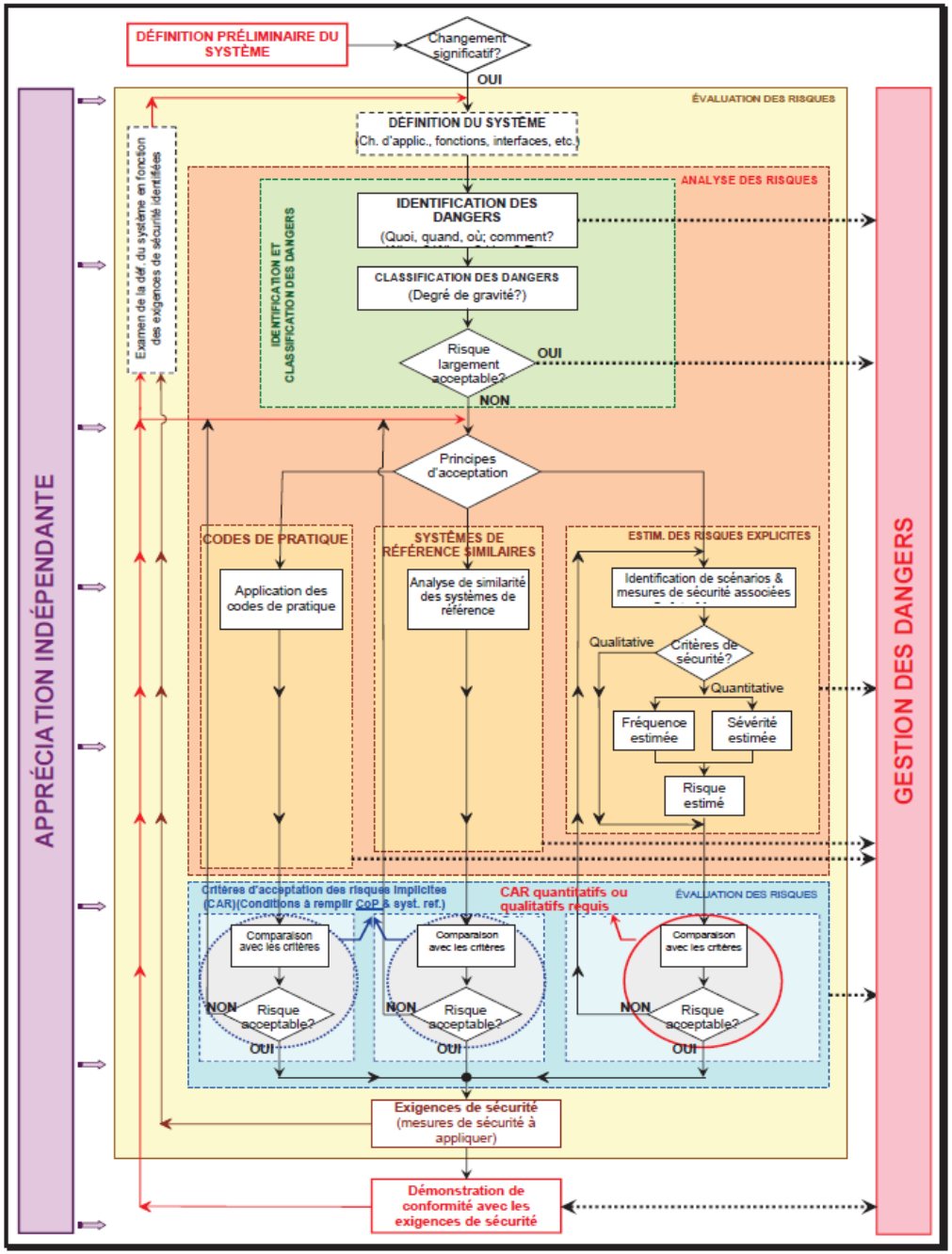
2 : Identirficação dos perigos
classificação dos perigos
Aceitação dos perigos

3 : princípios de aceitação:
- *regras de arte (PiU)*
- *GAME*
- *estimação explicita*

4 : Avaliação dos riscos

5 : Exigencias de segurança

6 : Demonstração de conformidade as exigências de segurança



Exemples

Changement de nature technique :
Transmission of the traction and braking command (Rolling Stock)
Emergency braking functionality of a Rolling Stock.
Swiss NSA - Micro LX (Infra).
Automatic LX with light signals to road users and train drivers (Infra).
Interlocking (Infra).
Trainborne Hot Box Detector.
Train door opening authorization

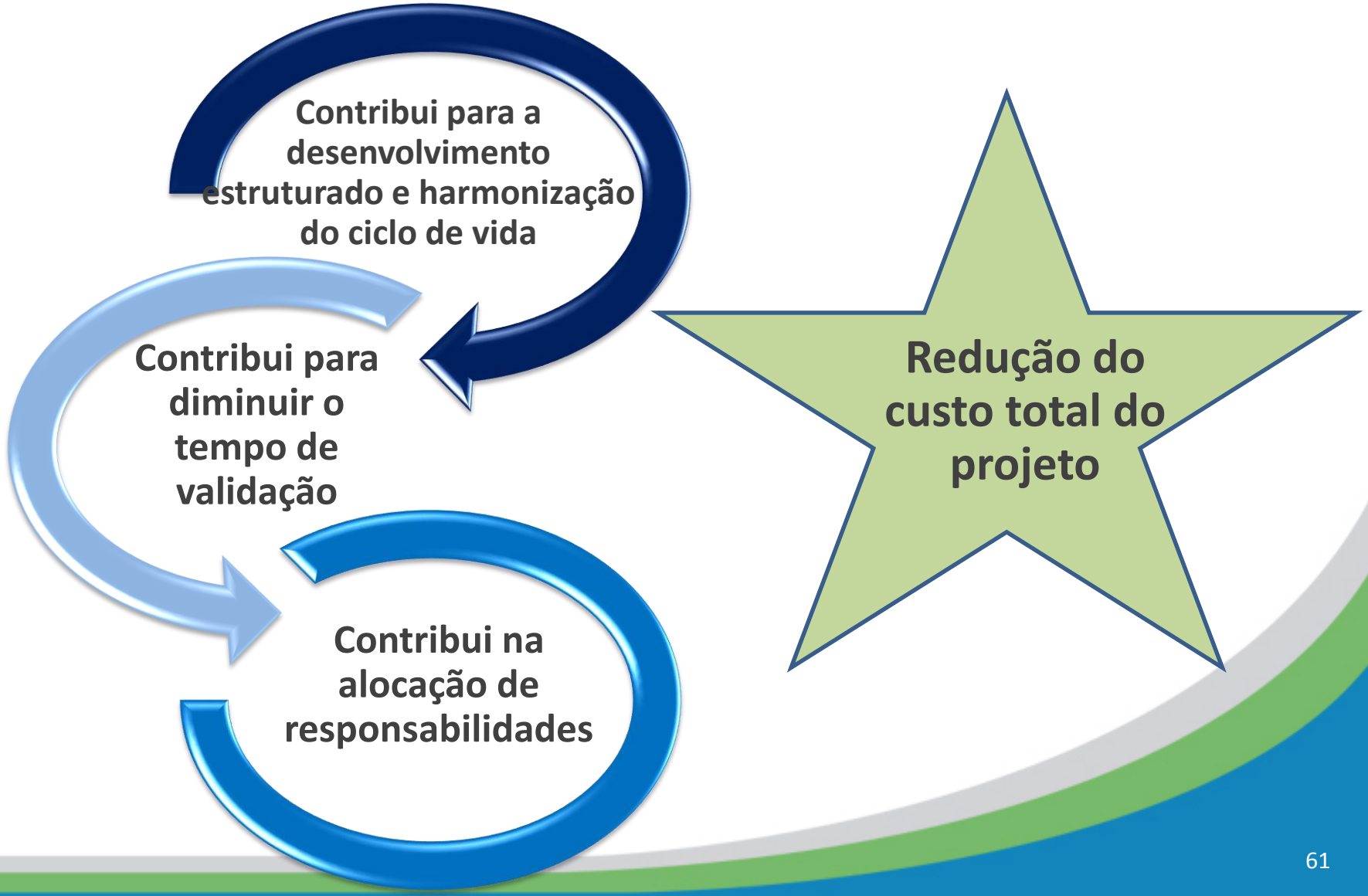
Changement de nature organisationnelle :
Modification d' organisation : reconstruction du poste de Vitry

Changement de nature opérationnelle :
Modification du processus d'échange des e-depeches dans
le cadre de l'organisation des travaux.
MSC relative à l'utilisation de la RSTpour assurer la protection arrière
voyageurs sur la section de ligne Schweighouse-Haguenau, exploitée
agent seul

Changement de nature organisationnelle et opérationnelle :
Automatisation des PN à CROIX DE SAINT ANDRE – PN à SAL2 GN :
Industrialisation de la mise en œuvre des PN GN

Merci pour votre attention,
Des questions ?

Conclusão


Contribui para a desenvolvimento estruturado e harmonização do ciclo de vida
Contribui para diminuir o tempo de validação
Contribui na alocação de responsabilidades
Redução do custo total do projeto

Contact us

In America Latina:

By phone at: +55 11 5085 5391

On our web site: www.certifer.eu

By e-mail address at: aryldo.russo@certifer.eu
jose.orbino@certifer.eu

Or visit us at: Certifer America Latina
Avenida Rebouças, 1169
05401 - 150 Sao Paulo
Brazil