

# Implémentation de la CEI 61508 dans le secteur de l'énergie :

## Exemple de certification

**Workshop SIPI 2003**



**BUREAU  
VERITAS**

**Benjamin NICOLAS**

01 47 14 33 45

[benjamin.nicolas@fr.bureauveritas.com](mailto:benjamin.nicolas@fr.bureauveritas.com)

Dans l'intérêt des entreprises et des Hommes

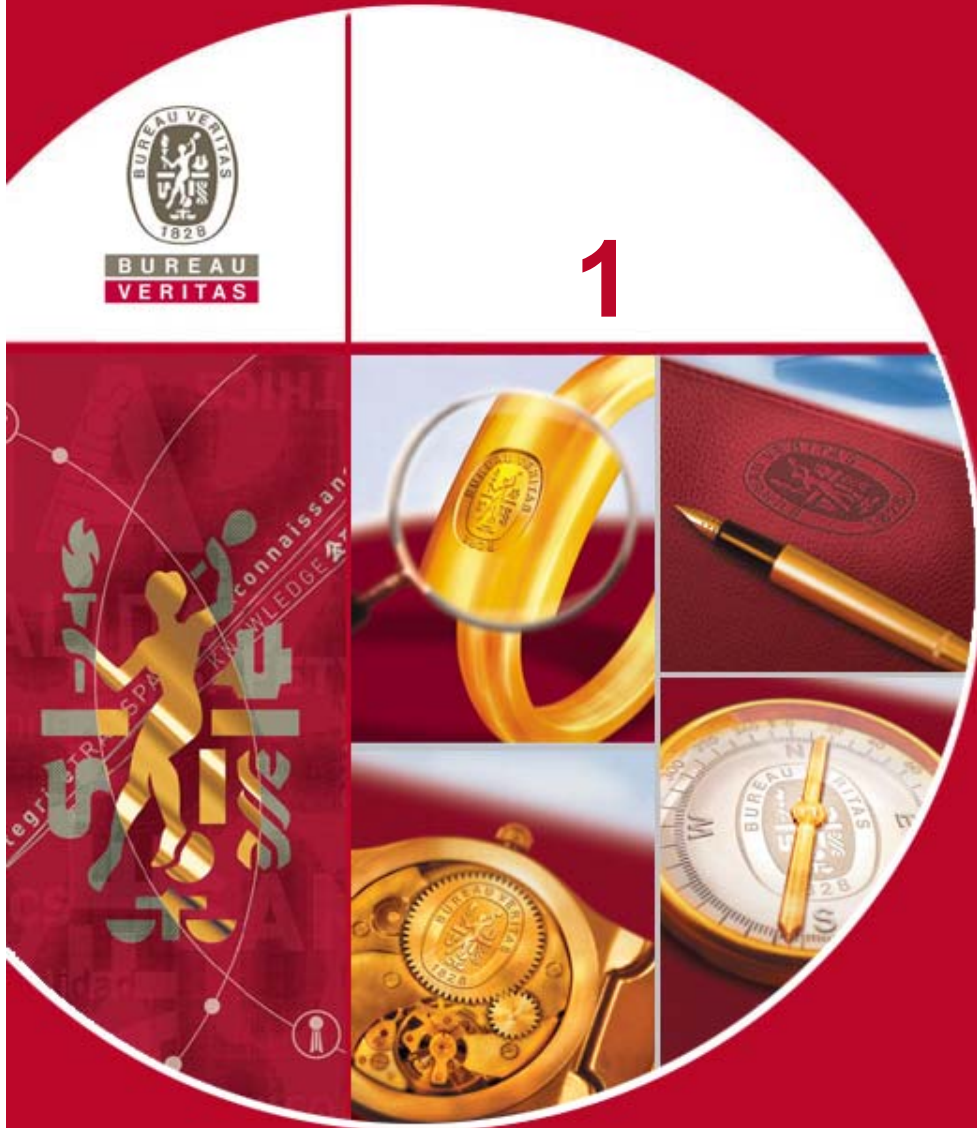


BUREAU  
VERITAS

## SOMMAIRE

- 1 Présentation du projet
- 2 Résultats
- 3 Faits Marquants





## > Présentation du projet

▶ **Client :**

- ABB Power Automation, Baden, Suisse.

▶ **Dates :**

- De Février 2002 à Août 2002

▶ **Objectifs :**

- Délivrer à ABB un certificat de conformité pour leur système de protection contre la survitesse pour les turbines à gaz et à vapeur vis-à-vis de la norme CEI 61508
- Objectif : SIL 3

▶ **Langue de travail :**

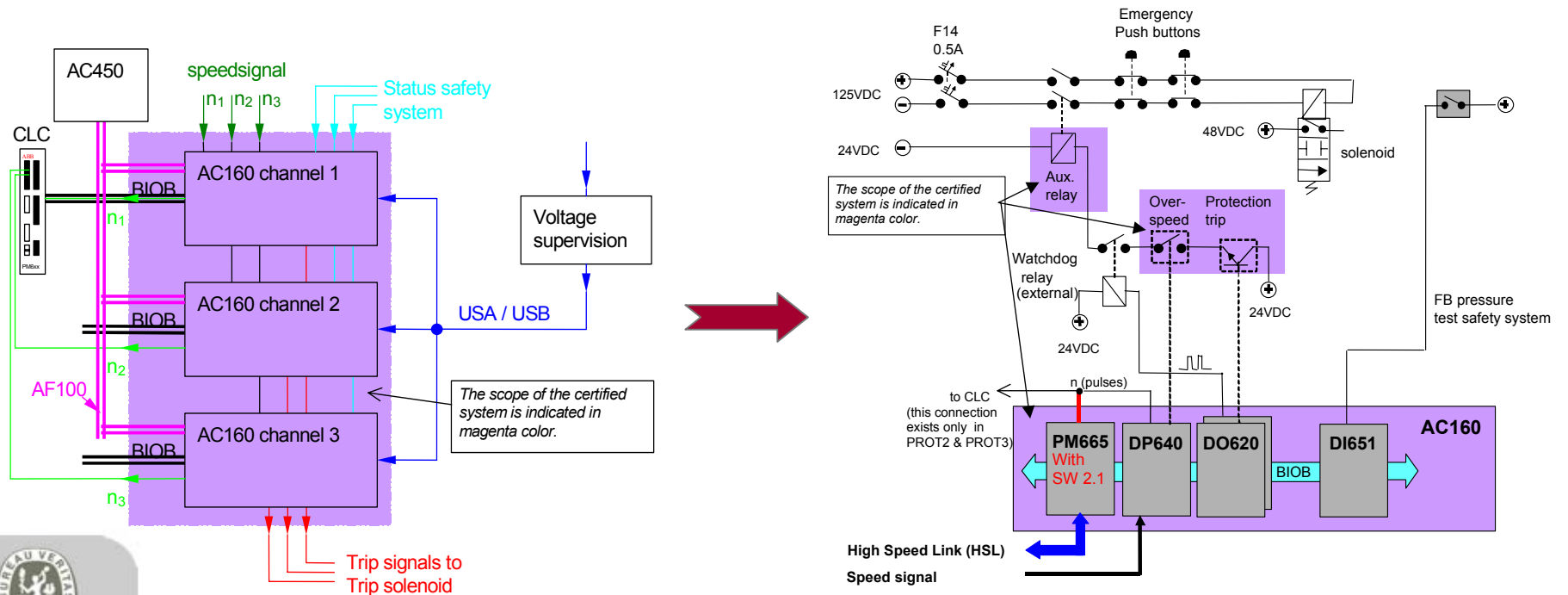
- Anglais

► **Système :**

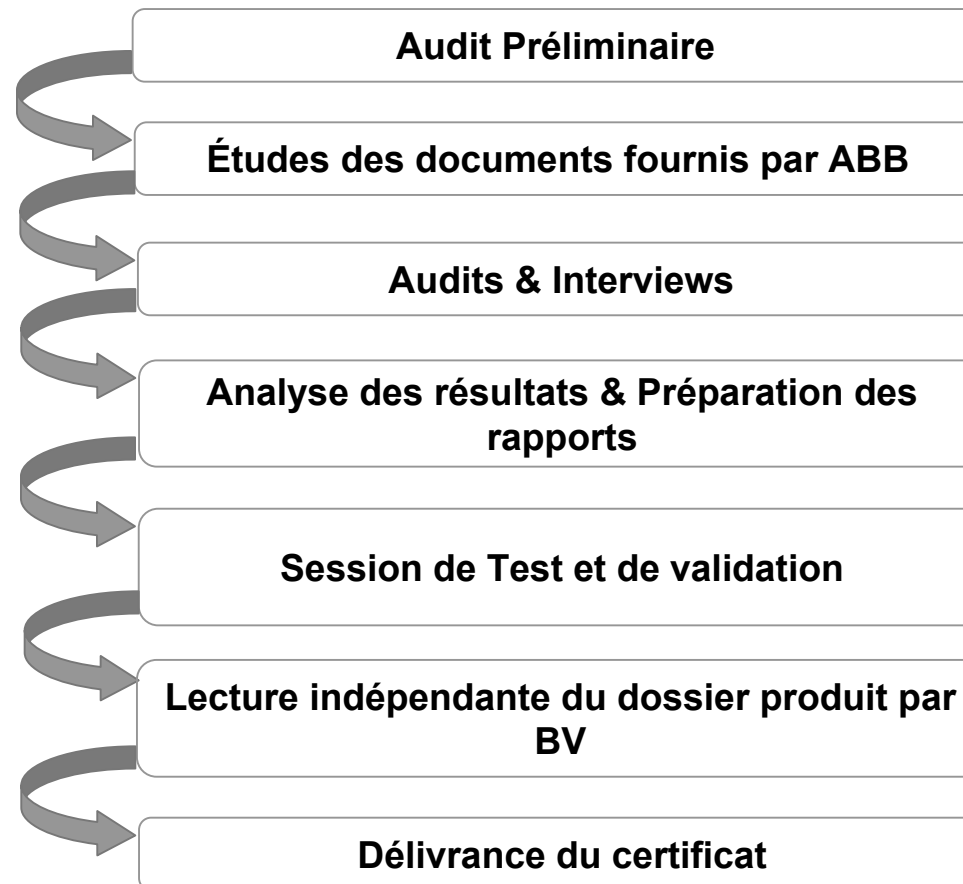
- **Système de protection contre la survitesse**

- » **3 sous-systèmes AC 160 en 2oo3**

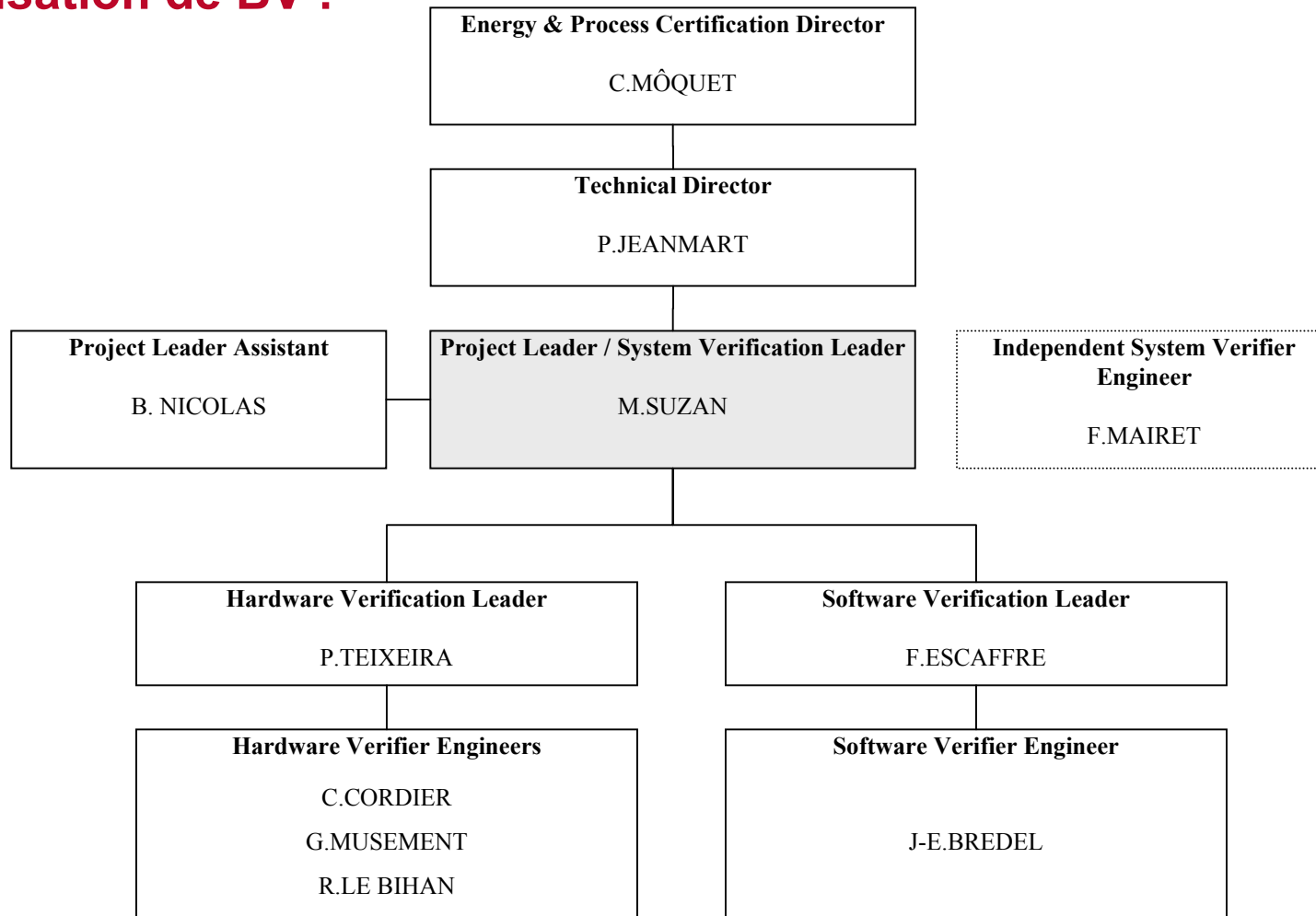
- » **Chaque sous-système est composé de plusieurs cartes selon les schémas ci-dessous**



- Les principales tâches de BV sont données ci-dessous :



## ► Organisation de BV :





BUREAU  
VERITAS

2




➤ Résultats

### ► **Références ABB :**

- **Les exigences de la norme ont été analysées sur la base notamment :**
  - » **des documents de gestion de projet & qualité produits par ABB,**
  - » **des documents décrivant le matériel produits par ABB,**
  - » **des documents décrivant le logiciel produits par ABB,**
  - » **d'interviews des développeurs Logiciel & Matériel ABB,**
  - » **d'interviews des chefs de projet, des responsable qualité d'ABB,**
  - » **d'interviews des responsables de vérification et validation d'ABB.**

- ▶ Objectifs : SIL 3
- ▶ Système 2003 : Tolérant à 1 anomalie
- ▶ Faible Sollicitation.

Safety integrity level (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand)
3	$\geq 10^{-4}$ to $10^{-3}$



Safe failure fraction	Hardware fault tolerance		
	0	1	2
60%	Not allowed	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	<b>SIL 3</b>	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4




Table 2: Architectural constraints on type B safety related subsystems

▶ **Résultats Qualitatifs:**

- Une matrice de conformité a été élaborée par BVC. Celle-ci reprend tous les points de la norme et indique la référence ABB correspondante.

▶ **Résultats Quantitatifs :**

- Étude du système Matériel & Logiciel
- AMDEC des sous-systèmes
- Étude de la couverture de diagnostic
- Évaluation du Beta Factor

▶ **Résultat :**

- Seule la carte DP 640 permet la protection contre la survitesse indépendamment des autres.

▶ **Chiffres :**

» **Beta Factor : 2%**

» **MTTR : 6h**

» **T1 : 672h**


» **PFD = 1,48E- 4**                   ( < 1E-3 )

» **SFF = 92%**                       ( > 90% )

▶ **Conclusion :**

» **Le système de protection contre la survitesse est bien SIL 3 selon la norme CEI 61508**

► **Certificat délivré :**

		
<b>CERTIFICATE OF COMPLIANCE FOR ABB Power Automation</b>		
<p><b>Reference:</b> BN/MS/A3.1011462/02/C/253/0</p>		
<h2 style="color: red;">BUREAU VERITAS</h2>		
<p>certifies that the design of the Overspeed Protection System for Gas and Steam Turbines based on triple redundant Advant Power<sup>®</sup> AC 160 architecture – the protection is ensured by DP640 module – as presented to BUREAU VERITAS, complies with the IEC 61508 level SIL3 standard ("Functional safety of electrical/electronic/programmable electronic safety-related systems") with respect to the risk of failure of the protection.</p>		
<p>For the purpose of the present certificate, the texts referred to are the following IEC 61508 :</p> <ul style="list-style-type: none"> <li>• Part 1 - 1998-12 , 1<sup>st</sup> edition</li> <li>• Part 2 - 2000-05 , 1<sup>st</sup> edition</li> <li>• Part 3 - 1998-12 , 1<sup>st</sup> edition</li> <li>• Part 4 - 1998-12 , 1<sup>st</sup> edition</li> <li>• Part 5 - 1998-12 , 1<sup>st</sup> edition</li> <li>• Part 6 - 2000-04 , 1<sup>st</sup> edition</li> <li>• Part 7 - 2000-03 , 1<sup>st</sup> edition</li> </ul>		
<p>The list of components of the above system is described in the ABB document "<u>Parts List - AC160 Turbine Overspeed Protection IEC 61508 SIL3</u>" dated 05/27/2002 and referenced <u>1KHZ.101993</u>.</p>		
<p>The installation, start-up, user instructions, and maintenance literature related to that system are stated in the document reference <u>3BDS.005.555R301</u> dated <u>November 2001</u>.</p>		
<p>The main characteristics of the system planned by ABB are the following:</p> <ul style="list-style-type: none"> <li>• Three channel fail safe system : 2oo3 protection system,</li> <li>• DP 640 is used for measurement conditioning of the speed probes,</li> <li>• DP 640 is able to de-energise independently the turbine.</li> </ul>		
<p>The reviews performed by BUREAU VERITAS in order to certify the compliance of the above design are recorded in the "IEC 61508 Compliance of ABB Turbine Over-speed Protection System - Overall Report" which is fully part of the present certificate and referenced <u>BN/MS/A3.1011462/02/R/246/0</u> dated <u>07/26/2002</u>.</p>		
<p>The present certificate issued for ABB relates exclusively to the design of the above system.</p>		
<p>The present certificate is valid only for a system exclusively provided to and used by professionals. The present certificate is subject to the terms of BUREAU VERITAS General Conditions of services.</p>		
<b>Michel SUZAN</b> Product Manager	<b>Philippe JEANMART</b> Technical Director	<b>Christian MOQUET</b> Energy & Process Certification Director
<i>July, 26th 2002</i>		
<p><b>BUREAU VERITAS</b> 10, rue Jacques Daguerre - 92565 Rueil-Malmaison cedex, FRANCE Phone : 00 33 147 143 388 - FAX : 00 33 147 143 399</p>		



3



## > Faits Marquants

▶ **Pour BV :**

- Étude d'un haut niveau technique
- Image d'une société innovante (ce certificat est un des premiers délivrés dans le monde des turbines)

▶ **Pour ABB:**

- Connaissance accrue de leur système
- Amélioration de leur gestion de projet
- Avantage concurrentiel grâce à l'évaluation tierce partie.

- ▶ **Les interlocuteurs ABB n'étaient pas tous formés à la norme au début du projet.**
- ▶ **La recherche des données fut longue car les développements ont eu lieu plusieurs années avant.**
- ▶ **La connaissance du système initiale n'était pas suffisante (étude sur toute le sous-système AC160 puis seulement sur le DP640)**