Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 07 avril 2005

N° 1027/SGDN/DCSSI/SDS/LSC

Fournitures attendues pour la qualification TEMPEST d'un équipement

Version : 1.0

Ce document comporte 13 pages.

SUIVI DES VERSIONS

Version	Date	Nature
1.0	18 février 2005	Révisions majeures du document
0.9	20 janvier 2005	Création du document

SOMMAIRE

Introduction

Ce document liste les exigences en termes de fournitures pour la réalisation de l'évaluation TEMPEST d'un équipement. L'obtention de l'ensemble des éléments décrits dans ce document conditionne le démarrage de l'étude du produit.

Les éléments demandés concernent :

- **La description fonctionnelle** de l'équipement. Par définition, la description fonctionnelle représente une description de haut niveau de l'interface visible par l'opérateur du comportement de l'équipement à tester.
- **Les documents de conception de haut niveau**. Par définition, les documents de conception de haut niveau apportent une description de l'équipement à tester en termes d'éléments structurels principaux (i.e. sous-systèmes) et relient ces éléments aux fonctions qu'ils remplissent.

  Les documents de conception de haut niveau sont un raffinement de la description fonctionnelle pour chaque sous-système.
- **Les documents de conception de bas niveau**. Par définition, ces documents traduisent l'implémentation matérielle retenue pour réaliser chaque sous- système.

  Parmi ces documents peuvent être cités à titre d'exemple :
  - les schémas d'implantation des cartes électroniques (côté composant, côté(s) cuivre)
  - les plans de câblage ;
  - …
- **Les outils** (équipement à évaluer, logiciel d'émulation de flux, matériel de stimulation) nécessaires à la mise en œuvre fonctionnelle des sous-systèmes du produit qui devra être réalisée depuis les interfaces visibles par l'opérateur.

1. Description fonctionnelle

La description fonctionnelle de l'équipement doit permettre d'apprécier notamment :

- la norme visée par la qualification du matériel ;
- la fonction élémentaire que remplit le matériel ;
- son environnement de fonctionnement ;
- la manière dont il est utilisé et les interactions qu'il peut avoir avec des éléments extérieurs ;
- la manière dont il doit être installé ;
- s'il s'agit d'un équipement de série ou d'un prototype ;
- …

Par exemple : *L'équipement se présente sous la forme d'une station de travail constituée d'une unité centrale, d'un moniteur vidéo, d'un clavier et d'une souris. Il est connecté au réseau : nom_du_réseau, grâce auquel il a accès au système lambda de partage de données. Les échanges de données entre l'équipement et le système lambda sont chiffrés.*

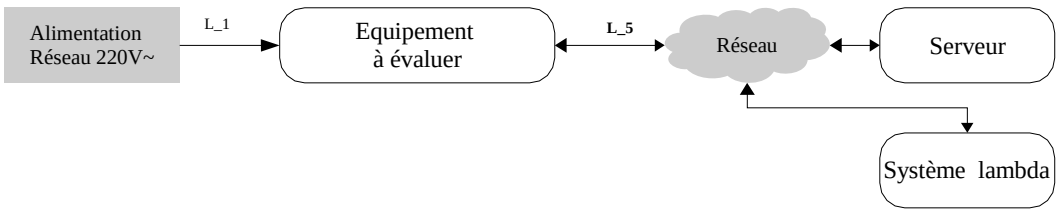
Marque :

Référence :

N° de série :

Ou encore *L'équipement est constitué d'un boîtier principal accueillant le cœur cryptographique. Il est équipé de trois interfaces de communication respectivement connecteés à un injecteur de clés, à l'équipement de terminaison et au réseau de communication.*

Cette description peut être agrémentée d'un schéma représentant l'équipement dans son environnement.



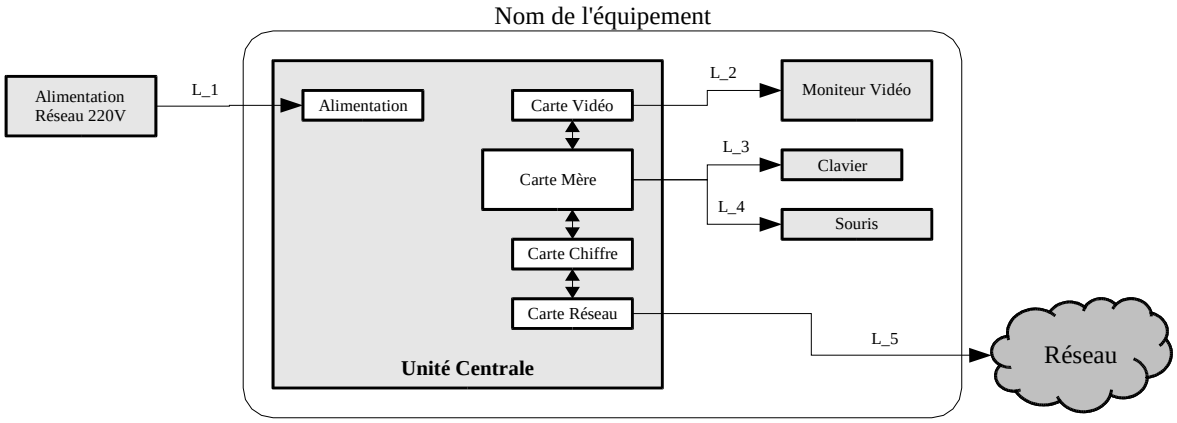
2. Documents de conception de haut niveau

Les documents de conception de haut niveau doivent permettre de comprendre le fonctionnement général de l'appareil en le découpant en sous-systèmes (i.e. affichage,

chiffrement, clavier, injecteur, lecteur de cartes…). Par ailleurs, ils doivent présenter les lignes d'interfaces reliant les sous-systèmes.

Un schéma représentant l'ensemble des sous-systèmes ainsi que les lignes d'interfaces doit être joint. Chaque sous-système et ligne d'interface doit être clairement identifié à l'aide d'un identifiant unique.

Exemple de schéma :



2.1. Les sous-systèmes

Chaque sous-système doit être décrit (i.e. identifiant, rôle au sein de l'équipement, modes de fonctionnement et ensemble des configurations possibles).

Exemple :

Moniteur Vidéo : Il affiche les données que lui fournit l'unité centrale. Les résolutions d'affichages disponibles sont : 1024*768, 800*600, 640*480.

Marque : ……

Réf : ……

N° de série

Unité Centrale : ……

2.2. Les lignes d'interfaces

Cette rubrique doit lister l'ensemble des lignes d'interfaces de l'équipement. La description d'une ligne doit comporter un identifiant unique, la fonction de la ligne au sein de l'équipement, la source et la destination des informations véhiculées. Pour chaque ligne, le ou les connecteurs devront être définis broche à broche. (n° de broche accompagné d'un commentaire).

Exemple de liste :

L_x : elle véhicule les informations en provenance de ……. à destination de ……. Elle est conforme au standard …….

Connecteur xx mâle	
Broche	*Commentaire*
1	*Masse*
2	*VCC*
3	*D_0*
4	*…*

Connecteur yy femelle	
Broche	*Commentaire*
1	*Masse*
2	*VCC*
3	*…*

L_y : …

3. Documents de conception bas niveau

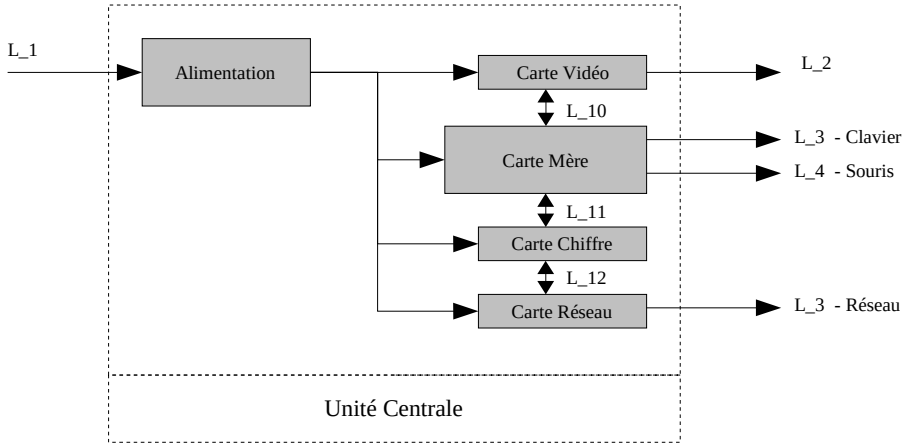
A partir des éléments présentés au paragraphe 2, ces documents reprennent les sous-systèmes précédemment listés et doivent en faire l'analyse détaillée. C'est-à-dire que chaque sous-système doit être détaillé en modules. Chaque module doit être identifié à l'aide d'un identifiant unique.

La seconde partie de l'analyse doit indiquer les lignes d'interfaces utilisées par les modules pour communiquer entre eux.

3.1. Schéma fonctionnel et description des modules

Un schéma par sous-système représentant ses modules et les lignes d'interfaces doit être fourni.

Exemple : Le module Unité Centrale



Pour chaque module identifié, une description détaillée doit être réalisée (identifiant, rôle au sein de l'équipement, modes de fonctionnement, configurations disponibles…).

Exemple :

Alimentation : elle fournit les tensions continues de 3,3V, 5V et 12V à partir de la tension secteur 220V alternatif, sa puissance est de 300 Watts. Elle intègre également des fonctionnalités de protection contre les courts-circuits, elle est distribuée vers les modules …

Marque : ……

Réf : ……

N° de série : ……

3.2. Les lignes d'interfaces

L'ensemble des lignes d'interfaces de chaque sous-module doit être décrit. Cette description comprend notamment :

- l'identifiant qui doit être unique ;
- le protocole utilisé ;
- la nature du signal véhiculé ;
- la source et la destination du signal ;
- le type et le brochage des connecteurs (n° de broche accompagné d'un commentaire).

Exemple de liste :

L_10 : elle véhicule les informations en provenance du micro-contrôleur à destination de la carte vidéo. La communication est conforme au protocole WW. Les données sont transmises sur xx bits en parallèle au débit de xxMo/s.

Connecteur xx mâle	
Broche	*Commentaire*
1	*Masse*
2	*VCC*
3	*D_0*
4	*…*

L_y : …

3.3. Modes d'utilisation

L'objectif des essais à réaliser est de vérifier que dans chacun des modes d'utilisation, le produit ne génère pas de perturbation dont le niveau ne soit pas acceptable. Pour cela, il est donc nécessaire de lister tous ses modes d'utilisation. A chacun d'eux sera associé un flux de données.

Chaque mode devra comporter :

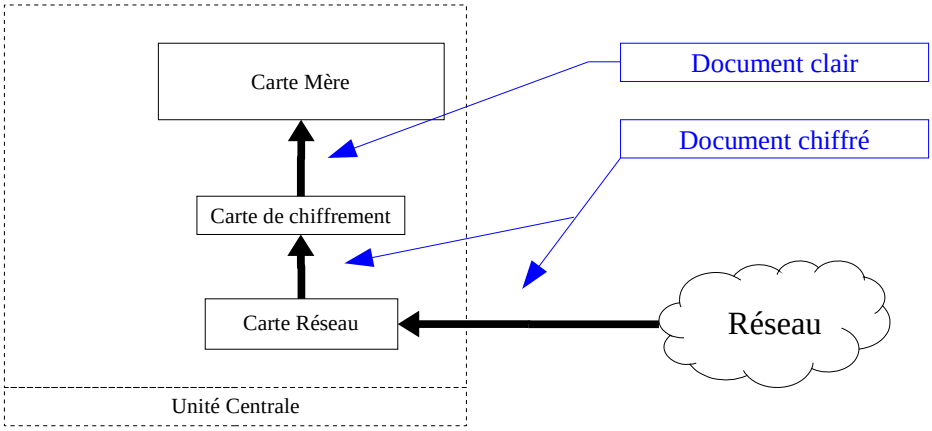
- un schéma global où doit apparaître le cheminement du flux de données dans l'équipement,
- une description détaillée du flux,
- une description de la mise en œuvre opérationnelle du mode (cf paragraphe 4),
- un schéma détaillé des circuits mis en œuvre,
- une description des signaux électriques qui composent le flux. Elle sera faite comme suit :

Identifiant du signal : *identifiant du flux – identifiant du signal*	
Emetteur	
Signal analogique ou numérique	
Mode de transfert	
Nombre de bits	
Format	
Répétitivité	
Parité	
Synchrone / Asynchrone	
Code	
Amplitude du signal	
Largeur du bit unitaire (à mi-hauteur)	
Temps de montée (entre 10% et 90%)	
Temps de descente (entre 10% et 90%)	
Temps de répétition (si répétitif)	

Type de code correcteur d'erreur ou code de compression de données	
Type de modulation (si analogique)	
Signal Clair ou chiffré	
Mode d'émission (EVF)	

3.4. Exemple de description d'un mode d'utilisation et du flux associé :

Réception de données sur le port Ethernet – Flux_F



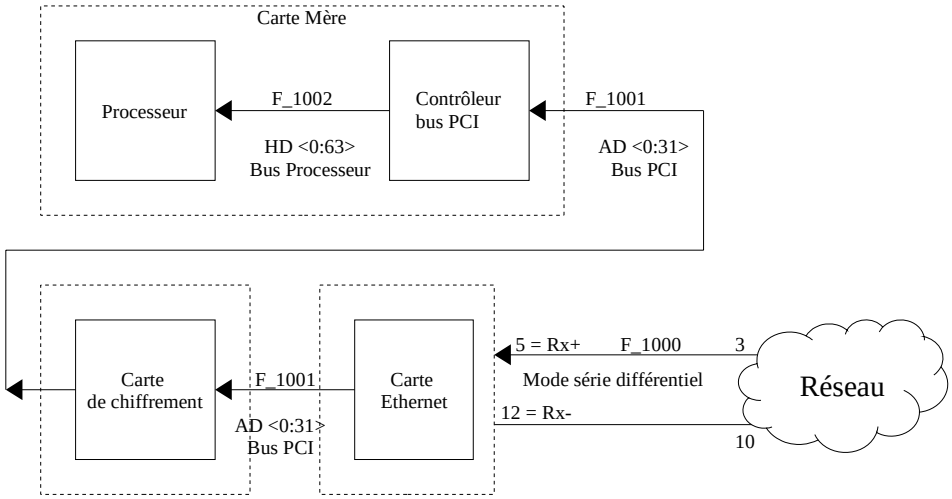
Description du flux

La réception se fait via la carte éthernet qui envoie les données chiffrées à la carte chiffre, qui à son tour les transmettra via le bus PCI à la carte mère de l'unité centrale. …

Programme de test

L'émulation de ce flux consiste à établir une liaison entre l'équipement et le réseau. A l'aide du programme d'émulation : nom_du_programme, l'équipement va pouvoir communiquer avec un serveur distant et ainsi recevoir des données….

Schéma détaillé des circuits mis en œuvre



Description des signaux

Identifiant du signal : F_1000	
Emetteur	Réseau
Signal analogique ou numérique	numérique
Mode de transfert	Bus série, différentiel
Nombre de bits	8 bits (sans start, ni parité, ni stop)
Format	RZ
Répétitivité	Non répétitif
Parité	Sans
Synchrone / Asynchrone	Synchrone
Code	MANCHESTER
Amplitude du signal	1,4V
Largeur du bit unitaire (à mi-hauteur)	50 ns
Temps de montée (entre 10% et 90%)	8 ns
Temps de descente (entre 10% et 90%)	6 ns
Temps de répétition (si répétitif)	
Type de code correcteur d'erreur ou code de compression de données	Encodage de Hamming
Type de modulation (si analogique)	
Signal Clair ou chiffré	Chiffré
Mode d'émission (EVF)	

Identifiant du signal : F_1001	
Emetteur	Carte Ethernet
Signal analogique ou numérique	numérique
Mode de transfert	Bus // PCI
Nombre de bits	……

3.5. Porteuses potentielles

Les horloges doivent faire l'objet d'une description succincte.

Exemple :

Carte mère - Fréquence fixe à 100 MHz - Fréquence fixe à 48 MHz - Oscillateur à 32,768 MHz
Carte Vidéo - Fréquence fixe à …… Hz

3.6. Risques potentiels et précautions prises

Si l'équipement présente un ou plusieurs risque(s) potentiels identifié(s), ils devront être indiqués et les précautions opérationnelles devront être précisées.

3.7. Les documents de conception

Les documents suivant sont également à fournir pour l'évaluation du produit :

- Le manuel utilisateur ;
- Le manuel d'installation ;
- Les documents de conception (spécification fonctionnelle et schémas d'implantations, de câblage …) ;
- Le dossier de conception de durcissement (s'il existe) ;
- La description des interfaces avec l'extérieur (câblage et standard des connecteurs).

4. Les outils

Les essais sont effectués avec l’équipement en situation opérationnelle réelle ou simulée. Ceci implique que l’équipement soit fourni avec l’ensemble des matériels et logiciels nécessaires à sa mise en oeuvre. Les outils fournis doivent permettrent d'activer l'ensemble des modes d'utilisation.

4.1. Exigences matérielles

Les équipements doivent être fournis en nombre suffisant pour permettre la mise en œuvre de l’ensemble des modes d’utilisation (exemple : équipement de radiocommunication émetteur/récepteur). Dans la mesure du possible, un minimum de deux équipements est souhaité (un pour prélever les signaux, l'autre pour les essais). Par ailleurs, l’équipement doit être fourni avec le câblage approprié. Enfin, si des équipements annexes sont utilisés pour stimuler l’équipement, ils doivent être fournis pour la qualification et leur installation/configuration doit être précisée.

4.2. Exigences relatives à la stimulation des modes opératoires

Pour chacun des modes d'utilisation recensés, un scénario de test doit être fourni (vecteur). Celui-ci doit comprendre la configuration matérielle à utiliser (positionnement de l'équipement et des matériels de stimulation) et éventuellement le logiciel à utiliser pour stimuler le mode.

Dans le cas où la mise en œuvre des modes opératoires se fait de façon logicielle, les guides d’installation et d’utilisation de chaque programme doivent également être fournis. Dans le cas où l’équipement est un micro-ordinateur, le système d’exploitation utilisé doit être installé, et les mots de passe doivent être fournis.

A la demande de l'opérateur, les outils de mise en œuvre devront permettrent de stimuler le flux jusqu'à ce qu'il intervienne à nouveau pour interrompre l'opération.