



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Paris, le 23 juin 2014

*Agence nationale de la sécurité
des systèmes d'information*

INSTRUCTION INTERMINISTERIELLE N° 300

LA PROTECTION CONTRE LES SIGNAUX COMPROMETTANTS



HISTORIQUE DES VERSIONS			
DATE	VERSION	ÉVOLUTION DU DOCUMENT	RÉDACTEUR
Novembre 2013	Initiale 1.0	La présente instruction abroge l'instruction interministérielle n°300/SGDN/TTS/SSI/DR du 20 juin 1997 sur la protection contre les signaux compromettants.	ANSSI
20/11/2013	1.1	Version enregistrée sous le numéro 4021/ANSSI en date du 20/11/2013	ANSSI
23/06/2014	1.2	Annule et remplace la version 1.1 Version enregistrée sous le numéro 2512/ANSSI en date du 23/06/2014	ANSSI

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	2/42

Sommaire

<u>PARTIE 1. INTRODUCTION</u>	<u>4</u>
CHAPITRE 1. Généralités.....	5
<i>Article 1 : Objet de l'instruction</i>	<i>5</i>
<i>Article 2 : Champ d'application de l'instruction</i>	<i>5</i>
<i>Article 3 : Définitions</i>	<i>6</i>
CHAPITRE 2. Responsabilités et dispositions contractuelles.....	10
<i>Article 4 : L'organisation des responsabilités relatives à l'application de la réglementation.....</i>	<i>10</i>
<i>Article 5 : Passation des contrats.....</i>	<i>10</i>
CHAPITRE 3. Présentation de la démarche de sécurisation	11
<i>Article 6 : Démarche de sécurisation</i>	<i>11</i>
<u>PARTIE 2. MISE EN ŒUVRE DE LA DEMARCHE DE SECURISATION</u>	<u>12</u>
CHAPITRE 1. Le zonage du local	12
<i>Article 7 : Principe du zonage TEMPEST.....</i>	<i>12</i>
<i>Article 8 : Mise en œuvre du zonage TEMPEST</i>	<i>12</i>
CHAPITRE 2. Le choix du matériel.....	13
<i>Article 9 : Équipements certifiés au plan TEMPEST</i>	<i>13</i>
<i>Article 10 : Équipements commerciaux évalués au plan TEMPEST</i>	<i>14</i>
<i>Article 11 : Les équipements commerciaux conformes aux directives CEM</i>	<i>14</i>
<i>Article 12 : Les prototypes ou les équipements commerciaux modifiés.....</i>	<i>14</i>
<i>Article 13 : Contrôle des matériels.....</i>	<i>14</i>
CHAPITRE 3. Les règles d'installation	15
<i>Article 14 : Règles d'installation des sites</i>	<i>15</i>
<i>Article 15 : Dossier des installations</i>	<i>15</i>
<i>Article 16 : Audit et suivi du maintien en conditions de sécurité des installations.....</i>	<i>16</i>
CHAPITRE 4. Solution de remplacement à la démarche de sécurisation	17
<i>Article 17 : Évaluations système sur site.....</i>	<i>17</i>
<i>Article 18 : Moyens de durcissement électromagnétique.....</i>	<i>17</i>
<u>ANNEXE 1 Liste des textes de référence</u>	<u>18</u>
<u>ANNEXE 2 Recueil de notes techniques proposant les moyens de protection pour les sites et systèmes traitant des informations sensibles ne relevant pas du secret de la défense nationale</u>	<u>21</u>

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	3/42

PARTIE 1. INTRODUCTION

Tout matériel ou système, qui traite ou transmet des informations, sous forme électrique, produit des perturbations électromagnétiques. Ces perturbations, qualifiées de signaux parasites, sont provoquées par les variations du régime électrique établi dans les différents circuits qui composent le matériel considéré durant son fonctionnement. Certains de ces parasites peuvent être représentatifs des informations traitées. Leur interception et leur exploitation peuvent permettre de reconstituer les informations.

L'interception et l'exploitation des signaux compromettants, en vue de reconstituer les informations traitées, constitue la « menace TEMPEST¹ ».

Les signaux compromettants peuvent être captés à des distances pouvant atteindre quelques dizaines de mètres pour les parasites rayonnés et même plusieurs centaines de mètres pour les parasites conduits (cf. définitions *infra.*). En outre, des captures de signaux compromettants peuvent être réalisées sur de très longues distances en cas de couplage fortuit avec des émetteurs radioélectriques.

L'augmentation de l'utilisation des périphériques et de technologies de communication sans fil induit de nouvelles menaces qu'il convient de prendre en compte pour assurer la confidentialité, l'intégrité, l'authenticité et la disponibilité des informations traitées. Ainsi, de nombreux produits directement équipés d'émetteurs (radio, infrarouge...) sont disponibles dans le commerce. La puissance et les caractéristiques connues de ces signaux peuvent faciliter l'interception des informations transmises.

Par ailleurs, la menace liée à l'interception et à l'exploitation des signaux compromettants est toujours présente et ne doit pas être minimisée, malgré l'évolution des matériels. Sans surestimer la réalité de cette menace, il est en effet dangereux, pour la protection des informations traitées, de la minimiser ou de l'écarter.

La présente instruction décrit la démarche de sécurisation à appliquer afin de protéger les informations traitées contre la menace TEMPEST.

Le niveau de la menace ainsi que les conditions d'emploi doivent être identifiés au préalable afin d'appliquer une protection optimale.

¹ Le terme TEMPEST désigne l'ensemble du domaine des signaux parasites compromettants

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	4/42

CHAPITRE 1. Généralités

Article 1 : Objet de l'instruction

La présente instruction interministérielle fixe les règles applicables aux mesures de protection face aux risques provoqués par la menace TEMPEST et par l'utilisation des périphériques et technologies de communication sans fil.

La protection contre les signaux compromettants, qu'ils soient parasites ou intentionnels, est l'une des mesures concourant à la sécurité des systèmes d'information traitant des informations classifiées de défense, telle que définie par l'instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale [IGI 1300]. Cette protection s'inscrit dans un cadre plus global en intervenant de façon complémentaire avec d'autres mesures de sécurité.

Article 2 : Champ d'application de l'instruction

Les dispositions de la présente instruction s'appliquent aux systèmes d'information qui font l'objet d'une classification de défense au sens de l'instruction générale interministérielle [IGI 1300] et notamment du titre V concernant les mesures de sécurité relatives aux systèmes d'information.

Elles ont valeur de recommandation pour les systèmes d'information traitant des informations sensibles (en particulier de niveau Diffusion restreinte) non classifiées de défense. Ce cas particulier est traité en annexe 2.

La présente instruction est complétée par un ensemble de règles techniques qui décrivent de façon plus détaillée les différentes mesures de sécurité à mettre en œuvre pour les systèmes classifiés de défense, afin d'interdire la compromission de l'information par l'émission de signaux compromettants. Il s'agit notamment des directives n°485 relative aux règles d'installation des sites et systèmes d'information [DIR 485] et n°495 relative au zonage TEMPEST [DIR 495] qui sont publiées sous la mention Diffusion restreinte et ne sont donc pas publiques.

Les dispositions de la présente instruction sont applicables dans toutes les administrations centrales, tous les services déconcentrés de l'État et établissements publics nationaux placés sous l'autorité d'un ministre, dans toutes les entités, publiques ou privées, concernées par le secret de la défense nationale, ainsi qu'à toute personne physique ou morale dépositaire, même à titre provisoire, d'un tel secret, y compris dans le cadre de la passation et de l'exécution d'un contrat.

Pour les systèmes d'information traitant d'informations classifiées relevant des réglementations OTAN et UE, il convient également de respecter des règles complémentaires spécifiques, car l'application de la réglementation nationale est nécessaire mais non suffisante. Les références de tous les textes réglementaires applicables figurent en annexe 1.

Toute personne concernée par le domaine TEMPEST doit y être sensibilisée et formée. En effet, la protection contre la menace TEMPEST nécessitent une prise en compte globale et continue dans le cycle de vie des systèmes manipulant des informations classifiées., Les processus-métier de la conception, du développement, puis du déploiement et des installations sur site doivent donc traiter cette menace.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	5/42

Article 3 : Définitions

L'affaiblissement / atténuation est la diminution du niveau d'un signal, obtenue soit par la distance, soit par l'insertion d'un élément tel qu'un blindage ou un filtre. Cette diminution se mesure en décibel (dB).

L'autorité qualifiée en matière de sécurité des systèmes d'information (SSI) est l'autorité responsable de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, dans les établissements publics placés sous l'autorité d'un ministre ainsi que dans les organismes et établissements relevant de ses attributions.

L'autorité nationale TEMPEST est l'autorité qui fixe les règles applicables en matière de TEMPEST. Elle veille également au respect et à l'application de la réglementation dans le domaine TEMPEST.

Le couplage est l'interaction d'un circuit source de perturbations électromagnétiques sur un circuit sensible à ces perturbations. On parle de couplage par diaphonie, rayonnement et conduction.

Le circuit approuvé est le circuit qui a subi des mesures spécifiques de protection physique dont des mesures permettant une inspection visuelle et qui a été autorisé à l'emploi pour la transmission d'informations classifiées de défense sans protection par chiffrement.

Le couplage acoustique est la vulnérabilité consistant en la transmission par inadvertance de signaux acoustiques ROUGES à un microphone faisant partie d'un équipement NOIR.

La compatibilité électromagnétique (CEM) est l'aptitude d'un dispositif, d'un appareil ou d'un système à fonctionner dans son environnement électromagnétique de façon satisfaisante, sans produire lui-même des perturbations électromagnétiques de nature à créer des troubles graves dans le fonctionnement des appareils ou des systèmes situés dans cet environnement. La conformité aux normes de compatibilité électromagnétique est obligatoire dans l'Union européenne conformément à la directive européenne 2004/108/CE relative à la compatibilité électromagnétique.

Le conducteur fortuit est le conducteur qui peut fournir un chemin non intentionnel aux signaux parasites compromettants, par exemple les canalisations d'eau, les câbles ou les parties de structures métalliques, etc....

COMSEC est le terme désignant la sécurité des communications dans un cadre OTAN.

Le décibel (dB) est le logarithme décimal du rapport entre 2 valeurs. Pour un rapport de tensions par exemple, $x(\text{dB}) = 20 \log(V1/V2)$. Pour un rapport de puissances par exemple, $x(\text{dB}) = 10 \log(P1/P2)$.

L'équipement TEMPEST est l'équipement spécialement conçu pour réduire au maximum les émissions conduites et rayonnées. Il respecte généralement les limites du niveau « A » qui sont les plus contraignantes de la norme OTAN [SDIP 27].

L'équipement de niveau « A » est l'équipement ayant subi une évaluation TEMPEST réalisée par un laboratoire agréé par l'ANSSI et qui respecte les limites du niveau A de la norme OTAN [SDIP 27]. C'est l'équipement qui protège le mieux les informations traitées.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	6/42

L'équipement de niveau « B » est l'équipement ayant subi une évaluation TEMPEST réalisée par un laboratoire agréé par l'ANSSI et qui respecte les limites du niveau B de la norme OTAN [SDIP 27].

L'équipement de niveau « C » est l'équipement ayant subi une évaluation TEMPEST réalisée par un laboratoire agréé par l'ANSSI et qui respecte les limites du niveau C de la norme OTAN [SDIP 27].

L'équipement de catégorie « D » est l'équipement qui n'a fait l'objet d'aucune évaluation TEMPEST ou qui correspond à un équipement commercial Dir. CEM (cf. *infra*) ayant subi des modifications, même externes (câblage). C'est l'équipement qui protège le moins les informations traitées.

L'équipement zone 1 est l'équipement ayant subi un zonage TEMPEST en rayonnement électrique uniquement réalisé par un laboratoire agréé par l'ANSSI et qui respecte les limites du niveau B de la norme OTAN [SDIP 27].

L'équipement zone 2 est l'équipement ayant subi un zonage TEMPEST en rayonnement électrique uniquement réalisé par un laboratoire agréé par l'ANSSI et qui respecte les limites du niveau C de la norme OTAN [SDIP 27].

L'équipement commercial Dir. CEM est l'équipement conforme aux normes de compatibilités électromagnétiques et pour lequel aucune contre-mesure TEMPEST (par exemple faradisation, filtrage des signaux) n'a été intégrée intentionnellement. Depuis 1996, tout équipement électrique ou électronique doit être conforme aux normes de compatibilité électrique EN55022 (norme civile dédiée aux appareils de traitement de l'information). Cet équipement est également appelé COTS.

COTS (*Commercial-off-the-Shelf* - équipement commercial sur étagère) est, dans ce document, l'équipement supposé être conforme aux directives de CEM et ne comporter aucun durcissement au plan TEMPEST.

La cage de Faraday est une enceinte blindée, constituée de parois métalliques sur ses six faces. Le blindage se comporte comme un écran vis-à-vis des champs électromagnétiques, ce qui limite la propagation des ondes électromagnétiques.

Le filtre est un dispositif à utiliser sur les lignes d'alimentation ou de transmission des signaux, conçu spécifiquement pour laisser passer certaines fréquences et pour atténuer fortement toutes les autres fréquences.

La gaine est la canalisation, la goulotte, la conduite en métal, en plastique ou en fibre de verre, utilisée comme élément de protection physique des câbles qu'elle contient.

L'information chiffrée est l'information devenue secrète grâce à un moyen de chiffrement agréé par l'ANSSI.

L'information classifiée de défense est l'information présentant un caractère de secret de la défense nationale (art. 413-9 du code pénal).

Le laboratoire de niveau 1 est le laboratoire agréé par l'autorité nationale TEMPEST pour réaliser des évaluations TEMPEST conformément aux prescriptions de la norme OTAN [SDIP 27].

Le laboratoire de niveau 2 est le laboratoire agréé par l'autorité nationale TEMPEST pour réaliser des évaluations TEMPEST réduites ou encore le zonage TEMPEST d'équipements commerciaux.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	7/42

La masse est le potentiel électrique (0 volt) de référence pour les circuits électriques et électroniques.

Le matériel certifié au plan TEMPEST est le matériel ayant reçu de l'autorité nationale TEMPEST un certificat de conformité à l'un des niveaux de la norme [SDIP 27].

Les modes de propagation sont la manière dont les signaux parasites, qu'ils soient ou non compromettants, se propagent vers l'extérieur. Deux modes de propagation existent : par rayonnement dans l'espace environnant, par conduction sur les lignes connectées au matériel ou sur les conducteurs métalliques proches de ce dernier après avoir été induits par le rayonnement.

Les mesures sur site recouvrent l'ensemble des opérations qu'il convient d'effectuer suivant une méthode définie, pour vérifier le niveau de sécurité d'une installation et le maintien de ce niveau dans le temps, dans le cadre de la protection contre l'émission de signaux parasites compromettants.

La menace TEMPEST est la menace constituée par l'interception et l'exploitation des signaux compromettants, en vue de reconstituer les informations traitées. Il s'agit de la menace que font peser les signaux compromettants sur la confidentialité des informations.

Le matériel zoné au plan TEMPEST est le matériel ayant fait l'objet de mesures décrites dans la directive [DIR 495] et qui respecte les limites en rayonnement électrique de la norme [SDIP 27]. Suivant leur niveau de rayonnement ces matériels sont classés : équipement zone 1 ou équipement zone 2.

NOIR est le terme générique qui désigne les conducteurs électriques, fibres optiques, composants, équipements et systèmes qui véhiculent des signaux non classifiés de défense ou chiffrés par un équipement agréé et filtrés, et les zones dans lesquelles n'apparaissent pas de signaux classifiés de défense non chiffrés.

OTAN est l'organisation du traité de l'atlantique nord.

Le processeur NOIR est l'appareil ou le système d'information ne traitant pas de donnée classifiée non chiffrée.

Le processeur ROUGE est l'appareil ou le système d'information qui traite des données classifiées non chiffrées.

RF est l'acronyme de radiofréquence.

ROUGE est le terme générique qui désigne les conducteurs électriques, fibres optiques, composants, équipements et systèmes qui véhiculent des signaux classifiés de défense non chiffrés par un équipement agréé, et les zones dans lesquelles apparaissent des signaux classifiés de défense.

SDIP (*SECAN Doctrine and Information Publication*). Publication de doctrine et d'information du SECAN.

SECAN est le bureau de sécurité et d'évaluation des systèmes de communication et d'information du comité militaire de l'OTAN.

Le système d'information est l'ensemble organisé de ressources (matériels, logiciels, personnel, données, etc.) permettant de traiter, stocker, ou transmettre de l'information au travers d'un support électronique.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	8/42

Le suivi du maintien en conditions de sécurité recouvre l'ensemble des opérations qu'il convient d'effectuer pour vérifier, tout au long du cycle de vie des systèmes que le niveau de sécurité de l'installation est conforme à l'état initial, dans le cadre de la protection contre l'émission de signaux parasites compromettants.

Les signaux parasites sont les perturbations électromagnétiques temporaires provoquées par les variations d'état des différents circuits qui composent le matériel ou le système qui traite ou transmet sous forme électrique des informations durant son fonctionnement.

Les signaux parasites compromettants sont les signaux parasites (non intentionnels) représentatifs des informations traitées par un système d'information qui, une fois interceptés et exploités, permettent d'en reconstituer tout ou partie du contenu.

TEMPEST est le terme désignant l'ensemble du domaine des signaux parasites compromettants.

Le test TEMPEST est le test effectué en laboratoire ou sur site permettant de déterminer la nature et l'importance des signaux non intentionnels transmis par conduction ou par rayonnement, et contenant des informations compromettantes. Le test TEMPEST comprend généralement la détection et la mesure de ces signaux, ainsi que l'analyse de la corrélation entre les signaux ROUGES et les signaux parasites.

UE est l'acronyme de l'union européenne.

La zone 0 désigne la pièce ou le bureau ayant subi un zonage TEMPEST réalisé par une équipe de mesure agréée par l'ANSSI et qui respecte les critères de caractérisation de la zone 0 définis par la directive [DIR 495]. Parmi les trois zones possibles, la zone 0 est la zone protégeant le moins bien le système d'information qu'elle abrite.

La zone 1 ou zone 2 respecte les critères de caractérisation de la zone 1 ou de la zone 2 définis par la directive [DIR 495].

La zone de couplage est la zone qui ne doit pas comporter d'équipements ou de conducteurs superflus susceptibles de capter par couplage des signaux parasites compromettants provenant des équipements traitant des informations classifiées de défense. La zone de couplage doit être entièrement contenue dans la zone de sécurité.

La zone de sécurité, appelée aussi zone de sécurité TEMPEST (ZST) est la zone dans laquelle des dispositions permanentes sont prises pour détecter et empêcher toute écoute électronique, activité de recherche de renseignements et mise en place de matériel d'écoute. La zone de sécurité TEMPEST est définie par l'autorité qualifiée SSI du site. Cette zone est aussi appelée *controlled space* dans les contextes OTAN et européen. Le terme *inspectable space* détermine la limite définie par le périmètre séparant le site de la zone extérieure.

Le zonage TEMPEST des équipements est une évaluation TEMPEST réalisée uniquement en rayonnement électrique sur des équipements commerciaux permettant de les classer en équipement zone 1 ou équipement zone 2. Pour les systèmes traitant des informations classifiées de défense, il convient de se référer à la directive [DIR 495].

Le zonage TEMPEST des locaux est un ensemble de mesures consistant à réaliser des tests en rayonnement électrique permettant de quantifier l'atténuation électromagnétique présentée par la structure physique des bâtiments. Les locaux sont ensuite classés en zone 0, zone 1 ou zone 2. Pour les systèmes traitant des informations classifiées de défense, il convient de se référer à la directive [DIR 495]. Pour les systèmes traitant des informations sensibles, il convient de se référer aux annexes.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	9/42

CHAPITRE 2. Responsabilités et dispositions contractuelles

Article 4 : L'organisation des responsabilités relatives à l'application de la réglementation

Cette instruction s'applique à tout système d'information ayant vocation à traiter des informations classifiées placées sous la responsabilité d'un ministère.

L'ANSSI est l'autorité nationale TEMPEST.

L'organisation des responsabilités relative aux systèmes d'information est détaillée au titre V de l'instruction générale interministérielle [IGI 1300], qui définit les mesures de sécurité relatives aux systèmes d'information.

Chaque ministère doit, par ailleurs, veiller à ce que les établissements ou organismes dépendant de lui et soumis au régime de la tutelle appliquent la présente instruction.

Les ministères qui ne disposent pas de moyen ou d'infrastructure nécessaire pour assurer la vérification des performances TEMPEST de leurs matériels peuvent faire appel au concours de l'autorité nationale TEMPEST.

Article 5 : Passation des contrats

Les dispositions de la présente instruction doivent faire l'objet de clauses particulières dans les marchés et contrats soumis aux dispositions de l'instruction générale interministérielle n°1300 [IGI 1300] qui entraînent la mise en œuvre de systèmes d'information faisant l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	10/42

CHAPITRE 3. Présentation de la démarche de sécurisation

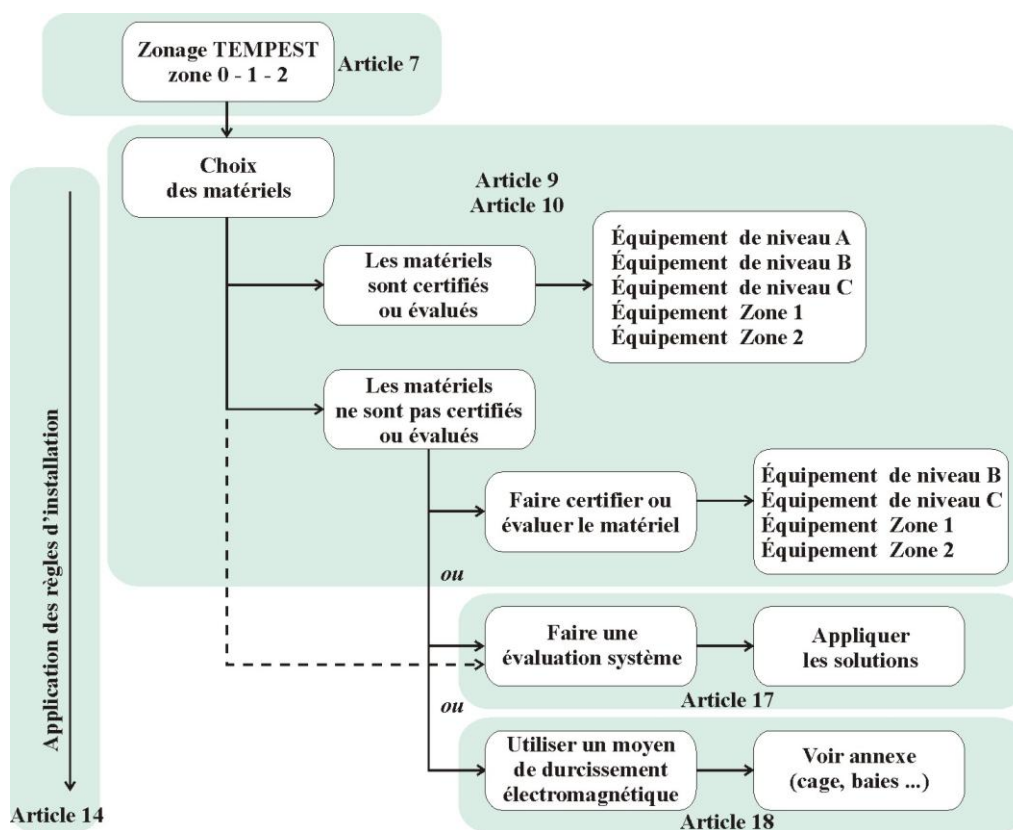
Article 6 : Démarche de sécurisation

Elle a pour but de proposer un mode opératoire visant la protection TEMPEST d'un système. Elle se déroule en quatre étapes successives :

- le niveau de sensibilité et de classification des informations traitées (*Diffusion Restreinte*, CONFIDENTIEL DEFENSE ou SECRET DEFENSE) doit être déterminé ;
- le local prévu pour l'installation du système doit faire l'objet d'un zonage TEMPEST prenant en compte l'affaiblissement électromagnétique naturel du bâtiment ;
- le matériel doit être choisi en fonction de la sensibilité des informations traitées et du zonage TEMPEST. Des équipements spécifiquement conçus (matériels TEMPEST) permettent de bénéficier d'une protection maximale ;
- en fonction du matériel retenu, des règles d'installation spécifiques doivent être appliquées car les normes techniques imposées aux matériels ou systèmes de traitement de l'information ne suffisent pas, à elles seules, à se protéger contre la menace TEMPEST.

Cette démarche sera dénommée « niveau de l'information/zonage/équipements/règles d'installation » dans la suite du document. Si elle ne peut pas être appliquée, une démarche d'évaluation TEMPEST ou la mise en place d'une enceinte blindée, peuvent constituer une solution de remplacement pour atteindre le degré de protection nécessaire au traitement des données.

La figure ci-dessous présente les solutions techniques assurant la confidentialité des informations classifiées, à l'encontre de la menace TEMPEST.



Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	11/42

PARTIE 2. MISE EN ŒUVRE DE LA DEMARCHE DE SECURISATION

CHAPITRE 1. Le zonage du local

Article 7 : Principe du zonage TEMPEST

Le principe du zonage TEMPEST est de délimiter, à l'intérieur d'un bâtiment, des zones qui sont caractérisées par leur aptitude, plus ou moins grande, à atténuer la propagation des signaux parasites susceptibles d'être émis par les matériels durant leur utilisation.

Le zonage des locaux ne prend en compte que les signaux parasites compromettants émis en rayonnement.

Les signaux parasites compromettants liés aux phénomènes de conduction doivent être traités conformément à la directive [DIR 485].

Article 8 : Mise en œuvre du zonage TEMPEST

Le déploiement d'équipements sur un site doit nécessiter une cartographie des bâtiments définissant l'atténuation naturelle mesurée dans chaque local. Ce zonage TEMPEST doit mettre en œuvre une méthode de mesures et une synthèse des résultats définies par la directive [DIR 495].

Dans certains ministères, des équipes de mesures réalisent des zonages. Ces équipes sont agréées par l'autorité nationale TEMPEST qui reconnaît ainsi leur capacité à effectuer ces travaux.

Lorsqu'une mesure de zonage n'est pas pertinente ou ne peut être mise en œuvre du fait de la proximité d'éléments extérieurs non contrôlés, le recours à une cage de Faraday est nécessaire. Ces cages doivent faire l'objet de mesures initiales à la recette puis de mesures périodiques tout au long de leur exploitation. Ces mesures d'atténuation de blindage électromagnétique sont décrites dans la norme civile [IEEE Std 299] et peuvent être réalisées en interne par des équipes compétentes ou externalisées auprès d'entreprises privées.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	12/42

CHAPITRE 2. Le choix du matériel

La protection contre la menace TEMPEST passe également par le choix d'équipements dont les performances TEMPEST sont adaptées à la menace et aux risques.

Il existe quatre niveaux de protection allant des équipements certifiés, qui sont durcis pour limiter au maximum l'émission de signaux parasites compromettants, aux équipements commerciaux évalués ou non et aux prototypes et équipements commerciaux modifiés qui n'offrent aucune protection particulière vis-à-vis de la menace traitée ici.

Article 9 : Équipements certifiés au plan TEMPEST

Les équipements certifiés au plan TEMPEST sont conçus et durcis spécifiquement pour contrer la menace TEMPEST. Des précautions particulières ont été prises dès leur conception pour protéger au mieux les signaux sensibles et réduire les émissions conduites et rayonnées de signaux parasites compromettants.

Ces équipements sont généralement conformes au niveau A de la norme OTAN [SDIP 27]. Ce sont les équipements qui protègent le mieux les informations traitées.

À la suite de leur certification, ils sont classés dans le [REP490]. Ce répertoire est mis à jour et édité par l'autorité nationale TEMPEST.

Contrôle continu des équipements certifiés

Les matériels certifiés au plan TEMPEST doivent faire l'objet de contrôles périodiques tout au long de leur cycle de vie. Ces contrôles sont destinés à vérifier le maintien des caractéristiques techniques liées à la protection contre les signaux parasites compromettants.

Ces contrôles sont exercés suivant un plan de tests réduit, élaboré par le laboratoire agréé de niveau 1 qui a évalué le matériel avant sa mise en service opérationnel.

Ainsi, tout matériel certifié est soumis à des contrôles :

- à l'issue de sa fabrication, au titre des opérations de recette, pour pouvoir prononcer l'admission du matériel ;
- à l'issue de toute intervention sur le matériel, afin de vérifier la « non altération » des caractéristiques TEMPEST ;
- au cours de sa durée de vie, afin de mesurer l'éventuelle dégradation des caractéristiques dans le temps.

Suivi ACSSI des équipements certifiés

Les matériels certifiés pour répondre aux exigences des normes TEMPEST et ne disposant pas de moyens de protection de leur intégrité doivent être identifiés comme des articles contrôlés de la sécurité des systèmes d'information (ACSSI). En effet, ce marquage vise à protéger l'intégrité des matériels par un marquage et un suivi spécifique. Les prescriptions de l'instruction interministérielle [II 910] sur les articles contrôlés de la sécurité des systèmes d'information doivent être appliquées.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	13/42

Article 10 : Équipements commerciaux évalués au plan TEMPEST

Les équipements commerciaux conformes aux directives CEM peuvent être évalués au plan TEMPEST. L'évaluation est réalisée soit par des tests avec recherche de compromission, soit par un zonage de l'équipement. Les équipements évalués seront classés soit niveau B ou niveau C, soit équipement zone 1 ou équipement zone 2.

À la suite de leur évaluation, les équipements sont classés dans le [REP490]. Ce répertoire est mis à jour et édité par l'autorité nationale TEMPEST.

Article 11 : Les équipements commerciaux conformes aux directives CEM

Les équipements commerciaux conformes aux directives CEM sont des équipements pour lesquels aucune contre-mesure TEMPEST n'a été intégrée intentionnellement (cf définitions *infra*). Cependant, leur conformité aux normes CEM permet de les utiliser sous certaines conditions pour traiter des informations classifiées. La [DIR485] précise les règles applicables à l'installation de ce type d'équipement.

Article 12 : Les prototypes ou les équipements commerciaux modifiés

Ces équipements sont classés dans la catégorie D. Il s'agit de tous les équipements prototypes, ou équipements commerciaux ayant été modifiés matériellement ou fonctionnant sans boîtier ou avec un boîtier ouvert.

Ce sont les équipements qui protègent le moins les informations traitées. Il conviendra donc de mettre en place des protections complémentaires de type baie faradisée ou cage de Faraday.

Article 13 : Contrôle des matériels

Que l'équipement soit certifié ou simplement évalué, l'élaboration des mesures est conduite par des laboratoires agréés par l'autorité nationale TEMPEST qui reconnaît ainsi leurs capacités à effectuer ces évaluations :

- les laboratoires de niveau 1 sont aptes à réaliser des évaluations TEMPEST, appelées évaluations initiales ;
- les laboratoires de niveau 2 sont aptes à réaliser des évaluations TEMPEST réduites, basées sur les évaluations initiales. Ces laboratoires sont dédiés aux vérifications systématiques réalisées avant la mise en production des équipements ou encore lors de leur retour de maintenance.

La liste des laboratoires agréés figure dans le répertoire [REP490].

Un matériel TEMPEST ne peut recevoir de certification nationale ou être évalué au plan TEMPEST que dans le cas où un ministère, ou un opérateur d'importance vitale, souhaite s'en équiper et en fait la demande auprès de l'autorité nationale TEMPEST. Cette certification ou évaluation ne peut être prononcée qu'à l'issue de tests effectués par un laboratoire agréé de niveau 1. Le plan et le rapport de tests ainsi que le plan de test réduit rédigés à l'occasion de l'évaluation du matériel sont fournis par le laboratoire à l'autorité nationale TEMPEST, qui procède, au vu de ces documents, à la certification du matériel. Cette procédure de certification est assortie de l'exigence, pour le constructeur, de disposer d'une structure industrielle capable de garantir les opérations de maintenance sur le territoire national.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	14/42

CHAPITRE 3. Les règles d'installation

Article 14 : Règles d'installation des sites

Les règles d'installation des sites sont fixées dans la directive [DIR 485] relative à l'installation des sites et systèmes d'information.

En outre, des précautions particulières doivent être prises au cas par cas pour les installations multicontextes, notamment dans le cas de la cohabitation de systèmes souverains et OTAN. Il convient alors de se concerter avec l'autorité nationale TEMPEST.

La présence de technologies de communication sans fil doit nécessiter une attention particulière, notamment pour ce qui concerne les règles d'installation s'appliquant aux systèmes de transmission.

Les règles d'installation sont plus ou moins exigeantes selon que les équipements utilisés sont protégés ou non contre l'émission de signaux compromettants. Ainsi, un matériel certifié au plan TEMPEST nécessite des règles d'installation minimales, tandis qu'un matériel non certifié exige des conditions d'installation sensiblement plus contraignantes.

Ces règles sont destinées à :

- supprimer toute possibilité de fuite par conduction des signaux compromettants à l'aide de moyens adaptés (filtres, rupture de continuité électrique, par exemple) ;
- instaurer des zones de protection en trois dimensions, appelées zones de couplage, autour des moyens de traitement. Les zones de couplage sont caractérisées par des volumes englobant chaque équipement traitant des informations sensibles.

Dans le cas d'une installation dans un immeuble maîtrisé, affecté à une seule entité, dont la zone de sécurité est également contrôlée, les règles d'installation peuvent être simplifiées de manière méthodique. L'attention se portera dans ce cas sur le traitement des lignes d'entrées et sorties du bâtiment.

Article 15 : Dossier des installations

Le dossier des installations est constitué de trois parties :

- la description du site permet d'identifier la position des installations ainsi que les moyens mis en œuvre pour le traitement d'informations classifiées sur le site. Il doit aussi identifier les réseaux de communication sans fil déployés sur le site ;
- le dossier des mesures collecte tous les comptes rendus des relevés effectués sur le site (zonage, affaiblissement des cages de Faraday, résultats de tests sur les équipements, etc.) ;
- le dossier de synthèse mentionne les non-conformités à la réglementation, les anomalies ou contraintes spécifiques à certains systèmes. Il propose un plan d'amélioration continue de la protection contre les signaux parasites compromettants.

Ce dossier doit être tenu à jour par l'autorité qualifiée en SSI du site ou du système auquel il fait référence. Il doit être mis à jour chaque fois qu'une modification significative est apportée à l'installation. Il doit faire partie du dossier d'homologation.

Une fiche dédiée de la directive [DIR 485] spécifie le contenu de chaque partie du dossier.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	15/42

Article 16 : Audit et suivi du maintien en conditions de sécurité des installations

Le suivi du maintien en conditions de sécurité doit porter sur la vérification des règles d'installation, sur le zonage TEMPEST des locaux et sur le contrôle des cages de Faraday. Il doit être effectué pendant toute la durée de vie de l'installation et comprend :

- un audit initial destiné à l'homologation de l'installation ;
- des audits occasionnels destinés à vérifier que la protection reste assurée à chaque fois qu'une modification significative est apportée à l'installation.

Les équipes spécialisées procèdent aux mesures sur site suivant les méthodes décrites dans les directives [DIR 485] et [DIR 495].

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	16/42

CHAPITRE 4. Solution de remplacement à la démarche de sécurisation

Article 17 : Évaluations système sur site

Lorsque les directives d'installation ne peuvent être respectées parce que la démarche classique « niveau de l'information/zonage/équipement/règles d'installation » n'est pas applicable, une démarche d'évaluation TEMPEST du système complet doit être mise en œuvre. Cette démarche s'applique aussi bien aux installations en infrastructure qu'aux systèmes installés sur des plates-formes mobiles (avion, bateau, véhicule terrestre). Elle doit englober l'analyse des sources et des chemins de fuite des signaux parasites compromettants et la réalisation de mesures. Ces mesures doivent mettre en œuvre, en limite de zone de sécurité, le même procédé d'évaluation TEMPEST que celui réalisé en cage de Faraday.

Tout changement dans un système ou dans son installation doit faire l'objet d'un complément d'analyse et éventuellement de mesures. Les mesures doivent être réalisées par les laboratoires agréés à ce titre par l'autorité nationale TEMPEST.

Article 18 : Moyens de durcissement électromagnétique

Lorsque, pour une installation donnée, le site d'implantation choisi pour un équipement non évalué TEMPEST ne permet pas d'assurer la protection contre les signaux compromettants, une protection électromagnétique (cage de Faraday, faradisation légère ou baie CEM) autour de l'équipement ou du système doit être mise en place.

Le blindage se comporte comme un écran électromagnétique qui atténue, par réflexion et par absorption, la propagation des signaux parasites émis par rayonnement. Les signaux émis par conduction doivent par ailleurs être traités par l'emploi de filtres ou de dispositifs de conversion optiques.

Il est nécessaire d'entretenir correctement les points faibles des moyens faradisés, notamment les ouvertures tels que les portes, les nids d'abeille et les plaques collectrices, afin de ne pas dégrader les caractéristiques globales d'affaiblissement. Il convient de s'assurer de la pérennité des performances par des contrôles périodiques dépendant du taux d'utilisation du moyen.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	17/42

ANNEXE 1
Liste des textes de référence

Réglementation nationale :	
[IGI 1300]	Instruction générale interministérielle sur la protection du secret de la défense nationale n° 1300/SGDSN/PSE/PSD publiée par l'arrêté du Premier ministre du 30 novembre 2011.
[II 910]	Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information (ACSSI) n° 910/SGDSN/ANSSI du 22 octobre 2013.
[II 920]	Instruction interministérielle relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel défense n° 920/SGDN/DCSSI du 12 janvier 2005.
[REP 490]	Répertoire des matériels évalués au plan de la protection contre l'émission de signaux parasites compromettants n° 490/ANSSI/DR du 13 mars 2014.
[DIR 485]	Directive d'installation des sites et systèmes d'information pour la protection contre les signaux parasites compromettants n° 485/ANSSI/DR du 20 novembre 2013.
[DIR 495]	Directive de zonage TEMPEST n° 495/ANSSI/DR du 20 novembre 2013.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	18/42

Réglementation OTAN :	
[AC/322-D0036]	<i>Infosec technical ant implementation directive on emission security – 23th of August 2007 (NATO RESTRICTED).</i>
[SDIP 27]	<i>SECAN doctrine and information publication, NATO TEMPEST requirements and evaluation procedures – Version 1, December 2009 (NATO CONFIDENTIAL).</i>
[SDIP 28]	<i>SECAN doctrine and information publication, NATO Zoning procedures – Version 1, December 2009 (NATO RESTRICTED).</i>
[SDIP 29]	<i>SECAN doctrine and information, Facility design criteria and installation of equipment for the processing of classified information – Version 1 – January 2011 (NATO RESTRICTED).</i>
[SDIP 55]	<i>TEMPEST product qualification and control – August 2009 (NATO RESTRICTED).</i>
http://www.ia.nato.int/niapc/tempest/emsec	

Réglementation UE :	
[IASP 7]	<i>Information assurance security policy on TEMPEST (EU RESTRICTED).</i>
[IASG 7-01]	<i>Information assurance security guidelines on selection and installation of TEMPEST equipment (EU RESTRICTED).</i>
[IASG 7-02]	<i>Information assurance security guidelines on TEMPEST zoning procedures (EU RESTRICTED).</i>
[IASG 7-03]	<i>Information assurance security guidelines on EU TEMPEST requirements and evaluation procedures (EU CONFIDENTIAL).</i>
[IASG 7-04]	<i>Information assurance security guidelines on accreditation of EU TEMPEST companies (LIMITE).</i>
http://www.consilium.europa.eu/policies/information-assurance/	

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	19/42

Autre :	
[IEEE Std 299]	<i>IEEE Standard method for measuring the effectiveness of electromagnetic shielding enclosures.</i>

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	20/42

ANNEXE 2

Recueil de notes techniques proposant les moyens de protection pour les sites et systèmes traitant des informations sensibles ne relevant pas du secret de la défense nationale

Cette annexe ne concerne pas les systèmes traitant des informations classifiées de défense pour lesquels il est nécessaire d'appliquer les directives [DIR 485] et [DIR 495].

Avant-propos

Cette annexe présente un recueil de notes techniques relatives à la mise en œuvre pratique de la protection contre la menace TEMPEST.

Ces éléments sont applicables à l'installation des matériels ou des systèmes de traitement des informations sensibles ne relevant pas du secret de la défense nationale. Ces informations sensibles, extérieures à tout niveau de classification, peuvent toutefois mériter une attention ainsi qu'une protection particulière notamment par un marquage spécifique.

La sécurisation TEMPEST peut s'appuyer sur les notes techniques présentées ci-après :

- en premier lieu, le concept du zonage TEMPEST est abordé afin de rechercher une mise en œuvre optimale de la protection en termes de coûts et d'efficacité et en fonction du résultat du zonage des locaux ;
- en second lieu, un choix des équipements adaptés en fonction du risque est requis. Des répertoires sont disponibles afin d'identifier les équipements évalués. Soit les équipements ont été durcis pour produire un minimum de signaux parasites : équipements TEMPEST également appelés équipements de niveau « A », soit leurs rayonnements ont été quantifiés lors d'une évaluation afin de leur attribuer le niveau « B », « C », « EZ1 » ou « EZ2 » ;
- en complément du choix des locaux et des équipements, il convient de suivre les règles d'installations adaptées à la configuration retenue. Les règles présentées ci-après abordent ainsi la mise en œuvre de filtres ou de dispositifs optiques.

Si les méthodes traditionnelles ne peuvent être utilisées, il est possible d'avoir recours à d'autres solutions de durcissement, en particulier une cage de Faraday.

Enfin, dans le but de conserver un niveau de protection optimal contre la menace TEMPEST, le dossier relatif aux installations permet d'établir l'état initial du système et d'en tracer ensuite les évolutions, afin de s'assurer de la pérennité des protections mises en œuvre.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	21/42

Sommaire

NOTE TECHNIQUE 1 : Le zonage TEMPEST d'un bâtiment	24
L'objectif	24
La mesure de l'affaiblissement des locaux	25
L'interprétation des résultats	25
Exemple de zonage d'une installation type	26
Figure 1 : Bâtiment type	27
Figure 2 : Emplacement des points de mesure	28
Figure 3 : Caractérisation des zones	29
NOTE TECHNIQUE 2 : Le durcissement des équipements	30
L'objectif	30
Le développement des cartes électroniques	30
Le câblage des interfaces internes	30
Le boîtier	31
Les câbles blindés	31
NOTE TECHNIQUE 3 : Les règles d'installation	32
L'objectif	32
La zone de sécurité	32
La zone de couplage.....	33
NOTE TECHNIQUE 4 : Les filtres	34
Les filtres d'alimentation	34
Les filtres analogiques basses fréquences	35
Installation et précautions de mise en œuvre des filtres	35
Figure 1 : Exemple de mise en œuvre d'une armoire de filtrage	35
NOTE TECHNIQUE 5 : Les fibres optiques	36
Caractéristiques des fibres optiques	36
Applications.....	36
NOTE TECHNIQUE 6 : La mise à la terre	37
La constitution du circuit de terre	37
Recommandations	37

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	22/42

<u>NOTE TECHNIQUE 7 : Autres solutions de durcissement</u>	38
La baie faradisée.....	39
La cage de Faraday modulaire.....	39
La cage de Faraday type feuillard de cuivre.....	39
La tente faradisée	40
Les revêtements muraux.....	40
<u>NOTE TECHNIQUE 8 : Dossier relatif aux installations</u>	41
La partie description	41
La partie mesures	41
La partie synthèse.....	42

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	23/42

NOTE TECHNIQUE 1 :

Le zonage TEMPEST d'un bâtiment

L'objectif

Le zonage d'un bâtiment consiste à mesurer l'atténuation présentée par ses murs et parois internes face à la propagation des ondes électromagnétiques. Au vu des résultats des mesures effectuées, l'intérieur des locaux est segmenté suivant différentes zones, caractérisées par leur aptitude, plus ou moins grande, à atténuer la propagation des signaux parasites émis par les équipements durant leur fonctionnement.

Le zonage vise à optimiser la protection contre la compromission électromagnétique en installant les équipements traitant des informations sensibles dans les zones les mieux adaptées.

Le zonage ne prend en compte que la propagation des signaux en rayonnement électrique. La propagation des signaux en conduction doit être traitée par l'application de règles d'installation spécifiques.

L'élément initial et essentiel d'une campagne de mesure de zonage TEMPEST est la définition de la limite de zone de sécurité TEMPEST (ZST) ou électromagnétique. Le zonage en lui-même et l'intégralité des résultats dépendent de la définition de cette zone. La limite de la zone de sécurité est déterminée par l'autorité SSI qualifiée du site et représente une zone dans laquelle des dispositions permanentes sont prises pour détecter et empêcher toute écoute électronique ou activité de recherche de renseignements. Des précautions particulières doivent également être prises pour contrôler les mouvements des personnels et des véhicules.

L'emplacement et le nombre de points de mesure dans le bâtiment à zoner doivent être choisis en limite de zone de sécurité et en fonction des différences de structure du bâtiment. Pour accroître le crédit que l'on accorde à cette méthode, il est souhaitable d'effectuer des mesures à partir d'un grand nombre de points. Le choix des points de mesure requiert l'application de quelques principes de base de l'électromagnétisme associés au bon sens, et doit tenir compte du type et de l'épaisseur des matériaux utilisés dans la construction du bâtiment ainsi que de la position des ouvertures.

Les mesures sont effectuées selon la méthode de la double pesée sur une gamme de fréquences allant de 10 MHz à 1 GHz par exemple. L'atténuation résultante est déterminée point de fréquence par point de fréquence entre un relevé de référence, effectué à 20m en espace libre, et le niveau relevé au travers de la structure du bâtiment. Cette comparaison permet d'obtenir l'atténuation apportée par la structure du bâtiment et d'attribuer une zone aux locaux mesurés.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	24/42

La mesure de l'affaiblissement des locaux

Pour effectuer cette mesure, il est nécessaire de disposer d'un ensemble d'émission et de réception composé d'un générateur de signaux et d'un analyseur de spectre.

En fonction du matériel de mesure disponible, la plage de fréquences 10 MHz à 1 GHz peut être découpée en plusieurs bandes de fréquences juxtaposées.

Le niveau de référence (REF) commun à toutes les mesures est déterminé en espace libre, en plaçant les antennes émission et réception à 1 m du sol et à 20 m l'une de l'autre.

Le signal émis est ajusté à un niveau suffisant pour permettre la mesure.

L'antenne d'émission est placée à l'intérieur du bâtiment aux différents points prédéterminés. L'antenne de réception est placée en limite de ZST du site en regard de l'émission. La configuration de l'instrumentation, ainsi que les niveaux d'émission décidés lors de la mesure de référence, doivent rester identiques durant tout le déroulement des mesures.

L'interprétation des résultats

L'interprétation des résultats consiste à comparer, point de fréquence par point de fréquence, les niveaux de référence correspondant à la propagation en espace libre, et les niveaux mesurés correspondant à l'affaiblissement apporté par le bâtiment. Cette comparaison permet d'obtenir l'atténuation apportée par la structure du bâtiment et attribue une zone aux locaux mesurés.

Au vu de l'interprétation des résultats des mesures, une zone est affectée à chaque pièce du bâtiment. La lettre X, Y ou Z attribuée à une zone est fonction du nombre de points de fréquence respectant au moins à 90 % le critère de la zone considérée.

Détermination de l'attribution d'une lettre à la zone considérée en fonction des critères ci-dessous :

Zone X :	ATM (dB) < 0 dB
Zone Y :	0 dB ≤ ATM (dB) < + 20 dB
Zone Z :	+ 20 dB ≤ ATM (dB)

Formule de l'atténuation réelle mesurée : $ATM (dB) = V_{ref} (dBV) - V_{att} (dBV)$

V_{ref} = niveau du signal de référence ;

V_{att} = niveau du signal mesuré dans le bâtiment ;

dB = unité du décibel.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	25/42

Exemple de zonage d'une installation type

L'installation type, représentée par la figure 1, correspond à un bâtiment qui comprend un centre informatique, un centre de transmission, divers locaux techniques et des bureaux.

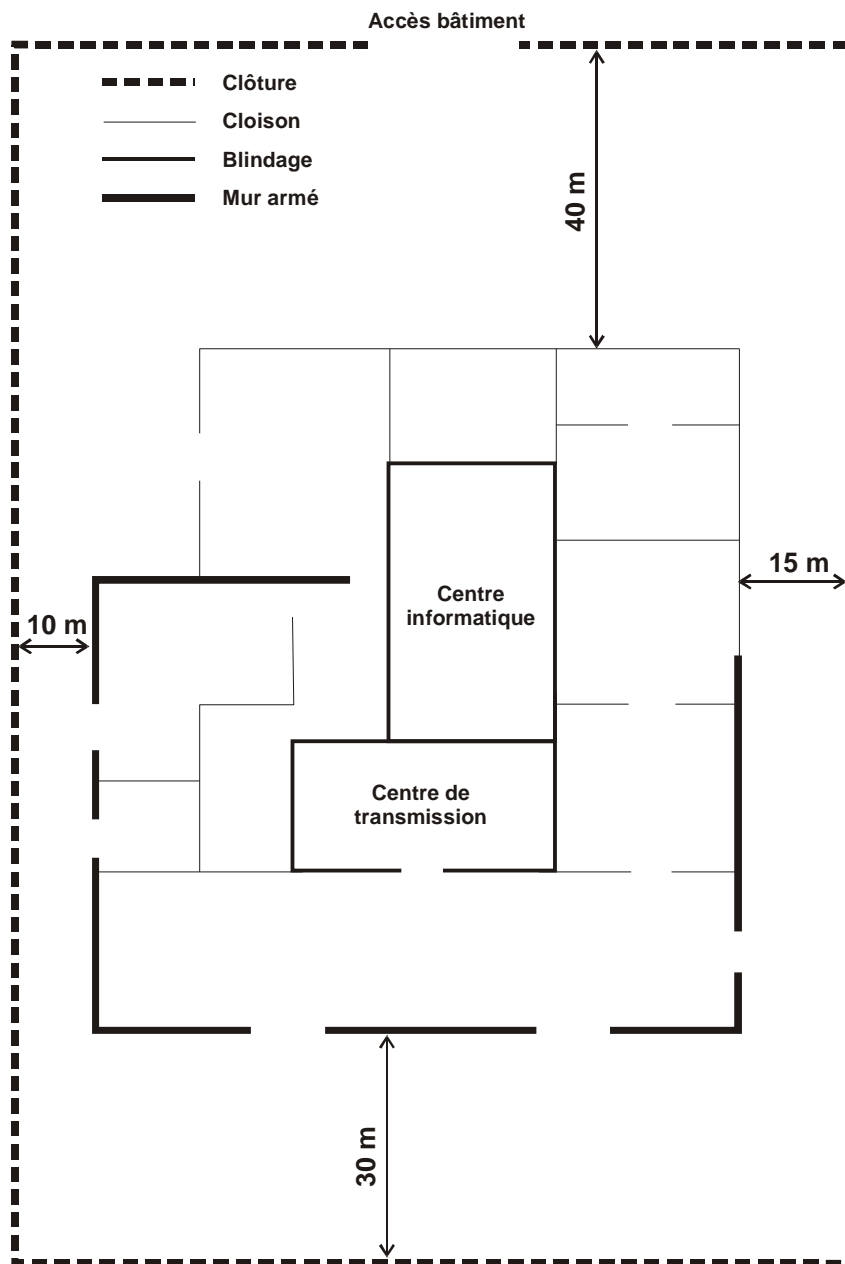
Les cloisons et les murs du bâtiment sont constitués de différents matériaux présentant des affaiblissements plus ou moins importants suivant leur résistance à la propagation des signaux. Le bâtiment est à l'intérieur d'une zone de sécurité, délimitée par une clôture.

La figure 2 précise l'emplacement des équipements de mesure ou points de zonage à l'extérieur, en limite de la zone de sécurité, et à l'intérieur du bâtiment. Le choix des emplacements à l'intérieur du bâtiment est effectué en fonction de la position des ouvertures des portes et des fenêtres et de la nature des matériaux intervenant dans la construction des murs, des parois et des cloisons. Un point extérieur peut être associé à plusieurs points intérieurs. L'inverse est également possible.

La figure 3 caractérise les différentes zones TEMPEST du bâtiment d'après les mesures effectuées. Ce schéma est donné à titre d'exemple.

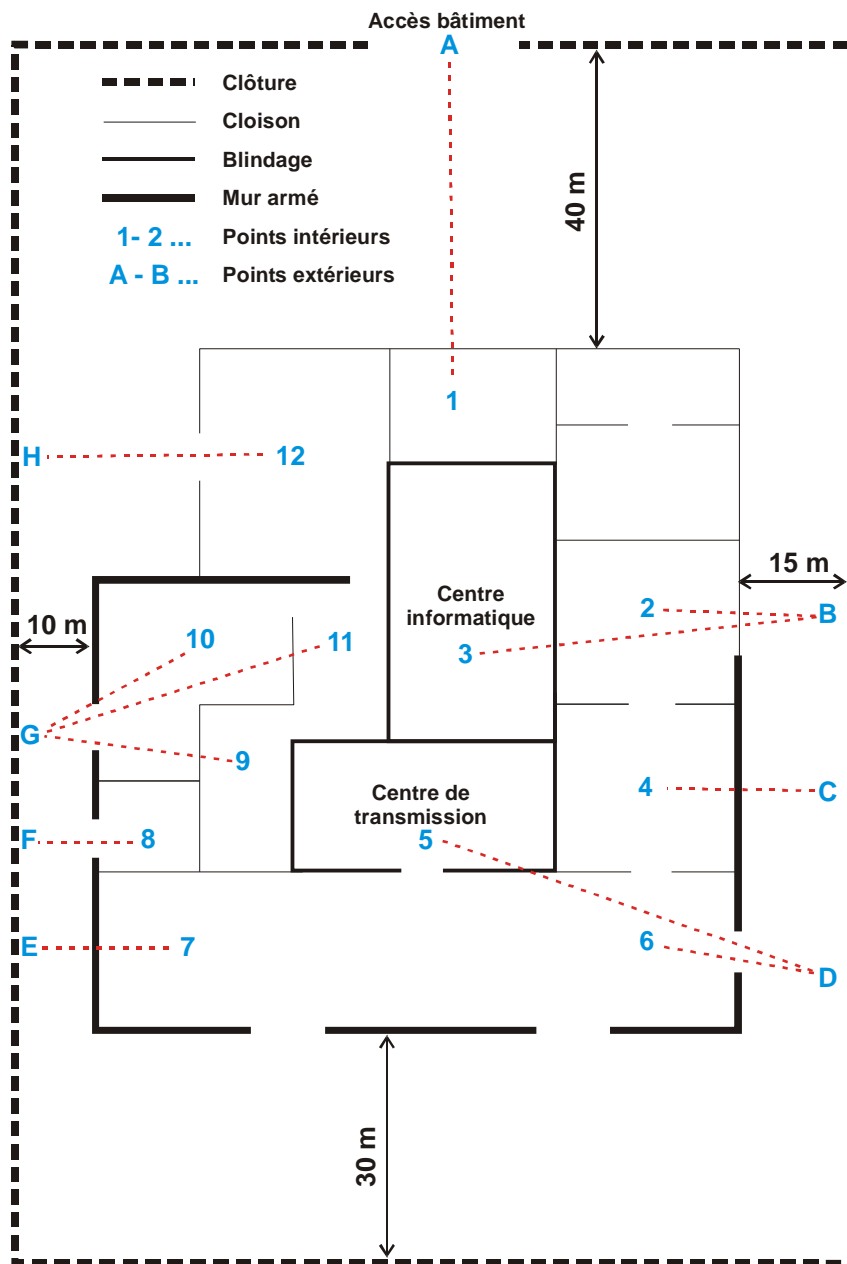
Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	26/42

Figure 1 : Bâtiment type



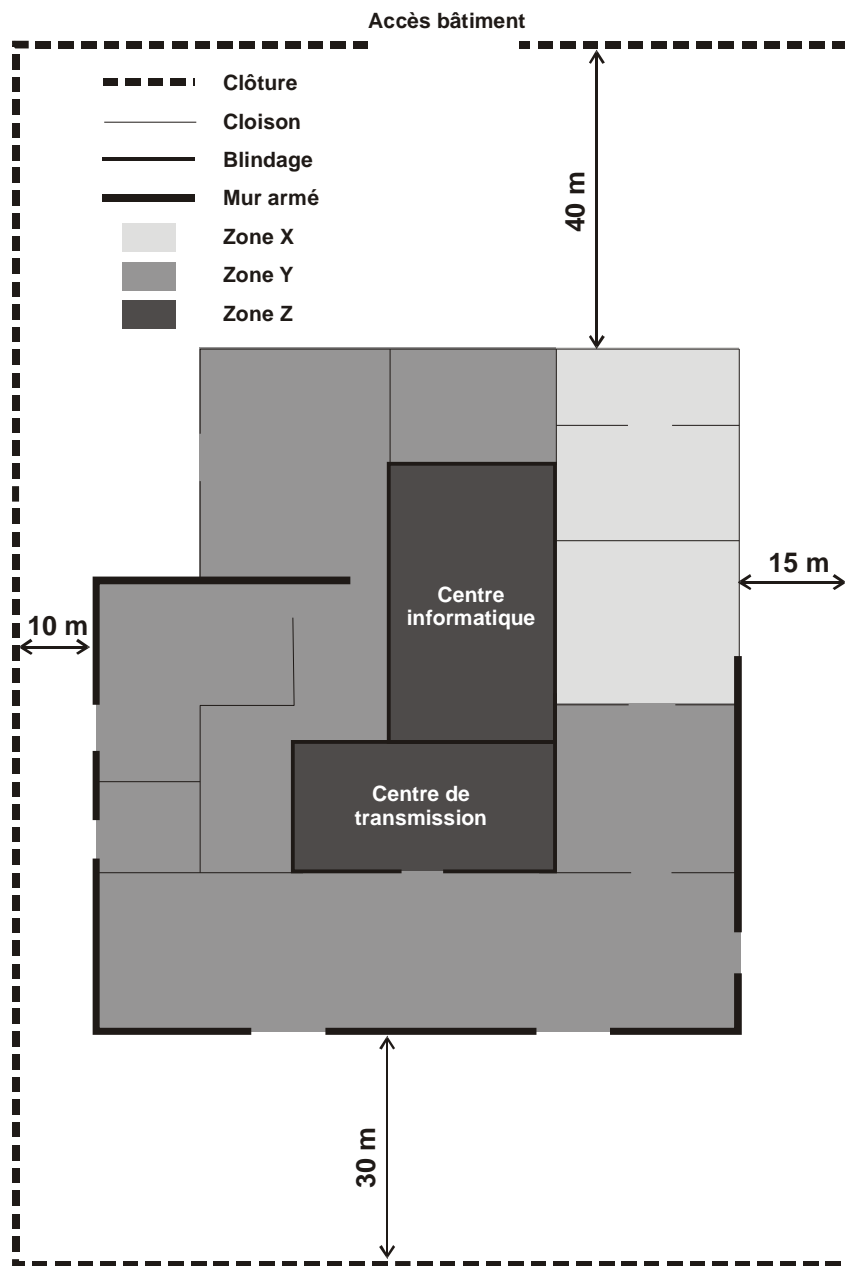
Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	27/42

Figure 2 : Emplacement des points de mesure



Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	28/42

Figure 3 : Caractérisation des zones



Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	29/42

NOTE TECHNIQUE 2 :

Le durcissement des équipements

L'objectif

L'objectif du durcissement est d'éviter que des signaux corrélés à l'information sensible traitée au sein de l'équipement puissent se propager vers l'extérieur et être interceptés.

Le concept ROUGE/NOIR, appliqué à un équipement ou à un système, permet de dissocier les parties où les informations sensibles sont traitées et véhiculées en clair (ROUGE), de celles où l'information ne nécessite pas d'être protégée (NOIR). L'information ROUGE devient NOIRE dès lors qu'elle est chiffrée, par un moyen de chiffrement adapté à son niveau de sensibilité.

Les termes ROUGE et NOIR sont utilisés pour identifier et distinguer les circuits, composants, équipements et systèmes. Ils servent aussi à distinguer les zones physiques qui les contiennent.

Le développement des cartes électroniques

La conception des cartes imprimées doit prendre en compte la séparation des composants ROUGES et des composants NOIRS. Les règles de conception CEM doivent être respectées, par exemple celles qui concernent les méthodes de routage évitant le couplage entre les pistes du circuit imprimé. Il faut confiner les signaux ROUGES entre deux plans d'alimentation par exemple, et prévoir les découplages des circuits actifs au plus près des broches d'alimentation en réduisant la surface des boucles.

Le câblage des interfaces internes

Le câblage des interfaces doit comporter des liaisons courtes et blindées pour la distribution des signaux et des alimentations ROUGES. Les liaisons transmettant les signaux ROUGES doivent être séparées des liaisons de signaux NOIRS. Une zone ROUGE confinée doit être créée pour limiter les risques de mélange entre signaux ROUGES et NOIRS. Cette zone doit être blindée et comporter une alimentation filtrée distincte des circuits situés en zone NOIRE. Les câbles non blindés devront être fixés au plus près de la masse métallique des boîtiers.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	30/42

Le boîtier

Le durcissement du boîtier d'un équipement peut s'opérer selon deux contextes.

Le premier traite la totalité des cartes comme des signaux ROUGES. L'ensemble est blindé en créant une cuve hermétique aux ondes radio et en isolant galvaniquement les entrées et sorties.

Le second contexte utilise le principe de séparation des zones ROUGE – NOIR. La zone ROUGE est blindée et filtrée à l'intérieur du boîtier afin de protéger au plus près les informations sensibles. Ceci minimise les risques de couplage interne et facilite la conception de boîtiers plus légers. La dimension des ouvertures et des aérations doit prendre en compte la nature des signaux à protéger (fréquence de travail / longueur d'onde). Une attention particulière doit être portée :

- aux dimensions internes des boîtiers pour limiter d'éventuelles résonances internes.
- au choix ou à la conception des filtres d'alimentation. En effet, les filtres secteur traditionnellement employés ne sont pas nécessairement adaptés aux signaux à traiter dans ce cas.

Les câbles blindés

La recherche d'un blindage optimal impose de connaître l'atténuation électromagnétique nécessaire et les caractéristiques de l'onde électromagnétique à traiter (gamme de fréquence, type de champ, notamment). Ces caractéristiques déterminent le type de matériau à utiliser et le choix du montage qui lui est associé.

Il existe plusieurs types de blindages de câbles, comme par exemple la tresse métallique, le feuillard ou l'écran métallique, choisis en fonction de l'application. L'efficacité du blindage dépend non seulement du type de câble retenu mais également de la qualité du raccordement du blindage au connecteur. Le blindage doit recouvrir au moins 85 % la surface de câble. Aux extrémités, le câble blindé doit être relié à un connecteur qui assure une continuité du blindage sur 360 degrés.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	31/42

NOTE TECHNIQUE 3 :

Les règles d'installation

L'objectif

Les conditions d'installation ont pour but de maîtriser la propagation des parasites en conduction. Celles-ci prennent en compte plusieurs facteurs, comme l'évaluation des équipements, la limite de la zone de sécurité et l'atténuation présentée par les locaux.

Dans le cas d'une installation dans un immeuble maîtrisé, affecté à une seule entité, dont la zone de sécurité est également contrôlée, les règles d'installation peuvent être simplifiées de manière méthodique. L'attention se portera dans ce cas sur le traitement des lignes d'entrées et sorties du bâtiment.

Dans le cas plus complexe de la protection d'une zone définie par un étage ou une seule pièce à l'intérieur d'un bâtiment, il convient de respecter les précautions décrites ci-après.

La zone de sécurité

Le résultat du zonage TEMPEST est directement lié à la détermination de la zone de sécurité, également appelée zone de sécurité TEMPEST (ZST) ou électromagnétique.

Il est généralement admis que plus une zone de sécurité électromagnétique est étendue, plus elle est difficile à contrôler. Le grillage ou le mur extérieur d'une enceinte peuvent être définis comme une limite de zone de sécurité. Cependant, le contrôle de l'ensemble des personnels et des véhicules se déplaçant sur le site devient dans ce cas une contrainte sévère à maintenir.

Il est préférable de définir à l'intérieur d'un site étendu une zone plus petite autour du lieu où sont traitées les informations sensibles, et de matérialiser le périmètre par un grillage ou tout autre dispositif. La zone libre de toute construction doit être aussi large que possible, et au moins supérieure à 20 m. Cette zone peut être matérialisée virtuellement par la présence d'une signalétique particulière excluant naturellement la présence et le stationnement de véhicules ou encore de mobilier urbain par exemple.

Une ZST peut être réduite à une seule pièce dans le cas d'un bâtiment non contrôlé ou partagé avec d'autres entités. Il convient alors de se protéger de façon appropriée, par exemple par la mise en œuvre de faradisation (enceinte, tente) ou de matériel TEMPEST de niveau « A » (rayonnement réduit et filtrage de l'alimentation).

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	32/42

La zone de couplage

Lors de l'installation d'un équipement, il faut tenir compte de la présence d'ouvrages métalliques tels que les tuyaux d'eau, les canalisations de chauffage, les gaines de climatisation et de câbles, y compris ceux des pièces adjacentes, afin d'éviter les couplages sur ces supports, qui favoriseraient la propagation des parasites. De ce fait, la continuité électrique des conducteurs métalliques doit être interrompue par l'insertion d'un manchon isolant placé à l'extérieur de toute zone de couplage et à l'intérieur de la zone de sécurité.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	33/42

NOTE TECHNIQUE 4 :

Les filtres

Les filtres sont des dispositifs conçus pour ne laisser passer que certaines fréquences. Ils sont généralement constitués de composants passifs (résistances, inductances et capacités...).

Les filtres sont couramment de type passe-bas et sont utilisés pour le filtrage de l'alimentation, de la téléphonie, de la transmission de données faible débit ou des signaux de servitudes. Pour les transmissions de données d'un débit supérieur à quelques kilobits par seconde, il est recommandé d'utiliser de préférence une transmission sur fibre optique, comme décrit dans la note suivante.

Un filtre se caractérise par :

- sa bande passante ;
- son atténuation ;
- ses impédances d'entrée et de sortie ;
- sa puissance nominale et son courant de fuite.

Par ailleurs, avant l'acquisition d'un filtre, il convient de s'assurer que :

- tous les circuits et les câbles inutiles ont été supprimés de la zone de couplage ;
- les circuits à filtrer ont été regroupés de façon optimale ;
- le filtre est compatible avec les caractéristiques de la ligne à filtrer.

Les filtres d'alimentation

Il est difficile de filtrer séparément tous les conducteurs sortant d'une zone de couplage et quittant la zone de sécurité. En effet, ces conducteurs sont généralement rassemblés dans une armoire de distribution.

Le choix du filtre résulte du besoin total en énergie électrique. Des solutions spécifiquement développées pour le TEMPEST existent sur le marché.

Un onduleur constitué d'un redresseur connecté au secteur et d'une batterie tampon, quelle que soit son architecture interne, ne constitue pas une protection suffisante vis-à-vis des signaux parasites compromettants. En raison de l'importance des courants de fuite liés aux filtres d'alimentation, l'ajout d'un transformateur d'isolement est parfois nécessaire.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	34/42

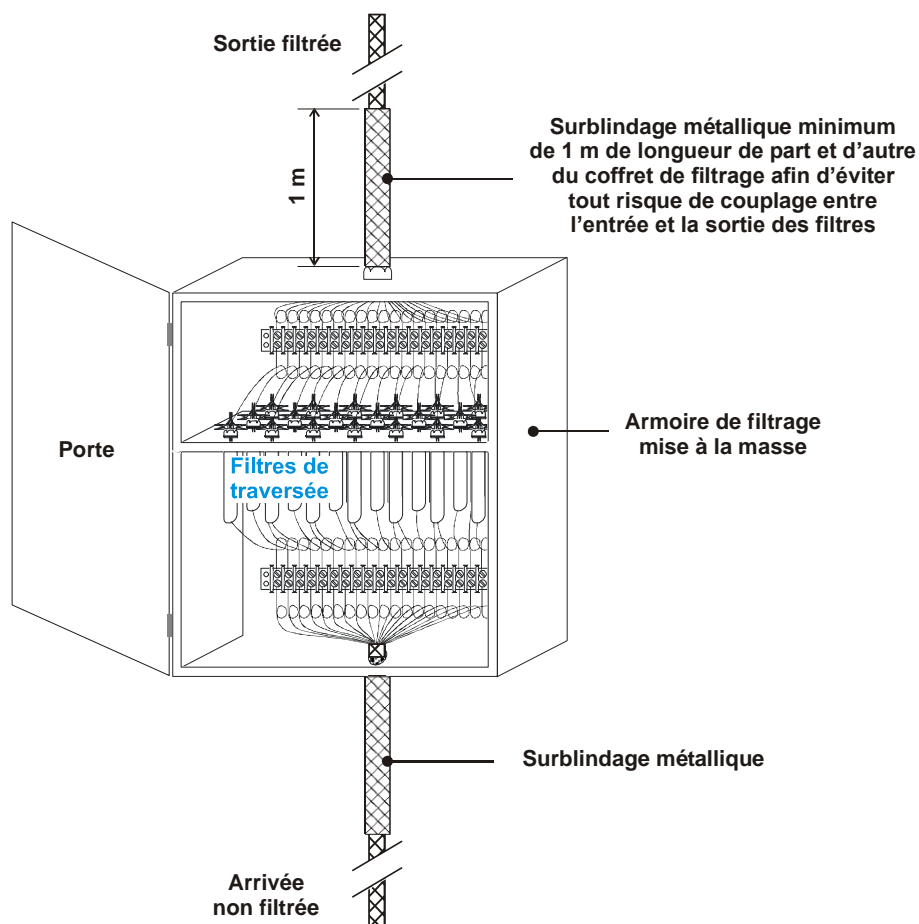
Les filtres analogiques basses fréquences

Les systèmes de téléphonie, les interphones et alarmes incendie peuvent aussi nécessiter un filtrage. Le filtre devra dans ce cas présenter une bande passante la plus étroite possible, n'excédant pas quelques kilohertz.

Installation et précautions de mise en œuvre des filtres

Les filtres doivent être installés à l'intérieur d'un coffret dont les entrées et sorties sont placées en opposition, tel qu'illustré en figure 1. Le coffret de filtrage doit être relié au plus court possible, soit au plan de masse local, soit au puits de terre de l'installation. Les performances des filtres utilisés pour les cages de Faraday ne doivent pas dégrader les caractéristiques de l'enceinte.

Figure 1 : Exemple de mise en œuvre d'une armoire de filtrage



Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	35/42

NOTE TECHNIQUE 5 :

Les fibres optiques

Un système à fibre optique se compose de deux organes de terminaison et d'une fibre optique.

Caractéristiques des fibres optiques

Les fibres optiques :

- ne génèrent pas de rayonnement électromagnétique ;
- ne sont pas sensibles aux phénomènes de diaphonie ;
- ne sont pas sensibles aux phénomènes de boucles de masse ;
- ne sont pas sensibles aux effets de résonance qui peuvent accentuer les trois effets précédents sur les câbles métalliques.

Pour toutes ces raisons, l'utilisation d'un système à fibre optique est préférable à l'utilisation de câbles conventionnels, pour la transmission d'informations sensibles en clair à l'intérieur d'une zone de sécurité. Toutefois, leur emploi demande des protections physiques contre les dommages et les altérations. Il reste par ailleurs recommandé de chiffrer les informations transmises pour empêcher tout risque de compromission par l'emploi de dispositifs d'écoute appliqués sur la fibre.

Si les fibres optiques elles-mêmes ne présentent pas de caractère rayonnant, il faut néanmoins apporter une attention particulière à l'installation des équipements de terminaison qui doivent être considérés comme partie intégrante du matériel de transmission.

Applications

Les systèmes optiques peuvent être utilisés pour supprimer la fuite de signaux parasites compromettants vers l'extérieur de la zone de sécurité, d'une façon semblable au filtrage. Néanmoins, il faudra considérer, lors de l'installation du système, la zone de couplage propre au terminal optique. Afin de ne pas augmenter la zone de couplage globale, le terminal optique pourra être placé au centre de celle-ci.

Les fibres optiques servent également à réaliser une isolation galvanique entre deux installations ou à transmettre des informations par le guide d'onde d'une cage de Faraday, en évitant ainsi l'utilisation de filtres. Dans ce cas, il convient de s'assurer que la protection mécanique de la fibre n'est pas métallique.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	36/42

NOTE TECHNIQUE 6 :

La mise à la terre

La mise à la terre des installations, des matériels et des filtres est rendue obligatoire pour assurer la protection physique des personnels. Lorsque le puits de terre ne se situe pas dans la zone de sécurité, des précautions particulières sont nécessaires pour éviter tout raccordement illicite.

La constitution du circuit de terre

Un circuit de terre peut être décomposé en 3 éléments :

- le puits de terre, lieu de contact électrique entre le sol (terrain) et l'installation électrique ou électronique à protéger ;
- le conducteur de liaison entre le puits de terre et l'installation ;
- le réseau de conducteurs de masse ou terre, qui distribue le potentiel zéro auprès de tous les équipements de l'installation.

Recommandations

- le circuit de terre doit être câblé en étoile ;
- si le puits de terre est éloigné de plusieurs dizaines de mètres, alors il est préférable de recréer un plan de masse local, plancher technique par exemple, connecté au puits de terre général. De nombreux ouvrages publics traitent de ce sujet en détail.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	37/42

NOTE TECHNIQUE 7 :

Autres solutions de durcissement

Si les règles d'installation ne peuvent pas être respectées, il est possible d'opter pour des moyens basés sur le principe de faradisation. Il convient alors de procéder à une prise en compte globale du durcissement, réalisée par des spécialistes et mise en œuvre par du personnel sensibilisé à ces moyens de protection.

Un moyen de protection faradisé a pour but d'atténuer le champ électrique, le champ magnétique et les ondes planes à l'intérieur d'un espace clos.

Afin de maintenir les performances attendues il convient :

- de traiter toutes les entrées et sorties par des dispositifs adaptés, y compris les portes et fenêtres ;
- d'appliquer des filtres aux lignes d'alimentations électriques et aux signaux faibles ; la mise en place de guides d'ondes autorise le passage de fibres optiques non blindées métalliquement ou de canalisations non conductrices (manchons isolants) ; les nids d'abeille autorisent les ouvertures nécessaires aux aérations ;
- de s'assurer de la bonne installation des dispositifs pour ne pas dégrader l'affaiblissement global recherché ;
- de relier la masse du moyen en un seul point à la terre. Tout autre contact d'un élément métallique externe à l'enceinte doit être éliminé, et il convient de disposer d'une barrette de coupure de terre permettant la vérification de la mise à la terre ;
- de réaliser enfin une maintenance préventive sur les éléments mécaniques, sur les joints des ouvrants et sur la corrosion de certains éléments, comme les nids d'abeilles.

Selon les conditions d'utilisation, il peut également être nécessaire d'effectuer un entretien périodique.

Différentes solutions techniques permettent de réaliser des ensembles faradisés. Ces moyens dépendent des performances de l'atténuation globale souhaitée et du volume utile nécessaire pour déployer les équipements. D'autres facteurs entrent en compte dans le choix de la faradisation. Les matériaux de construction seront différents selon les conditions d'utilisation attendues, occasionnelles ou permanentes, et selon la configuration des locaux d'accueil, par exemple en cas d'installation dans des combles.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	38/42

La baie faradisée

Ce moyen est conçu pour abriter des appareils de petites dimensions faisant partie d'un système. Différents types de baies sont disponibles, les baies TEMPEST et les baies CEM. Le choix d'un produit dépend de ses conditions d'installation sur le site.

Caractéristiques :

- performances d'atténuation de 30 à 40 dB selon les solutions techniques retenues ;
- administration à distance des systèmes hébergés dans la baie conseillée ;
- installation fixe ou mobile.

La cage de Faraday modulaire

La cage modulaire permet de créer des volumes faradisés de grandes dimensions sur mesure. Les systèmes installés à l'intérieur n'exigent pas de règles d'installation rigoureuses. La performance de ce type de cage est définie sur la base de gabarits dédiés en fonction des utilisations souhaitées.

Caractéristiques :

- atténuation de 80 à 100 dB pour un site de traitement d'information ;
- composée de panneaux composites recouverts de tôles galvanisées ;
- mise en place facile et de conception robuste ;
- panneaux démontables et transformables ;
- bon rapport coût/atténuation/mise en œuvre.

La cage de Faraday type feuillard de cuivre

Cette conception est utilisée pour protéger un local au sein d'un bâtiment. L'atténuation est généralement réalisée au moyen de feuilles de cuivre de 3/10^e mm plaquées sur les murs, puis soudées à l'étain. Cela implique le traitement des ouvrants tels que les portes et les fenêtres.

Caractéristiques :

- atténuation de 80 dB en champ électrique et ondes planes ;
- réalisation non démontable, mais qui se prête à certaines transformations ;
- construction fragile au niveau des soudures à l'étain ;
- pratique pour les grandes pièces à géométrie variable.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	39/42

La tente faradisée

Ce moyen est utilisé pour des protections occasionnelles sur des systèmes projetables, notamment pour des mises en œuvre sur le terrain, à l'intérieur des bâtiments ou dans des espaces non contrôlés.

Caractéristiques :

- atténuation de 50 à 60 dB en champ électrique et ondes planes ;
- installation rapide et disponible en plusieurs tailles ;
- fragilité des matériaux constituant la tente, durant la mise en œuvre et l'exploitation ;
- un contrôle systématique doit être réalisé après chaque installation, avant la mise en service opérationnelle.

Les revêtements muraux

L'atténuation apportée à une pièce est réalisée au moyen de papiers, tissus ou peintures conductrices, qui sont appliqués sur les murs. Cela implique que les six faces du local et ses ouvrants soient traités. L'application de ces produits ne peut être réalisée que par des professionnels sensibilisés à la technique de faradisation.

Caractéristiques :

- atténuation faible en champ électrique et ondes planes ;
- mise en œuvre délicate ;
- performances directement liées à la qualité de la mise en œuvre.

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	40/42

NOTE TECHNIQUE 8 :

Dossier relatif aux installations

Ce dossier est constitué de trois parties : la description, les mesures et la synthèse. Il doit être mis à jour chaque fois qu'une modification significative a été apportée à l'installation.

Il est recommandé que le responsable de sécurité du site contrôle, ou fasse contrôler, périodiquement la conformité de l'installation vis-à-vis de son état initial, et procède si nécessaire à sa mise en conformité.

La partie description

Elle permet d'identifier la position des installations, ainsi que les moyens mis en œuvre pour le traitement d'informations sensibles sur le site. Elle doit contenir :

1. un plan du site (avec échelle) précisant :
 - la limite de la zone de sécurité ;
 - la situation du bâtiment dans la zone de sécurité vis-à-vis de la clôture et des autres bâtiments ;
 - les points d'arrivée de l'énergie dans la zone de sécurité ;
 - les conduits métalliques (tuyau d'eau, de chauffage) sortant de la zone de sécurité ;
 - les arrivées des lignes de communication quittant la zone de sécurité (PABX, notamment) ;
 - la position du puits et des barrettes de terre.

2. un plan de masse du bâtiment avec l'échelle du plan précisant :
 - la localisation des dispositifs de filtrage ;
 - la localisation des locaux faradisés ;
 - la localisation des matériels traitant des informations sensibles s'il y a peu de postes ;
 - la localisation des moyens de communication sans fil présents sur le site.

La partie mesures

Cette partie collecte tous les comptes-rendus des mesures effectuées sur le site (zonage, affaiblissement des cages de Faraday, résultats de tests sur les équipements, etc...).

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	41/42

La partie synthèse

Cette partie énumère les points faibles relevés dans le dossier de mesures et mentionne les corrections à apporter et les conditions d'emplois particulières à respecter, comme par exemple :

- l'amélioration de la protection physique ;
- le déplacement de certains équipements sensibles ;
- les appareils à mettre hors service lors de l'utilisation de certains équipements (émetteurs RF, par exemple).

Instruction interministérielle n° 300 relative à la protection contre les signaux compromettants			
Version	Date	Critère de diffusion	Page
1.2	23 juin 2014	Public	42/42