EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
ORGANISATION EUROPÉENE POUR LA RECHERCHE NUCLÉAIRE

CERN - ST Division

CERN-ST-2000-026
February, 2000

IDENTIFICATION DES FONCTIONS ET DES CONTRAINTES PRINCIPALES LIEES A LA REALISATION DES SYSTEMES DE SURETE DU LHC

E. Cennini

Résumé

Dans la perspective de la spécification des systèmes de sûreté du LHC (systèmes de contrôle d'accès et de verrouillage des faisceaux), les études actuelles consistent à identifier les contraintes et les performances pour la définition des différentes fonctions requises. Du concept d'accès aux ouvrages souterrains du LHC et de l'expérience acquise dans la réalisation et l'exploitation de systèmes de sûreté découlent les spécifications des fonctions à implanter au niveau des couches *Equipement*, *Contrôle* et *Supervision*. Les fonctions des systèmes de sûreté sont soumises à un nombre élevé de contraintes et doivent satisfaire des critères de performances précis. Le présent document a pour objectif d'identifier les fonctions et les contraintes principales, de les classer selon leur nature, d'exprimer certains critères de performance et enfin de décrire leur impact sur les fonctions requises au niveau des couches énoncées ci-dessus. De cette analyse découleront des propositions concrètes liées à l'architecture et à la composition des systèmes de sûreté ainsi qu'à l'exploitation du système de contrôle d'accès du LHC.

Presented at the 3rd ST Workshop
Chamonix, France, January 25 - 28, 2000

1 INTRODUCTION

Le concept d'accès au LHC [1] définit un cheminement à travers quatre zones (fig. 1) dont les risques intrinsèques déterminent les caractéristiques des contrôles à effectuer.

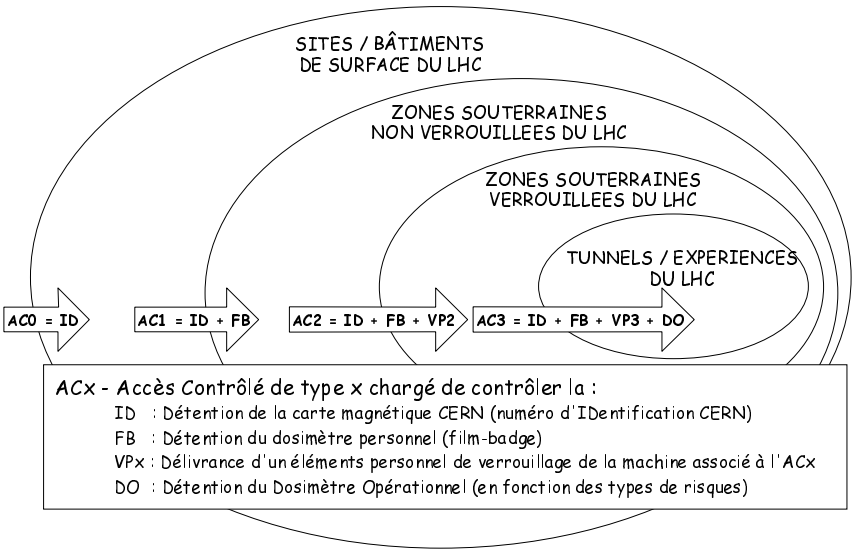

Figure 1 : Concept d'accès et classification des ouvrages souterrains du LHC.

Pour spécifier les systèmes de sûreté du LHC, la démarche adoptée consiste à recueillir les contraintes intrinsèques et à définir les critères de performances requis pour chaque zone identifiée dans le concept ci-dessus. Elle aboutit ainsi à la spécification des fonctions requises au niveau des systèmes de contrôle d'accès et de verrouillage des faisceaux.

2 IDENTIFICATION ET CLASSIFICATION DES CONTRAINTES

2.1 Caractéristiques des utilisateurs

Toute personne travaillant pour le compte de l'Organisation doit posséder sa carte d'accès nominative, non transmissible, délivrée par les Services Administratifs (AS) conformément à la *Circulaire Opérationnelle No. 2*. L'accès aux ouvrages souterrains du LHC nécessite la détention d'un film-badge ainsi que des autorisations spécifiques délivrées via *l'Authorization Management System - AMS*.

2.2 Contraintes organisationnelles

2.2.1 Gestion opérationnelle de projet

Le projet LHC utilise une gestion opérationnelle de projet [2] dont l'organisation des relations entre le *client* et le *fournisseur* identifie des rôles précis (fig. 2). Conceptuellement, pour la partie *client*, le *Maître d'Ouvrage - MO* achète le produit et peut arrêter le projet à tout moment ; le *Maître d'Ouvrage délégué - MOd* est le directeur du projet, il définit le jalon final du projet et exprime les attentes des *utilisateurs*. Pour la partie fournisseur, le *Maître d'Oeuvre - ME* est financièrement responsable du bon achèvement du projet et peut allouer des moyens supplémentaires après en avoir convenu avec le *MO* ; le *Maître d'Oeuvre délégué - MEd* est le chef de projet, il est en contact régulier avec le *MOd* pour assurer l'adéquation de la fourniture ou du service implanté par les *contributeurs*.

2.2.2 Organisation établie pour le sous-projet de fourniture des systèmes de sûreté du LHC

Le *sous-projet* de fourniture des systèmes de sûreté du LHC touche une partie importante de l'organisation du projet LHC en plus de l'identification des besoins liés à l'accès. En effet, afin de définir les interfaces du système de verrouillage des faisceaux, il est impératif d'identifier les scénarios d'arrêt de l'accélérateur.

Ce système doit offrir des fonctions de sécurité du matériel, c'est pourquoi les services et les groupes de travail de l'accélérateur lui-même sont représentés comme des utilisateurs des systèmes de sûreté. Les contributeurs impliqués dans la fourniture des systèmes de sûreté du LHC appartiennent à divers services du CERN tels que ST-EL pour l'alimentation des systèmes et pour les réseaux de communication audio, IT pour les réseaux de communication etc…

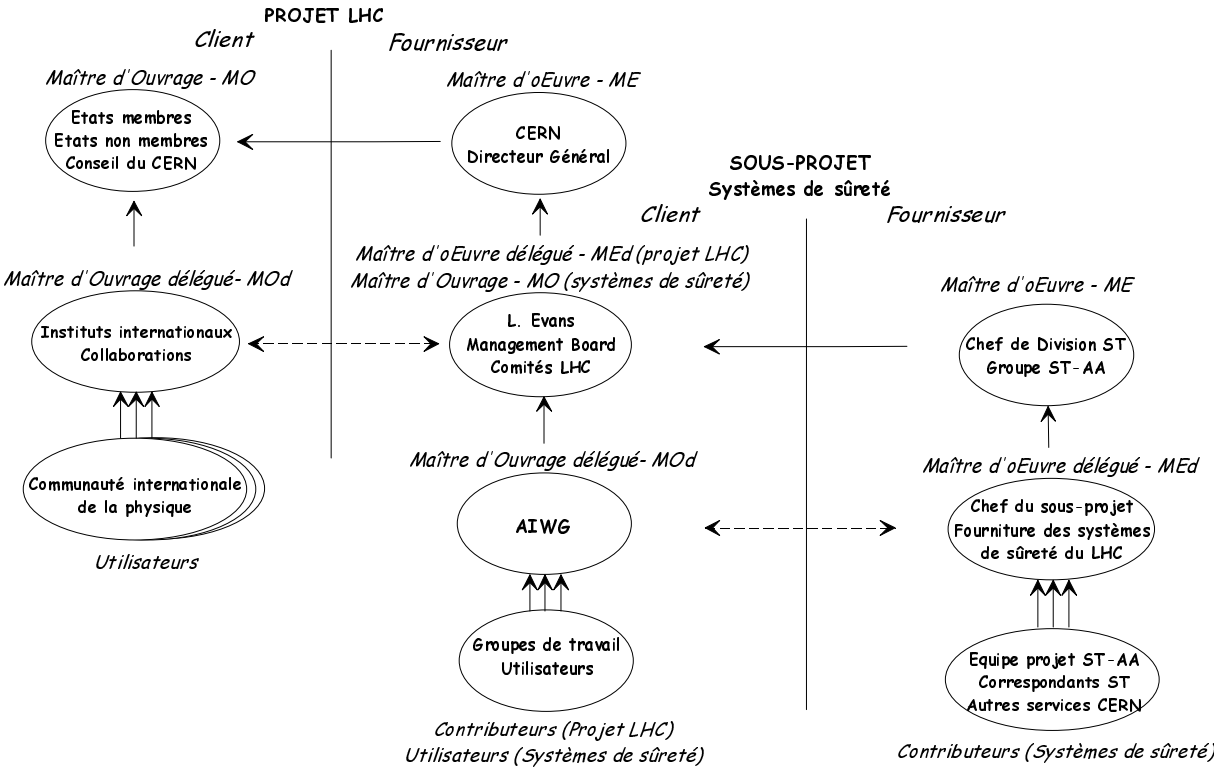

Figure 2 : Organisation pour la gestion opérationnelle du projet des systèmes de sûreté au sein du projet LHC.

2.3 Contraintes INB

Bien que le LHC, du point de vue INB, ne souffre d'aucune comparaison avec le LEP, les recommandations émises pour les systèmes de sûreté du LEP constituent des indications et des contraintes importantes pour le design des systèmes du LHC à savoir :

- les signaux redondants des Eléments Importants de Sûreté doivent impérativement être acheminés par des voies physiques indépendantes tout au long de l'architecture des systèmes de sûreté,
- dans le cas de l'utilisation d'automates programmables dans la réalisation d'un système de sûreté, ceux-ci doivent être *auto-contrôlés*,
- le redémarrage de l'accélérateur doit être précédé par une signalisation *Faisceaux imminents*.

2.4 Contraintes d'exploitation

Une contrainte importante pour le système de contrôle d'accès du LHC réside dans l'absence de mode libre. En clair, l'accès aux zones verrouillées du LHC est contrôlé en permanence. Les maintenances corrective et préventive doivent se dérouler sans empêcher l'accès contrôlé à l'accélérateur. Une caractéristique de haute disponibilité est donc requise au niveau des points d'accès.

En mode machine les systèmes de sûreté doivent garantir le verrouillage de tous les zones et surtout l'arrêt immédiat de l'injection et de la circulation des faisceaux dans le cas d'un accès intempestif par activation d'un dispositif de passage d'urgence. La caractéristique de haute sécurité s'impose donc au niveau des organes de contrôle dédiés à la sûreté.

2.5 Contraintes environnementales

Lorsque les faisceaux circulent, les perturbations radiologiques, magnétiques, électromagnétiques … engendrées par l'accélérateur constituent des contraintes non négligeables pour la protection des équipements de l'accélérateur. Au sein des systèmes de sûreté ces contraintes sont d'autant plus critiques que les pannes, consécutives à une altération occasionnée par ces perturbations, entraînent l'arrêt de l'accélérateur et sont susceptibles d'endommager des équipements importants de la machine.

2.6 Contraintes de réalisation

2.6.1 Contrainte géographique

Tout comme pour le LEP, les distances à parcourir ainsi que le nombre de signaux à acheminer constituent des contraintes importantes notamment pour l'architecture du réseau de contrôle lié à la sécurité de par le fait que les signaux des systèmes de sûreté doivent être acheminés jusqu'au système d'interverrouillage localisé en salle de contrôle.

2.6.2 Contrainte topologique

La configuration des ouvrages souterrains du LHC et la concentration des EIS-accès dans les sections droites représentent également des contraintes pour l'architecture de contrôle locale liée à la sûreté et celle liée à l'exploitation.

2.6.3 Contraintes matérielles

Les principales contraintes pour les équipements d'accès découlent des considérations suivantes :

- l'accès par rafales du personnel et du matériel (pics de sollicitation des équipements d'accès),
- l'emprise de la machine au sein des tunnels du LHC et la nécessité d'octroyer un passage à encombrement minimum pour les véhicules de levage,
- verrouillage mécanique fiable et résistant des portes/grilles d'accès.

2.6.4 Contrainte de conception système

Afin de réduire au minimum la probabilité de défaillance des systèmes de sûreté du LHC, l'expérience acquise ainsi que l'analyse de sûreté des systèmes du LEP ont démontré que seul l'acheminement redondant de signaux à boucle de courant câblés et à sécurité positive offre les meilleures performances. Cette caractéristique implique l'utilisation de systèmes d'automatisation à haute disponibilité et à haute sécurité. L'alimentation secourue de ces systèmes doit également être prise en considération.

2.6.5 Contrainte liée à l'installation et à la validation des équipements machine

Dans le planning d'installation du LHC, une phase de test d'injection des faisceaux est prévue dès le début de l'année 2004. En conséquence, des systèmes de sûreté provisoires devront être mis en service pour les sites et les EIS-machine concernés.

3 IDENTIFICATION ET CLASSIFICATION DES FONCTIONS PRINCIPALES

3.1 Architecture et fonctions principales des systèmes de sûreté

L'architecture des systèmes de sûreté se décline suivant trois couches distinctes :

- la couche *Equipement* correspond au procédé à contrôler, en l'occurrence il s'agit de tous les EIS (accès et machine) du LHC,
- la couche *Contrôle/Communication* couvre les éléments de gestion et de contrôle du procédé. Pour les systèmes de sûreté, il est envisagé de réaliser un réseau industriel basé sur l'utilisation d'automates programmables spécifiques.
- la couche *Supervision*, comme son nom l'indique, contient le matériel et l'infrastructure de communication permettant la supervision et le suivi du procédé.

Au sein de ces couches, chaque élément constitutif des systèmes de sûreté remplit des fonctions précises dédiées, soit au contrôle de l'accès, soit au verrouillage des faisceaux. Celles-ci se répartissent suivant les deux caractéristiques principales suivantes :

- la sûreté (tableau 1 en Annexes) garantissant l'arrêt de l'accélérateur en cas d'accès intempestif et protégeant les équipements de la machine lors de ces arrêts d'urgence. Le déclenchement des commandes de verrouillage de l'un des systèmes de sûreté sur l'autre doit s'effectuer de manière automatique avec un haut niveau de sécurité (caractéristiques fail-safe, redondance …) ;
- l'exploitation (tableau 2 en Annexes) du système de contrôle d'accès pendant les arrêts de la machine pour la supervision des procédures d'accès. L'absence de mode libre pour le LHC implique que les fonctions et les équipements d'accès soient hautement disponibles notamment pour l'arrêt technique (1 heure d'accès par tranches de 24 heures).

Les tableaux 1 et 2 en *Annexes* représentent les fonctions des systèmes de sûreté réparties suivant les couches et les caractéristiques décrites ci-dessus. Ces listes de fonctions, non exhaustives, et cette forme de classification aident à la spécification des systèmes et permettent la vérification ainsi que l'établissement de deux cahiers de recette indépendants, un pour la sûreté et l'autre pour l'exploitation.

4 PROPOSITIONS POUR LES SYSTEMES DE SURETE

L'identification des contraintes ainsi que la définition des fonctions requises au niveau des couches *Equipement*, *Contrôle* et *Supervision* amènent, au stade actuel des études, des propositions concrètes pour les systèmes de sûreté du LHC. Celles-ci concernent aussi bien le concept d'accès général que la supervision, le contrôle et le matériel envisagés. Toutes ces propositions seront présentées pour approbation au maître d'ouvrage et permettront de poursuivre la rédaction des spécifications fonctionnelle et opérationnelle des systèmes de sûreté.

4.1 Distinction accès machine/accès expérience

Une première estimation du nombre d'automates nécessaires à la réalisation des systèmes de sûreté dépasse la configuration maximale indiquée par le constructeur. Il est donc indispensable de revoir l'architecture du réseau de contrôle. D'autre part, la proximité de certains EIS-accès de l'enveloppe des zones verrouillées avec l'accélérateur constitue un risque important pour la sécurité du matériel dans le cas d'un passage d'urgence. Cette proximité est essentiellement localisée dans les zones de service des expériences accessibles pendant le fonctionnement de l'accélérateur. En conséquence, il est proposé et recommandé de structurer le réseau de contrôle en distinguant les zones d'accès dédiées à la machine de celles dédiées aux cavernes expérimentales.

4.2 Méthode permettant de définir les zones de tests du LHC

L'identification des zones de test du LHC découle de la méthode proposée ci-dessous :

- Localiser les équipements machine à tester pendant les arrêts.
- Localiser les éléments de contrôle des équipements concernés (pour le verrouillage) et définir les caractéristiques des interfaces (signaux de sûreté, commandes de verrouillage, signal de présence de câble, conditions particulières).
- Identifier/choisir le point d'accès principal et les limites de chaque zone de test (enveloppe).
- Rajouter une zone tampon aux limites de la zone de test.
- Au cas ou des équipements machine spécifiques localisés dans la zone de test nécessitent un autre type de test, un secteur associé à ces équipements doit être défini.
- Définir le mode d'accès à chaque zone de test (base de données restreinte, …).
- Identifier les autres besoins.

4.3 Supervision centralisée/décentralisée

De par l'étendue et la fréquentation prévue du LHC, il est proposé une supervision locale (au niveau des sites) des points d'accès. Ainsi, une fois la sécurité établie via les clés de sécurité centrale du système d'interverrouillage, des personnes autorisées et formées seront en mesure de donner l'accès à leur caverne expérimentale ou à leur zone de test. Ou encore, lors d'une défaillance du réseau de communication, la possibilité de superviser l'accès depuis chaque site est un avantage notoire. La décentralisation de la supervision du système de contrôle d'accès est possible du fait qu'aucune des fonctions liées à la sécurité ne sont assurées par l'informatique.

4.4 Organisation des bases de données du Personnel pour l'accès au LHC

Cette organisation découle directement de la définition des modes d'accès. Afin de couvrir l'ensemble des besoins il est proposé d'associer, à chaque mode et pour chaque voie/point d'accès, une base de données dédiée (tableau 1). Cette organisation, lourde en première approche, permettra néanmoins de couvrir les futures restrictions d'accès sans modifier les programmes de supervision.

Tableau 1 : Distribution des bases de données du Personnel pour l'accès au LHC.

Organisation des bases de données du Personnel	Zones vérouillées pour l'accès dédié à la machine	Zones vérouillées pour l'accès dédié aux expériences
Modes d'accès du LHC	**Par voie/point d'accès (systèmes AC2 et AC3-p)**	**Par point d'accès (systèmes AC3-p)**
Fermé + Veto	Accès interdit	Accès interdit
Fermé	Accès interdit	Accès interdit
Test	Accès interdit ou 1 base de données	
Patrouille/Survey	1 Base de données	1 Base de données
Supervisé restreint	1 Base de données	1 Base de données
Supervisé	1 Base de données	1 Base de données
Contrôlé automatique	1 Base de données	1 Base de données
Nombre de voie/point d'accès	~ 50	~15
Nombre de DBs nécessaires	200	60

4.5 Systèmes *d'Accès Contrôlé AC3-p*

Sur la base des fonctions requises et des contraintes associées à ces systèmes, la constitution suivante est proposée :

Système AC3-p pour l'accès dédié à la machine :

- un intercom et une caméra vidéo pour la procédure d'accès,
- un moniteur local pour l'affichage des modes d'accès et pour l'assistance à l'utilisateur,
- un sas pour le passage du Personnel contenant :
  - un lecteur de film-badge (insertion manuel),
  - un lecteur détectant la détention du dosimètre opérationnel de radioprotection,
  - un système électronique de vérification de la présence d'une seule personne dans le sas,
  - un dispositif de passage d'urgence (en entrée/sortie),
- une *cage* d'accès équipée d'une porte pour le passage du matériel.

Système AC3-p pour l'accès dédié aux expériences :

- Idem plus un système de délivrance de *token*.

Ces systèmes seront modulaires afin de s'adapter aux différentes configurations pour faciliter l'accès du personnel et du matériel.

4.6 Systèmes *d'Accès Contrôlé AC2*

Sur la base des fonctions requises et des contraintes associées à ces systèmes, ils proposent deux voies d'accès distinctes (disponibilité) constituées des équipements suivants :

Système AC2 pour l'accès dédié à la machine (par voie d'accès) :

- un intercom et une caméra vidéo pour la procédure d'accès,
- un moniteur local pour l'affichage des modes d'accès et pour l'assistance à l'utilisateur,
- un lecteur de film-badge (insertion manuel),
- un système de délivrance de *token*,
- un sas pour le passage du Personnel contenant :
    - un système électronique de vérification de la présence d'une seule personne dans le sas,
    - un dispositif de passage d'urgence (en entrée/sortie),
- un sas pour le passage du gros matériel (sas LEP existants remis à neuf).

Le passage du matériel s'effectue selon une procédure d'accès prédéfinie par l'intermédiaire du sas prévu à cet effet. La consigne principale de la procédure interdit formellement le passage du personnel via le sas matériel.

5 CONCLUSIONS

La réalisation des systèmes de sûreté du LHC nécessite la prise en compte d'un nombre important de caractéristiques liées au fonctionnement de l'accélérateur et surtout à la sûreté du personnel et du matériel. Ces caractéristiques requièrent la mise en oeuvre de fonctions fiables qui doivent tenir compte de différentes contraintes. La composante humaine au sein d'un système de sûreté demeurant la moins fiable, il est indispensable de concevoir une architecture technique capable de tenir compte des contraintes inhérentes à l'environnement et au fonctionnement d'un accélérateur tel que le LHC. Toutefois, à trop vouloir éliminer les contraintes on risque de changer la fonctionnalité requise. En conséquence, la discipline des utilisateurs et des opérateurs du LHC passe par le respect de consignes simples qui complètent efficacement le bon fonctionnement des systèmes de sûreté. Il est à noter que ce document est extrait de la Note de Division ST en cours de publication sous la référence ST-AA (99–003).

REFERENCES

[1] G. Rau - Rapport préliminaire de sûreté du LHC.

[2] Cours *Gestion Opérationnelle de Projet* mandaté par P. Bonnal et suivi, en particulier par le personnel du Groupe ST-AA.

ANNEXES

Tableau 1 : Classification et liste des fonctions liées à la sûreté du LHC.

SÛRETÉ DU LHC	
Fonctions liées à la sûreté (système hardware autonome)	
L'informatique n'intervient pas pour la sûreté de l'accélérateur	**COUCHE SUPERVISION / DBs**
Fonctionnement et opérabilité du système d'interverrouillage : ~ modules de clés de sûreté centrales, locales, tests, ~ gestion des résultantes des chaînes de sûreté, ~ génération des commandes de verrouillages VETO.	**COUCHE CONTRÔLE/COMMUNICATION**
Connexion au système d'interverrouillage : ~ interface avec les automates concentrateurs, ~ caractéristiques du système (clés de sûreté centrales, clés test …), ~ modularité/extensibilité du système.	
Organisation et gestion des résultantes de sûreté : ~ établissement des chaînes de verrouillage principales, locales, tests, ~ les caractéristiques des automates concentrateurs "accès" et "machine", ~ paramétrisation/modularité des chaînes de verrouillage.	
Acheminement des résultantes des système de sûreté : ~ identification du cheminement vers le système d'interverrouillage, ~ interconnexion avec les concentrateurs "accès" des sites adjacents, ~ relayage des résultantes de sûreté.	
Organisation et gestion des signaux de sûreté : ~ établissement des chaînes de verrouillage locales et tests, ~ les fonctions liées à la patrouille, aux tests, ~ les caractéristiques des automates, ~ génération des signaux de sûreté résultants.	
Architecture de contrôle/communication à haute sécurité	
Acquisition des signaux de sûreté par le réseau de contrôle : ~ format et caractéristiques des signaux de sûreté, ~ architecture locale (vers le bas) du réseau de contrôle lié à la sûreté.	**COUCHE EQUIPEMENT**
Interfaces hard pour la connexion au réseau de contrôle : ~ type d'interface hardware, ~ caractéristiques des borniers (modularité, signalétique).	
Acheminement des signaux de sûreté des EIS : ~ caractéristiques des câbles, ~ caractéristiques des boîtes de jonction.	
Acquisition des signaux de sûreté des EIS : ~ définition des interfaces hardware (contacts, systèmes,…), ~ caractéristiques des interfaces.	
Définition des signaux de sûreté pour les EIS	
Identification des EIS du LHC : ~ liste des interfaces, ~ descriptions fonctionnelle et opérationnelle, ~ topologie, localisation.	

Tableau 2 : Classification et liste des fonctions liées à l'exploitation du LHC.

EXPLOITATION DU LHC		
Fonctions pour l'exploitation (Opérateurs)	**Fonctions pour l'exploitation (Utilisateurs)**	
Gestion, organisation des bases de données : ~ bases de données associées au mode d'accès, ~ bases de données par point d'accès, ~ mise à jour "en ligne" des bases de données.		**COUCHE SUPERVISION / DBs**
Supervision des systèmes de sûreté en mode *machine* : ~ synoptiques généraux, ~ signalisation des états de tous les signaux de sûreté, ~ historique des événements, ~ génération des alarmes, ~ assistance aux opérateurs.		
Supervision des systèmes de sûreté en mode *accès* : ~ synoptiques généraux, ~ signalisation des états de tous les signaux de sûreté, ~ historique des événements, ~ génération des alarmes, ~ assistance aux opérateurs.		
Supervision des procédures d'accès en mode "supervisé/supervisé restreint" : ~ procédures associées aux modes d'accès appliqués, ~ autorisation pour la décentralisation de la supervision.		
Supervision des procédures d'accès en mode "Patrouille/Survey" : ~ procédures associées au mode d'accès appliqué, ~ autorisation pour la décentralisation de la supervision.		
Supervision des procédures d'accès en mode "Tests" : ~ procédures associées au mode d'accès appliqué, ~ autorisation pour la décentralisation de la supervision.		
Supervision depuis les salles de contrôle des expériences : ~ gestion des modes d'accès, ~ suivi du procédé (synoptiques locaux, signalisation des modes), ~ interface MMI pour les procédures et historiques d'accès.	Supervision locale liées pour l'exploitation des points d'accès : ~ base de données locales, ~ interface MMI pour l'assistance à l'utilisateur, ~ liste des présences, des token délivrés.	
SCADA pour l'interface avec la couche de supervision : ~ caractéristiques techniques (protocole, types et format des données/fichiers), ~ caractéristiques fonctionnelles (adaptabilité, homogénéité, fiabilité), ~ organisation/répartition du réseau de communication.		**COUCHE CONTRÔLE/COMMUNICATION**
Cheminement des communications jusqu'aux salles de contrôle : ~ architecture du réseau, ~ noeuds de communication, ~ voies de secours.		
Interface avec les réseaux de communication à haut débit : ~ type d'interface/protocole, ~ mode de fonctionnement, ~ supervision de l'accès au niveau d'un site (accès à la machine), ~ supervision de l'accès au niveau d'un site (accès à l'expérience).		
Communications pour la gestion centrale des EIS-accès : ~ architecture de communication générale, ~ réseau de communication pour l'accès aux expériences, ~ réseau de communication pour l'accès à la machine.	Communications pour la gestion locale des points d'accès : ~ architecture de communication au niveau d'un site, ~ réseau de communication pour l'accès aux expériences, ~ réseau de communication pour l'accès à la machine.	
Le réseau de contrôle dédié à l'exploitation des points d'accès : ~ gestion des équipements des points d'accès du LHC (AC2, AC3-p), ~ communication des données pour les synoptiques généraux et locaux, ~ les caractéristiques du contrôle et de la communication (disponibilité), ~ concentrateurs de communications avec les points d'accès.		
Architecture de contrôle/communication à haute disponibilité		
Acquisition des signaux de sûreté par le réseau de contrôle : ~ format et caractéristiques des signaux de sûreté, ~ architecture locale (vers le bas) du réseau de contrôle lié à la sûreté.		**COUCHE EQUIPEMENT**
Interfaces hard pour la connexion au réseau de contrôle : ~ type d'interface hardware, ~ caractéristiques des borniers (modularité, signalétique).		
Acheminement des signaux de sûreté des EIS : ~ caractéristiques des câbles, ~ caractéristiques des boîtes de jonction.		
Acquisition des signaux de sûreté des EIS : ~ définition des interfaces hardware (contacts, systèmes,…), ~ caractéristiques des interfaces.		
Définition des signaux de sûreté pour les EIS		
Identification des EIS du LHC : ~ liste des interfaces, ~ descriptions fonctionnelle et opérationnelle, ~ topologie, localisation.		