

Comité d'Experts

Diagnostic et Sûreté de Fonctionnement

Synthèse

19 février 2007

1 Préambule

1.1 Objectifs et fonctionnement du CE

Le comité a été créé fin novembre 2005 par Robert Plana. Ce comité réunit des chercheurs des communautés automatique, informatique et traitement du signal, spécialistes des problèmes de diagnostic, surveillance, supervision et sûreté de fonctionnement. Il a pour objectifs la mise en évidence de verrous scientifiques disciplinaires et défis inter-disciplinaires, et la définition d'actions prioritaires. La composition du CE et les compétences de ses membres sont décrites en Annexe 1.

Pour des raisons d'incertitudes quant à son financement et son devenir, il n'a pu se réunir que deux fois: en janvier et décembre 2006. Les tâches de fond envisagées lors de sa mise en place sont rappelées en Annexe 2.

1.2 Remarques sur l'intitulé et le champ du CE

Il est souvent délicat de désigner un domaine d'activité par quelques mots dans lesquels toutes les communautés scientifiques concernées se reconnaissent spontanément.

Les membres du groupe se sont accordés à considérer qu'il conviendrait d'élargir le mot *diagnostic* à *surveillance et supervision*. Pour un intitulé en forme de *Diagnostic, Sûreté, Surveillance, Supervision*¹. Un groupe de travail du GDR MACS porte d'ailleurs le nom de *Sûreté, Surveillance, Supervision (S3)*.

D'autre part, de par les compétences de certains de ses membres ou leur implication dans d'autres comités (e.g. ANR), le CE n'a pas censuré *a priori* les problématiques relevant de la *sécurité*, informatique en particulier, d'autant qu'il ne dispose pas de la synthèse produite par le CE du même nom.

1. Même si, dans son acception la plus large, la sûreté de fonctionnement est liée à la capacité d'un système à résister aux défaillances matérielles, logicielles et humaines, et englobe tout ce qui concourt à la conception et la réalisation de systèmes et installations sûrs.

1.3 Contenu de la note

Les problèmes de sûreté, de surveillance et de supervision de systèmes complexes, qu'il s'agisse de systèmes et réseaux informatiques ou de structures, machines ou procédés instrumentés et informatisés, se sont vus accorder ces dernières années une reconnaissance croissante de leur importance, dans leurs enjeux tant scientifiques que socio-économiques.

Les divers comités, structures, programmes mis en place aux niveaux national, européen et international témoignent de l'importance accordée par la communauté scientifique à ce thème de recherche. L'objectif *Sécurité et sûreté des systèmes matériels et logiciels* mis en avant par le département ST2I est aussi dans cette lignée. Cette note ne contient donc pas de plaidoyer supplémentaire.

On dégage par contre ci-dessous deux types de verrous scientifiques. Tout d'abord les verrous et défis techniques mono-disciplinaires propres à chacune des trois communautés de la section 07 que sont l'informatique, l'automatique et le traitement du signal. Puis des verrous et défis pluridisciplinaires *intra* section 07. Enfin, et sans prétendre à l'exhaustivité, des défis en interaction nécessaire avec d'autres communautés, du département ST2I ou d'autres départements.

2 Verrous et défis mono-disciplinaires

2.1 Systèmes informatiques et réseaux

2.1.1 Systèmes et réseaux informatiques

- Conception de grands systèmes résistant à différents types de menaces.
- Redondance matérielle et logicielle; algorithmes répartis assurant la résilience aux fautes et garantissant des propriétés de sûreté; vérification de la résilience.
- Systèmes critiques adaptatifs et autonomes, y compris pour la reconfiguration.
- Étalonnage, évaluation et robustesse de la sûreté de fonctionnement.
- Grandes infrastructures inter-connectées et dépendantes (réseaux informatiques et électriques).
- Informatique diffuse: distinguer entre une panne et le mouvement d'un objet portable communicant, gestion de la confiance entre dispositifs mobiles.
- Sécurité informatique: technologies respectueuses de la vie privée, recueil de traces d'attaques à large échelle à des fins de validation.

2.1.2 Réseaux de télécommunications

- Dimension *réseau* dans le contexte de grande échelle (e.g. internet), de grande dynamique, de gestion embarquée et de généralisation des services en ligne.
- Supervision et contrôle de grands réseaux (qualité de service, trafic, alertes, décisions, corrections).
- Supervision de systèmes complexes distribués sans modèle global; modèles discrets et traitements statistiques; incertitudes et robustesse.
- Indicateurs quantitatifs fonctionnels et non fonctionnels (contrats et qualité de service).
- Répartition et distribution des mesures, traitements, contrôles et décisions.
- Systèmes embarqués (y compris aspects communicants) et autonomes.
- Placement dynamique de capteurs (sondes de flux, temps d'attente).

- Reconfiguration de réseaux, ressources et services; résilience vis-à-vis de défaillances de liens, commutateurs, ou sites.
- Convergence sécurité/supervision.

2.1.3 Informatique temps-réel

- Spécification fonctionnelle et conception d'architecture logicielle *prouvée*: méthodes et langages pour formaliser les exigences de sûreté, analyser l'impact d'événements sur la sûreté, spécifier des normes, et développer de manière sûre un système.
- Architectures techniques: conception d'architectures opérationnelles *faisables*; mécanismes adaptatifs pour l'interopérabilité; spécification de procédures de validation, certification, normalisation.
- Montée en puissance des *networked control systems*. Voir aussi 2.2.

2.2 Automatique

- Conception de systèmes automatisés sûrs garantissant des propriétés structurelles et fonctionnelles; analyses de détectabilité et diagnosticabilité des défauts et de reconfigurabilité du système, en vue de sa conception: instrumentation - placement optimal de capteurs et d'actionneurs - et redondances.
- Modèles plus complexes (non-linéaires, hybrides) et méthodes associées; intégration de modèles de types différents; coopération de méthodes de diagnostic.
- Diagnostic global par fusion d'informations locales; diagnostic distribué.
- Diagnostic actif (synthèse d'entrées facilitant le diagnostic).
- Diagnostic des systèmes dormants.
- Diagnostic prédictif, pronostic.
- Interaction entre commande et diagnostic.
- Tolérance aux pannes et reconfiguration.
- Incertitudes et robustesse; performances; qualité (garantie) de sûreté; testabilité.
- Implantation des algorithmes, "embarqué", temps-réel, distribution et répartition des traitements, synchronisation, communications inter-calculateurs. Voir aussi 2.1.3.
- Interfaces HM.

2.3 Signal et statistique

2.3.1 Signal

- Surveillance de systèmes complexes, modèle externe de l'observation basé sur des connaissances physiques partielles;
- Analyse et interprétation: détection, extraction, caractérisation de paramètres proches de la physique, décision.
- Observations complexes (multi-physiques, non stationnaires, multi-bandes, multi-composantes, différents types de perturbations).

2.3.2 Inférence et décision statistiques

- Intégration de contraintes (connaissances) dans les algorithmes de décision, en particulier de rejet de nuisances.
- Traitements basés sur des modèles physiques (d'état) paramétrés; inférence de paramètres de modèles continus dynamiques linéaires et non-linéaires.
- Robustesse aux variations autres que les défauts (incertitudes, environnement).
- Passage à l'échelle (modèles issus de la simulation multi-physique, données issues de grands réseaux de capteurs).
- Pronostic.

2.3.3 Apprentissage statistique et raisonnement incertain

- Classification de grandes masses de données, ou de grands ensembles de variables.
- Données imprécises, de faible volume, voire manquantes.
- Classes peu ou pas connues, ou non disjointes.
- Modèles d'incertitudes sur les données, liens avec inférence statistique, décision.
- Fusion de connaissances expertes et de modèles empiriques, de modèles boîte-noire, ou de modèles (physiques) de conception.

3 Verrous et défis multi/inter-disciplinaires

On décrit ici tout d'abord des problématiques communes à au moins deux des trois communautés de la section 07 que sont l'informatique, l'automatique et le traitement du signal, problématiques qui devaient bénéficier d'interactions plus fréquentes entre ces communautés.

Puis des défis pour lesquels l'interaction avec d'autres communautés scientifiques est nécessaire.

3.1 Problématiques communes info-auto-signal

- Modèles pour le diagnostic, la surveillance et la supervision; synthèse automatique de tels modèles (modèles boîte blanche, grise, noire; quels éléments extraire des modèles de conception, de simulation, de commande et d'analyse de sûreté?); intégration de modèles de types différents; diagnostic dynamique.
- Détectabilité et diagnosticabilité des défauts ou pannes.
- Placement statique ou dynamique des capteurs.
- Génération automatique d'indicateurs de pannes ou défauts.
- Diagnostic prédictif, pronostic.
- Tolérance aux pannes et reconfiguration.
- Robustesse aux variations autres que défauts, pannes ou endommagements, et aux incertitudes de tous ordres et niveaux (modèles, mesures, facteurs exogènes).
- Généricité, évolutivité et maintenabilité des méthodes et algorithmes de surveillance.
- Passage à l'échelle (systèmes, modèles, données).
- Distribution des traitements et du contrôle; contrôle dans un contexte réparti.
- Continuum spécification-conception-fabrication-déploiement-maintenance; standardisation des outils de diagnostic.
- Procédures et indicateurs pour vérification, validation et évaluation de performances.

3.2 Défis avec/pour d'autres communautés

Sont manifestes le besoin et la nécessité de croisement d'outils des disciplines de la section 07 (informatique, automatique, traitement du signal) avec ceux d'autres communautés scientifiques, du département ST2I (mécanique, génie civil, aéronautique, spatial, automobile, électrotechnique, génie des procédés) ou d'autres départements, en particulier MPPU (probabilités/statistiques, théorie de l'information, fiabilité).

- *Probabilités/statistiques:*
 - Modèles continus dynamiques non-linéaires et inférence statistique, pour surveillance de systèmes industriels complexes.
 - Modèles discrets dynamiques et inférence statistique, pour contrôle et supervision de systèmes répartis à grande échelle (internet).
- *Fiabilité:*
 - Diagnostic et fiabilité; intégration des modèles de sûreté de fonctionnement (AMDEC, ...) dans le cahier des charges de la surveillance et les algorithmes de diagnostic; surveillance en fonctionnement pour la maintenance conditionnelle.
 - Pronostic et évaluation de la sûreté de fonctionnement (fiabilité, disponibilité, sécurité-innocuité, sécurité-immunité).
- *Autres:*
 - Conception conjointe de normes de sécurité (e.g. anti-pollution) et d'algorithmes permettant de vérifier en fonctionnement que ces normes sont respectées.
 - Mise en cohérence des indicateurs de performances de systèmes ou procédés et des critères d'optimalité d'algorithmes de diagnostic.

4 Priorités d'action

- **Interactions à favoriser:**
 - *Info-auto-signal:*
 - * Modèles hybrides (discret/continu), modèles multi-physiques, approches multi-modèles.
 - * Robustesse aux variations autres que défauts, pannes ou endommagements, et aux incertitudes de tous ordres et niveaux (modèles, mesures, facteurs exogènes).
 - * Diagnostic global: gestion (ou fusion) optimale des indicateurs de pannes locaux.
 - * Concepts et algorithmes pour exploiter l'état distribué accessible par exemple *via* les capteurs laser, l'enregistrement synchronisé de mesures distribuées *via* les réseaux sans fil, et les modèles multi-physiques accessibles grâce aux grilles de calcul.
 - * Informatique temps-réel et implantation des algorithmes.
 - * Diagnostic à base de modèles et détection d'intrusions.
 - *Informatique et probabilités/statistiques:*
 - * Modèles hybrides (discret/continu), approches multi-modèles.
 - * Statistique et détection d'attaques de déni de services, intrusions...

- **Moyens incitatifs:**

- **Postes de chercheurs** affichés sur le thème *Sûreté, Sécurité, Diagnostic, Surveillance, Supervision*.

Nota: tous les acteurs concernés de la section 07 ne se reconnaissent pas dans la seule appellation *Sûreté de Fonctionnement* utilisée en 2007 pour le concours 07/03.

- **Allocations post-doctorales**, pour l'interaction avec des scientifiques possédant un profil scientifique complémentaire et en forte adéquation avec tout ou partie des domaines d'application étudiés par l'équipe d'accueil.
- **Autres accueils à durée déterminée** (délégations, détachements) dans le même but.

Annexe 1 - Composition du CE et compétences de ses membres

Composition

- Michèle Basseville (CNRS-IRISA), membre CS ACI S&I, et CE ARA SSIA et ANR SetIn, vice-présidente IFAC TC Safeprocess;
- Vincent Cocquempot (U.Lille 1-LAGIS), co-responsable GT S3, membre IFAC TC Safeprocess;
- Philippe Dague (U.Paris Sud-LRI);
- Thierry Denoeux (UTC-Heudiasyc);
- Sylviane Gentil (INPG-LAG), responsable de l'ex-RTP 20, membre IFAC TC Safeprocess;
- Claude Jard (ENS Cachan-IRISA), responsable de l'ex-RTP 19;
- Nadine Martin (CNRS-Gipsa-lab);
- Igor Nikiforov (UTT-Inst.C.Delaunay), membre IFAC TC Safeprocess;
- David Powell (CNRS-LAAS), membre CS ACI S&I, vice-président CE ARA SSIA et ANR SetIn;
- Françoise Simonot-Lion (INPL-LORIA), membre CS ACI S&I et CE ARA SSIA;
- Ali Zolghadri (U.Bordeaux 1-LAPS).

Compétences scientifiques principales

- **MB**: surveillance en fonctionnement de systèmes dynamiques; traitement statistique de signaux multi-dimensionnels sur la base de modèles physiques (d'état) paramétrés; détection, localisation et diagnostic de petites déviations; détectabilité; placement optimal de capteurs.
- **VC**: surveillance en fonctionnement de systèmes dynamiques; automatique; méthodes à base d'observateurs; tolérance aux pannes, reconfiguration.
- **PD**: diagnostic à base de modèles et supervision, raisonnement qualitatif, raisonnement sur les systèmes physiques et applications des techniques de l'I.A. aux sciences de l'ingénieur.
- **TD**: diagnostic; apprentissage statistique, classification, fusion d'informations, raisonnement incertain, I.A.
- **SG**: diagnostic, supervision et aide à l'opérateur; automatique et I.A., raisonnement causal, diagnostic distribué, applications industrielles.
- **CJ**: diagnostic et supervision; méthodes formelles pour la programmation des architectures parallèles et réparties, spécification, vérification et test dynamiques des logiciels répartis sur des réseaux de processeurs.
- **NM**: diagnostic, traitement de signaux mono-dimensionnels, modèles temporels non-stationnaires, modèles de chocs, modèles probabilistes temps-fréquence, analyse spectrale et temps-fréquence, détection en fréquence, segmentation temps-fréquence, classification et fusion dans des domaines transformées.
- **IN**: surveillance en fonctionnement; traitement statistique de signaux multi-dimensionnels; détection, localisation et diagnostic; détectabilité; optimalité des algorithmes.
- **DP**: sûreté de fonctionnement, tolérance aux fautes et autres menaces internes et externes, résilience informatique: conception, vérification, évaluation.
- **FSL**: sûreté de fonctionnement; temps-réel; évaluation de la sûreté de systèmes distribués temps-réel; déploiement sûr et optimal d'applications contraintes par le temps.
- **AZ**: diagnostic, surveillance à base de modèle, contrôle d'intégrité, commande tolérante aux fautes.

Domaines d'application principaux

- **MB**: surveillance vibratoire: génie civil (ponts), aéronautique et spatial (avions, lanceurs); automobile (diagnostic de dispositifs anti-pollution), énergie (turbo-alternateurs, turbines à gaz).
- **VC**: véhicules intelligents, moteurs électriques.
- **PD**: automobile (Numatec Automotive, PREDIT); réseaux de télécommunication; services web; spatial; circuits électriques.
- **TD**: transports ferroviaire et automobile; environnement.
- **SG**: énergie (nucléaire et électrique); pétrochimie.
- **CJ**: télécommunications et réseaux.
- **NM**: systèmes mécaniques à entraînement électrique, automobile (moteur et habitacle).
- **IN**: contrôle de l'intégrité des systèmes de navigation.
- **DP**: systèmes répartis mobiles, objets portables communicants, robotique.
- **FSL**: automobile (systèmes embarqués).
- **AZ**: aéronautique et spatial; systèmes environnementaux.

Annexe 2 - Tâches de fond envisagées

- Didactique intra-CE.
- Recueil des besoins des industriels en matière de recherche, validation et certification des algorithmes, et recensement de leurs outils et savoir-faire, au travers d'invitations, d'entretiens. Les appels à projets de pôles de compétitivité et les priorités des accords-cadre entre le CNRS et les grandes entreprises pouvant constituer une autre source d'informations utiles.