CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

RTP 21 : Sûreté de fonctionnement des systèmes informatiques complexes ouverts

Objectifs thématiques et Finalités

Le périmètre couvert par ce réseau concerne la **conception**, la **validation**, l'**exploitation** et la **maintenance** des systèmes informatiques destinés à des domaines d'application critiques :

- transports - santé - finances
- énergie - communication - commerce

L'accent est mis sur les contraintes mises en jeu sur le plan d'un ou plusieurs **attributs de la sûreté de fonctionnement** :

- fiabilité - disponibilité - sécurité
- intégrité - confidentialité - maintenabilité

La problématique couvre les différents défis liés à la **complexité** et à **l'ouverture** des architectures informatiques (envergure, répartition, mobilité, interaction, intégration, composition, évolution, autonomie,…) et inclut les aspects matériels et logiciels ainsi que leurs interdépendances. Parmi ces nouveaux défis, on peut citer :

- les problèmes posés par la sûreté de fonctionnement des **services *Internet* et *Web***,
- l'émergence de **l'autogestion des systèmes informatiques** afin d'assurer leur **adaptation de façon autonome** à différents facteurs d'évolution, soit de l'environnement, soit interne, y compris la défaillance de leurs composants.

Une autre dimension cruciale de la problématique est liée à la **dépendance croissante** des **grandes infrastructures civiles** (distribution des ressources, communication, santé, transport, etc.) **et militaires**, vis-à-vis de **l'infrastructure informatique** et de la **topologie des réseaux**.

Activités développées

L'obtention et le maintien à un niveau satisfaisant des attributs de la sûreté de fonctionnement sont entravés par les **défaillances** et leurs causes, c'est-à-dire les **fautes**. On distingue généralement les **fautes physiques** (résultant de dysfonctionnements matériels, soit internes, soit induits par l'environnement), les **fautes de conception** (résultant d'erreurs commises durant le développement des systèmes), les **fautes d'interaction** (résultant d'erreurs dans la conduite ou l'utilisation opérationnelle des systèmes, ou dans leur maintenance). Alors que les fautes physiques sont par nature accidentelles, les fautes de conception et d'interaction peuvent soit être accidentelles, soit résulter d'une décision consciente, sans ou avec intention nuisible ; dans ce dernier cas, il s'agit de **malveillances**.

Le programme des activités met l'accent sur les **systèmes complexes ouverts** en tenant compte de tout ou partie de ces différentes catégories de fautes. Il s'articule autour des trois moyens d'obtention et de validation de la sûreté de fonctionnement :

Tolérance aux fautes : *Comment fournir un service à même de remplir la fonction du système en dépit des fautes ?*

Thèmes : détection d'erreur, recouvrement d'erreur, empaquetage, masquage d'erreur, diversité,…

Élimination des fautes : *Comment réduire la présence (nombre, sévérité) des fautes ?*

Thèmes : spécifications formelles et vérification, test du matériel, test du logiciel, test de robustesse,…

Prévision des fautes : *Comment estimer la présence, la création et les conséquences des fautes ?*

Thèmes : évaluation analytique de la sûreté de fonctionnement (processus stochastiques), évaluation expérimentale, métrologie, étalonnage (*benchmarking*) de la sûreté de fonctionnement,…

Organismes / Entreprises partenaires

Caractéristiques

Date de lancement : **Novembre 2002**

Responsable : **Jean Arlat** <jean.arlat@laas.fr>

Site Web : **http://www.laas.fr/RTP21-SdF**

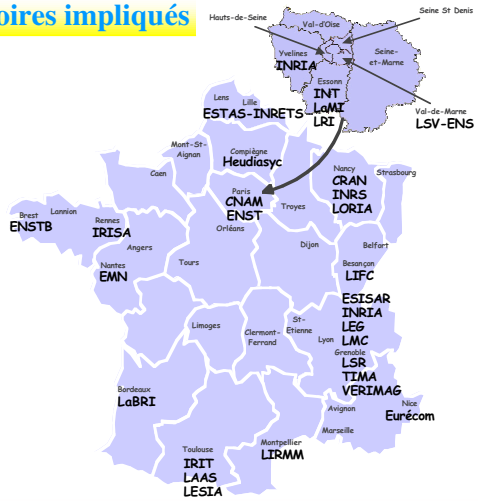
Mots clés

Sûreté de fonctionnement, systèmes ouverts, systèmes autonomes, systèmes mobiles, tolérance aux fautes, élimination des fautes, prévision des fautes, fautes physiques, fautes de conception, erreurs humaines, malveillances.

Comité de pilotage

D.STIC : Luis **Fariñas del Cerro**
Membres : Jean **Arlat** (LAAS), Michel **Banâtre** (IRISA), Frédéric **Cuppens** (ENSTB), Marie-Claude **Gaudel** (LRI), Bernard **Courtois** (TIMA), Christian **Landrault** (LIRMM), Jean-Claude **Laprie** (LAAS), Bernard **Pavard** (IRIT)

Laboratoires impliqués



Actions spécifiques et équipes-projets associées

AS23 - Techniques avancées de test des systèmes complexes
Animateurs : Richard Castanet <castanet@labri.u-bordeaux.fr> et Hélène Waeselynck <helene.waeselynck@laas.fr>
AS75 - Méthodes et outils logiciels pour le développement de systèmes d'exploitation
Animateur : Gilles Muller <gilles.muller@emn.fr>
AS111 - Techniques de spécification et de test pour les composants logiciels de communication
Animatrice : Ana Rosa Cavalli <ana.cavalli@int-evry.fr>
AS161 - Testabilité des systèmes informatiques
Animatrice : Lydie du Bousquet <lydie.du-bousquet@imag.fr>
Réseau d'Ingénierie de la Sûreté de fonctionnement (RIS)
Animateur : Jean Arlat (http://www.ris.prd.fr)

Fait(s) marquant(s)

Le rapprochement effectif avec le **Réseau d'ingénierie de la Sûreté de fonctionnement (RIS)**, qui regroupe déjà autour du **LAAS-CNRS**, **Airbus**, **EADS Astrium**, **Technicatome** et **Thales**, constitue une avancée significative dans le but de mettre en œuvre des coopérations avec des partenaires industriels majeurs sensibilisés à la problématique scientifique et technologique couverte par le réseau.

RIS AIRBUS EADS ASTRIUM PSA PEUGEOT CITROËN SNCF TECHNICATOME THALES