JOURNEES
SYSTEMES & LOGICIELS CRITIQUES
le 14/11/2000

Merlin Gerin
Modicon
Square D
Telemecanique

Mise en Œuvre des techniques synchrones pour des applications industrielles

Schneider Electric

Mise en œuvre des techniques synchrones pour des applications industrielles de sûreté

- **Bref historique**
- **De quoi dispose, aujourd'hui, l'industriel**
  - pour quelles applications
  - avec quelles perspectives d'utilisations
- **Tendances**
- **Synthèse**
  - quelques résultats et convictions …
  - prochaines étapes

Préalable : Applications industrielles de Sûreté ?????

- Sûreté : recouvre des enjeux de Sécurité et/ou disponibilité et/ou maintenabilité

- Applications industrielles : systèmes de commande et/ou protections de process industriels.
  - Programmés / programmables
  - process continus / manufacturiers

Pour ces applications, 2 types de domaines d ’application:
•domaines mûrs, réglementés (transport,nucléaire,chimie …)
•domaines émergents (cogénération,salles blanches,manufacturier, …)

Bref Historique (1)

« La Sûreté c'est
l 'affaire du Hard »

« Plus on programme,
Plus y 'a d 'bugs »

Ségrégation fonction
Protection/Commande

« n-version logiciel »
(Boeing, NASA)

Premiers systèmes numériques
critiques ,
(Nucléaire, Ferroviaire, chimie,
militaire)

LE CRITIQUE est SPECIFIQUE

Bref Historique (1)

« Plus on programme,
Plus y ’a d ’bugs »

Ségrégation fonction
Protection/Commande

Nelles architectures (NTIC)
Demandes de disponibilité et Sécurité
Recherche intégration systèmes informations
et systèmes de sûreté (MES)

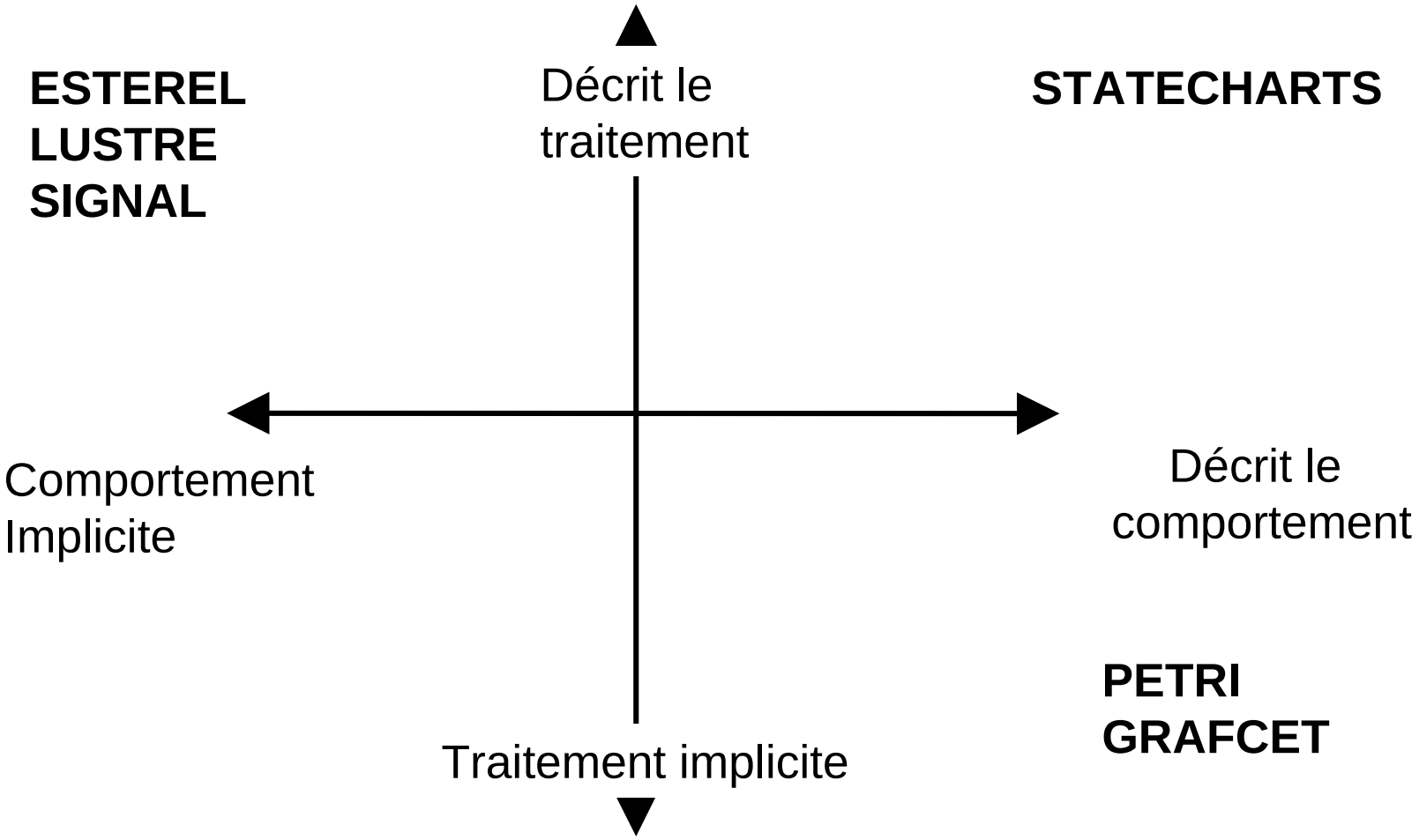
Le STANDARD est CRITIQUE

Premiers systèmes numériques
critiques ,
(Nucléaire, Ferroviaire, chimie,
militaire

Représentation d ’un automatisme
De quoi dispose l ’industriel ?

- Ce qui est **STANDARD :**
  - Nécessité de représenter:
    - le **comportement temporel** du système
    - les **traitements réalisés**.
  - Proposer des représentations indépendantes de l ’implémentation matérielles (mais implémentables facilement & sûrement)
- Ce qui est **SPECIFIQUE :**
  - La nature de l ’enjeu de sûreté :
    - non respect d ’un délai
    - traitement erroné
    - Défaut de Traçabilité
    - Arrêt du système
    - ….

Représentation d ’un automatisme
De quoi dispose l ’industriel (exples…)



Représentation d ’un automatisme
Positionnement de l ’approche Synchrone

ESTEREL
LUSTRE
SIGNAL

Décrit le traitement

STATECHARTS

<u>Spécificité</u> de ces formalismes synchrones:

Comport Implicite

- **Utilisé pour exprimer: les propriétés de sûreté et les fonctions de l ’automate, les conditions de validité des propriétés (assertions).**
- **Applications implémentables sur un Hardware assurant explicitement le comportement synchrone de l ’ensemble**

exple : automates de Protection,

(Perspective d ’) utilisation de l ’approche synchrone Génération d ’Automates exécutables

- **Automatisme Temps Réel Critique**
  - Décrire l ’application
  - Générer du code
  - Disposer d ’un modèle exécutable (graphe d ’états fini)
  - Utiliser ce modèle pour tester ou vérifier des propriétés.

  - Exple Programmation Automate Industriel Standard

Perspective d ’utilisation de l ’approche synchrone Description de Systèmes Automatisés

- **Décrire l ’environnement de l ’automatisme** (noté « process* »)
  - Le comportement attendu du process
  - Les hypothèses de fonctionnement du process
  - En déduire les spécifications de l ’automatisme

  - Exple. Spécification Automatisme et Architecture Tolérantes aux fautes.

*Le process = machines, hommes, flux de matières & d ’ énergie

Perspective d ’utilisation de l ’approche synchrone Evaluation de la Sûreté

- **Evaluer le niveau de sûreté**
  - En intégrant les caractéristiques de sûreté des composants.
    - déterministes pour l ’application,
    - probabilistes pour son environnement
  - En construisant un modèle de sûreté de l ’ensemble
  - Utiliser ce modèle pour évaluer les gains de sûreté et de coût d’ exploitation.

  - Exple. Evaluation d ’un Risk Reduction Factor selon CEI 61508.

Quelques Tendances pour les applications industrielles de sûreté

- **Nouvelle expression de besoins**
  - Productivité et traçabilité deviennent des valeurs d ’usages critiques.
  - Des normes stimulantes couvrent de nombreux domaines(CEI61508)
  - Accéder au procédé par le langage du procédé, idem pour la programmation des Automatismes Programmables Industriels (CEI1131).
- **La banalisation des solutions distribuées**
  - Menaces et opportunités générés par l ’utilisation des réseaux et les architectures distribuées.
- **La fin de la rupture déterministe/probabiliste pour l ’analyse de Sûreté des systèmes.**
  - Des outils nouveaux à développer.

Synthèse et perspectives pour AUTOFOR, Approche Synchrone

- Nouvelle expression de besoins
  - Productivité et traçabilité
  - Des normes (CEI61508)
  - Accéder au procédé
  - Automatismes Programmables Industriels
- La banalisation des solutions distribuées
  - Menaces et opportunités réseaux
  - architectures distribuées.
- analyse de Sûreté des systèmes.
  - Des outils nouveaux à développer.

→ Certification ou accréditation

→ *Matrice Causes.Effets formelles*

→ **Outils de conception Automates synchrones**

→ **Approche Mixte Déterministe/probabiliste**

Synthèse et perspectives pour AUTOFOR, Autres aspects liés à la Sûreté

- Nouvelle expression de besoins
  - Productivité et traçabilité
  - Des normes (CEI61508)
  - Accéder au procédé
  - Automatismes Programmables Industriels

→ Commande prédictive
Certification ou accréditation (GAMP)

- La banalisation des solutions distribuées
  - Menaces et opportunités réseaux
  - architectures distribuées.
- analyse de Sûreté des systèmes.
  - Des outils nouveaux à développer.

→ **Sûreté ATM, ETHernet,**
→ *Spécification de réseaux de sûreté à partir de standards*
Règles de conceptions d'applications réparties critiques