UBO

lab-sticc.univ-brest.fr/~babau/

Introduction au développement des systèmes embarqués temps-réel

Jean-Philippe Babau

Département Informatique, UFR Sciences, UBO
Laboratoire Lab-STICC

jean-philippe.babau@univ-brest.fr

UBO

jean-philippe.babau@univ-brest.fr

UBO

Une machine à coudre et à broder

Actionneur : contrôle de lâaiguille (déplacement et vitesse), pied de biche

Communication par clé USB

IHM : écran tactile

capteurs: épaisseur de tissu, fin de bobine, fil cassé

Utilisateurs non informaticiens (personnes âgées, é), cout non négligeable, é

jean-philippe.babau@univ-brest.fr

UBO

La voiture de demainé

http://www.weshow.com/fr/p/9009/prototype_voiture_nissan_pivo_2

Confort
Sécurité
Aide à la conduite
Aide aux déplacements
Aide aux manî uvres
Gestion de lâénergie, é .

Confiance dans lâaide à la conduite, sureté de fonctionnement, développement en série, intégration de fonctions et technologies diverses, é

jean-philippe.babau@univ-brest.fr

UBO

Le domaine spatial

- De 1 à 30 logiciels embarqués par satellite
- Durée de développement : 6 mois à 5 ans
- Durée de vie du système : quelques minutes (lanceurs) , de 1 à 15-20 ans (satellites ou sondes)

- Complexité et fonctionnalités très variables en fonction de la mission et des contraintes du système spatial
- 20.000 à 200.000 lignes de code
  - C, ADA, ou Assembleur (émergence de JAVA)
- Majoritairement modifiables en vol

jean-philippe.babau@univ-brest.fr

UBO

De plus en plus dôinformatique embarquée

- Transport
  - Automobile
    - Plus de 50 ECU (Electonic Control Unit)
    - 15 000 paramètres contrôlés toutes les ms
  - Avionique
    - Airbus A300 (1974) : 25 ko
    - Airbus A380 (2005) : 64 Mo
  - Spatial
    - Spot1 (1980) : 48 ko
    - Mars Express (2003) : 1,2 Mo
- Systèmes personnels
  - Systèmes portables communicants (smartphone, gps, cartes à puceé)
  - Image et son (Appareil photo numériques, é)
- Capteurs
  - Médical, industriel, identifiants, suivi
- Drones

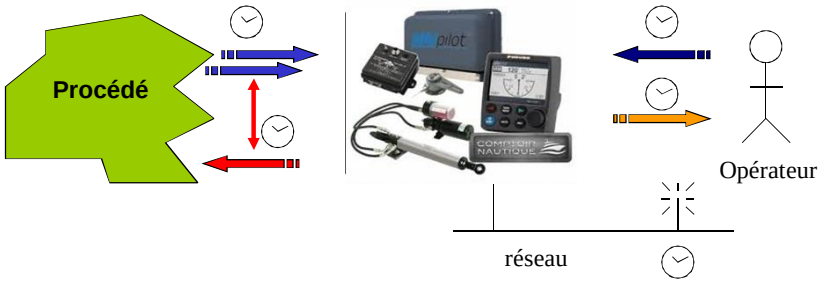
jean-philippe.babau@univ-brest.fr

Les domaines dôapplication

- Périphériques
  - imprimantes, modems, claviers, souris
- Domotique
  - HiFi, électroménager, confort
  - contrôle à distance, régulation
- Systèmes automatisés
  - contrôleurs industriels
  - système de mesure
- Systèmes personnels
  - carte à puce, objets connectés
  - téléphones mobiles, smartphones
- Systèmes de transport
  - véhicule : automobile, avion, train, fusée, robot
- **Systèmes dôacquisition et de surveillance et autonomes**
  - **Drones**
- Systèmes à réalité virtuelle
  - simulateurs de conduite
  - télé-opération

jean-philippe.babau@univ-brest.fr

Les systèmes embarqués temps-réel communicants

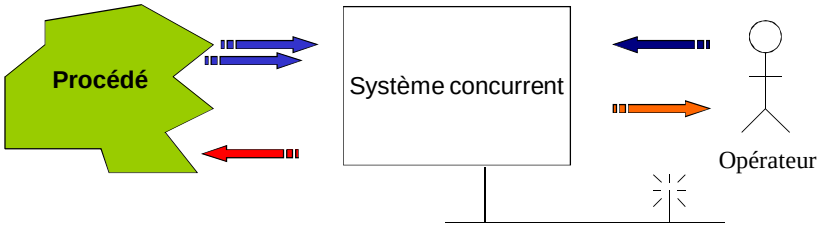


Contraintes temporelles

- acquisition, sorties, échéances

jean-philippe.babau@univ-brest.fr

Les systèmes embarqués temps-réel communicants



Contraintes temporelles

- acquisition, sorties, échéances

Contraintes d'embarquabilité

- Place limitée, contraintes physiques
- Contraintes d'énergie

Contraintes de coût

jean-philippe.babau@univ-brest.fr

Spécificités des systèmes embarqués temps-réel

- Fortes interaction avec le procédé
  - Évolution du procédé indépendante du contrôle
    - -> Contraintes temporelles
  - **Utilisation de capteurs et d'actionneurs**
    - **Suivi et contrôle**
- IHM limité ou spécifique
  - Parfois pas d'IHM (systèmes enfouis)
  - Modèles d'interactions avec l'utilisateur spécifique
    - Impact sur le développement et les tests
    - Impact sur le fonctionnement
  - Politique d'initialisation, de maintenance
    - Chargement du code, activation, reboot, installation/désinstallation
- Contraintes de coût, d'espace, de consommation
  - Matériel spécifique
  - Taille mémoire limitée
  - Processeurs limités

jean-philippe.babau@univ-brest.fr

UBO

Système en prise avec lœenvironnement : modélisation de lœenvironnement

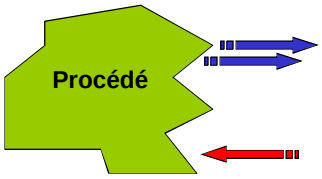
- Prise de décision
  - En fonction dœune vue partielle de lœenvironnement
  - Interprétation de données de bas-niveau
- Avion
  - " pas de rétro-propulsion sur un avion en l'air "
  - "Avion au sol" = " roue sorties et roues qui roulent "
  - Piste verglacée é
- Voiture
  - " pas de verrouillage lorsque le véhicule est occupé "
  - " véhiculé occupée " = " clé électronique proche "
  - Au garage, la clé doit être loin é
- Véhicule en mode « test »
  - Volant immobile, roues arrières bloquées, capot ouvert
  - Mode test : le système anti-pollution est activé é .
  - Mais est-il possible de capturer exactement le mode « test » é

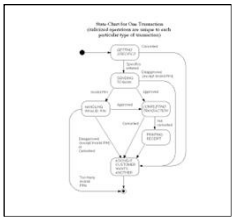
jean-philippe.babau@univ-brest.fr

UBO

Modes de fonctionnement

- Intégration dœaspects discrets
  - Un état du système -> un mode de fonctionnement
    - Lœétat est défini selon lœétat de lœenvironnement et du système
    - Dépendant des retours des capteurs
  - Un mode de fonctionnement : application dœune loi de commande
    - Comportement du système lié à un état
    - Actions sur le système via les actionneurs





jean-philippe.babau@univ-brest.fr

UBO

Des systèmes dédiés

- L'architecture matérielle et logicielle est adaptée aux besoins spécifiques de l'application
  - Importance de l'implémentation
- Le matériel
  - Peu coûteux, fiable, prédictible
  - Dimensionné pour l'application et son utilisation
    - Capacités de calcul et de stockage
    - Consommation
- Systèmes d'exploitation
  - Limités aux fonctions utilisées par l'application
    - Exécutifs, noyaux
  - Prédictible (temps de réponse borné pour les appels système)
  - « Royaltie-free »
  - Traçable

jean-philippe.babau@univ-brest.fr

UBO

De plus en plus d'interactions

- Suivi à distance
  - Gestion de flotte (GPS), gestion d'équipements
  - Réseaux de capteurs
- Diagnostic
  - Interrogation locale ou distante
- Contrôle à distance
- Complexité et personnalisation des fonctions
  - Interaction utilisateurs
- Être « connecté » et « Web attitude »
  - e-mail, SMS
  - Alertes (météo, route, é)
  - Consultation d'informations
  - Mise à jour de logiciels, é

jean-philippe.babau@univ-brest.fr

UBO

Les bogues célèbres

- Avion F16
  - déclaré « sur le dos » au passage à l'équateur
  - erreur de signe
- Métro de San-Francisco
  - trains fantômes
  - http://en.wikipedia.org/wiki/History_of_the_Bay_Area_Rapid_Transit
- Lancement 1ère navette américaine
  - faux départ
  - erreur de synchronisation entre les deux ordinateurs

jean-philippe.babau@univ-brest.fr

UBO

Les bogues célèbres

- Ariane V
  - l'exception logicielle est due à une conversion d'un flottant sur 64 bits en entier sur 16 bits (dépassement de capacité et code Ada)
    - pas de protection sur cette exception
  - l'erreur s'est produite dans une partie du logiciel utilisée uniquement avant le décollage
  - la valeur concernée était nettement plus élevée que la valeur escomptée
    - la trajectoire d'Ariane 5 diffère de celle d'Ariane 4
- Analyse
  - Les événements internes qui ont conduit a l'accident ont été reproduits par simulation
  - Erreur de codage : pas de protection sur exception non prévues
  - Erreur de spécification : domaine d'entrée des variables d'Ariane 4 au lieu d'Ariane5
    - Modélisation du procédé
  - Erreur de tests / mise au point : pas d'émulation des conditions de vol d'Ariane5
    - Pas de test d'intégration, désormais obligatoire
  - Erreur de conception
    - Une exception n'est pas une erreur grave
    - Un code inutile doit être arrêté ou confiné
  - Erreur de processus

→ Maîtrise du développement

jean-philippe.babau@univ-brest.fr

UBO

Un besoin fort de fiabilité

- Automobile
  - Image de marque (régulateur de vitesse)
  - Coût d'un retour de séries
  - Aspect psychologique du système enfoui
- Objets personnels
  - Rejet car « ne marche jamais »
  - Reset = perte de données !
  - Doit être accessible à tous, sans opération de configuration
  - Partagé par toute la famille
- QoS
  - image numérisée = image « parfaite »
  - Retard trop important = panne du point de vue de l'utilisateur
  - Consommation énergétique maîtrisée
- Durée de vie du système
  - Voiture : 10 ans, train : 20 ans
- Contractualisation
  - Vendeur du produit final : « la marque »
  - Intégrateur, sous-traitant

jean-philippe.babau@univ-brest.fr

UBO

Certification

- Certifier le processus (e.g. DO-178)
  - On fait le maximum pour s'assurer que le logiciel est correct
  - Ne prouve par le logiciel
- Certifier le produit (e.g. DEF-STAN 00-56)
  - Au travers de "safety cases"
  - On démontre l'absence de vulnérabilités
- Autorités de certification
  - Indépendant
- Contraintes sur le développement et les technologies

jean-philippe.babau@univ-brest.fr

UBO

Certification

- Plusieurs standard
  - Avionique civil ED 12B / DO 178
  - Automobile ISO 2626-2
  - Medical IEC 62 304
- Logiciel pour avionique civil
  - DO-178C ï level A (Catastrophic)
    - Failures will likely cause multiple casualties, or crash the airplane
  - DO-178C ï level B (Hazardous/Severe)
    - Failure will largely reduce the plane safety margin, or cause casualties to people other than the flight crew
  - DO-178C ï level C (Major)
    - Failure will significantly reduce the plane safety margin, or cause distress to people other than the flight crew
  - DO-178C ï level D (Minor)
    - Failure will slightly reduce the plane safety or discomfort to passengers of cabin crew
  - DO-178C ï Level E (No Effect)
    - Failure will have no effect for safety

jean-philippe.babau@univ-brest.fr

UBO

Exemple dôopérations de certification

- Spécification
  - Expliciter ce que le système doit faire
- Code
  - Doit être vérifiable
  - Productivité
    - 1 ligne de code par jour par développeur
    - 1 ligne de code pour 10 lignes de test
- Vérification
  - Relecture manuelle de code
  - Test de tous les chemins dôexécution
- Processus
  - Traçabilité des exigences

jean-philippe.babau@univ-brest.fr

UBO

Prédictibilité

- **Temps** : correction du contrôle
  - Maitrise des temps dôexécution des opérations
  - Analyse des temps de réponse (validation temps réel)
- **Espace** : maitrise du coût, de la place
  - Contrôle de lôoccupation mémoire (pas dôoverflow !)
- **Energie** : un défi majeur
  - Gestion des des accès mémoire
  - Gestion de la vitesse du processeur
  - Gestion de lôutilisation des composants électroniques

jean-philippe.babau@univ-brest.fr

UBO

Le temps-réel

- Arriver à lôheure ≠ aller vite
- Temps réel dur
  - une échéance stricte est à respecter

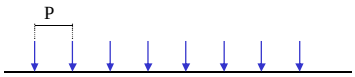
  «un résultat juste mais hors-délai est un résultat faux»
- Temps réel mou ou relâché
  - tolérance de dépassement dôéchéance
    - pourcentage de non respect
    - taux de dépassement
- Quelques unités de temps
  - milliseconde : systèmes radar
  - seconde : système de visualisation
  - minute : chaîne de fabrication
  - heure : contrôle de réaction chimique

jean-philippe.babau@univ-brest.fr

UBO

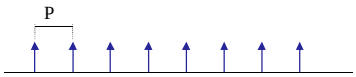
Propriétés temporelles

entrée périodique



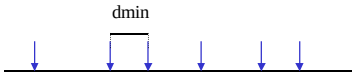
scrutation périodique, alarme programmable

sortie périodique



stimulation régulière

entrée sporadique



Intervalle minimum entre deux événements (dmin)

entrée apériodique

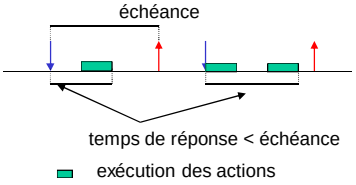
Pas d'information temporelle
Événement rare
Situation d'urgence ou événement anodin

jean-philippe.babau@univ-brest.fr

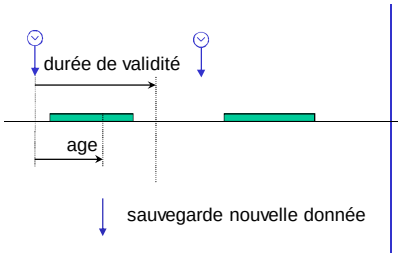
UBO

Contraintes temporelles

- Réaction aux événements d'entrée
  - Contrainte sur le temps de réponse maximal



- Age d'une donnée
  - Durée de validité
    - Contrainte sur l'âge maximal acceptable
  - Datation
    - Systèmes distribués



jean-philippe.babau@univ-brest.fr

UBO

Validation temporelle : respect des échéances

- Mise en place d'une politique d'ordonnancement
  - Séquence d'exécution statique
  - Ordonnancement à priorité (RM, EDF, é)
- Analyse des pire temps d'exécution
  - Pire cas (Worst Case Execution Time ou WCET)
  - Temps moyen
  - ≠ du temps de réponse
- Analyse d'ordonnançabilité
  - Analyse RMA, analyse holistique, preuve, é

jean-philippe.babau@univ-brest.fr

UBO

Définition de l'heure

- Jour solaire
  - 2 passages successifs au zénith
  - 1 jour : 24h de 60 min de 60s ()
- Seconde
  - 1 / 86 400 ème de jour
  - 9 192 631 770 périodes de la radiation correspondant à la transition entre deux niveaux hyperfins de l'état fondamental de l'atome de Césium 133
- TAI (Temps Atomique International)
  - nombre moyen (4 horloges) de tops horloge atomique à base de césium 133 depuis le 1er janvier 1958 divisé par 9 192 631 770 (1 seconde)
  - Échelle de temps linéaire et stable : mesuré par 250 horloges atomiques
- UTC (temps universel coordonné)
  - Heure officielle
  - Ajustement avec le TAI si écart (TAI - temps solaire moyen) > 900 ms
    - 1 seconde est sautée
    - En moyenne une seconde par an
    - 31 décembre 2005 : 1 seconde de plus
    - UTC - TAI = -33 (1er janvier 2006)

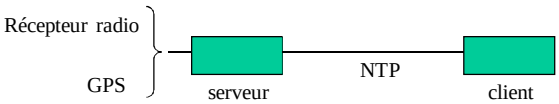
2005 Décembre 31	23h 59m 59s
2005 Décembre 31	23h 59m 60s
2006 Janvier 1	0h 0m 00s

jean-philippe.babau@univ-brest.fr

UBO

Gestion de l'heure

- UTC
  - UTC (OP) : erreur maximale de 100 nano secondes
  - Récupérable sur la fréquence porteuse de France Inter
- GPS
  - Liée à l'heure UTC(USNO)
  - Pas d'ajustement avec le TAI: actuellement 19 secondes d'avance
  - Erreur satellite
    - dispersion de 30 ns
    - erreur / UTC : 100 ns heure
    - TAI
- Exemple de synchronisation via le protocole NTP (Net Time Protocol)
  - Évaluation de la charge réseau
  - Évaluation du temps de transmission de l'heure



jean-philippe.babau@univ-brest.fr

UBO

Déroulement d'un projet (vue du développeur informatique)

1. Spécifications des besoins
2. Choix d'une architecture matérielle : processeur (puissance, famille), carte

- Puissance de calcul nécessaire
- Besoins en communication et entrées/sorties

- Choix a priori dans 75% des cas
  - énergie, prix
  - besoins spécifiques
  - Domaine d'application
  - culture d'entreprise
  - coût du changement (formation, prise en main)

jean-philippe.babau@univ-brest.fr

Déroulement dôun projet (vue du développeur informatique)

3 Choisir un langage de programmation et un OS (RTOS), si nécessaire

- Plus de 70 SE disponibles
- Disponibilité vis-à-vis de la plateforme
  - Processeur supporté ?
  - Drivers pour la carte à développer ?
- Coût
  - Plateforme de développement, intégration de services, royalties
- Domaine
  - Ferroviaire : QNX
- Documentation et fiabilité des fournisseurs sur le long terme

Déroulement dôun projet (vue du développeur informatique)

4 Choix de lôutil de développement (compilateur, suite de développement, debugger, simulateur)


- Dépend généralement de lôOS et du langage
- Mise en place dôun simulateur de lôenvironnement
  - Tests et mise au point
- Utilisation dôun IDE

UBO

Développement par étapes

- Spécification
  - Expression des besoins fonctionnels et contraintes matérielles
  - Description du procédé à contrôler et de son environnement
  - Contraintes de QoS (qualité de service) : temps-réel, coût, taille, consommation
- Conception
  - Découpage matériel / logiciel
  - Architecture matérielle
    - Cartes, composants
    - Traitements et protocoles à spécifier
  - Architecture logicielle
    - OS, environnement de développement
    - Décomposition modulaire
- Mise en œuvre et codage
  - Choix d'un environnement de développement et d'un langage (C)
- Validation
  - Choix de techniques et d'outils d'analyse
  - Respect de normes

jean-philippe.babau@univ-brest.fr

UBO

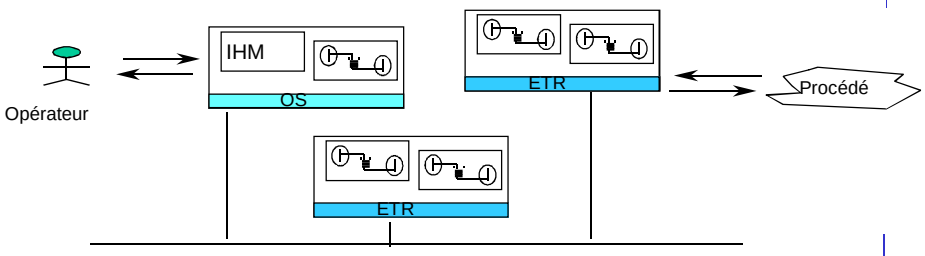
Méthodes, technologies et langages

- Langages de spécification et de modélisation
  - Spécification textuelle
  - SART : analyse fonctionnelle descendante
  - Matlab, StateMate : automates et lois de contrôle
    - Automatique discrete et continue
  - UML (paradigme objet peu répandu), profils UML (MARTE)
  - Méthodes et langages formels (B)
- Langages de conception
  - UML, codesign, ADL et Composants
  - multitâche
  - approches synchrones (Esterel, Signal, Lustre)
- Ingénierie dirigée par les modèles (IDM)
  - Model Driven Engineering (MDE)
  - Modèles , métamodèles (concepts), transformation de modèles

jean-philippe.babau@univ-brest.fr

UBO

Systèmes complexes



- Système hétérogène
  - temps réel / non temps réel
  - critiques / non critiques
- Système communicants
- Système évolutif / adaptatif
  - ajout / suppression / modification
  - modes d'urgence
  - garantie de QoS
  - adaptation à l'environnement

jean-philippe.babau@univ-brest.fr

UBO

Les défis actuels

- Maîtrise des systèmes complexes
- Portabilité des applications
  - Standardisation des plateformes d'exécution et de communication
- Intégration des nouveauté technologiques
  - Legacy code
- Réutilisation
  - Savoir-faire : composants métier
  - Composants à l'exécution
- Partage de services, sûr de fonctionnement
- Sécurité

jean-philippe.babau@univ-brest.fr

UBO

Objectifs du cours

- Appréhender le domaine des systèmes embarqués temps réel
- Gérer des entrées / sorties sur un « *exemple jouet* »
  - Brique NXT Lego ®
- Gérer le contrôle distant d'un système

jean-philippe.babau@univ-brest.fr