INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

FORMATION CONTINUE CT2 IR_SEMESTRE 9

Infos pratiques

Lieu(x)

Toulouse

Analyse prescriptive (AP)

ECTS
4 crédits

Volume horaire

Présentation

Objectifs

Ce cours adresse des modèles de traitement efficace des données rencontrées dans des problèmes industriels à caractère combinatoire. Les modèles sont basés sur l'inférence logique et l'optimisation : les problèmes de satisfaction de contraintes (CSP), les modèles à base de clauses disjonctives booléennes (SAT) et la programmation linéaire en nombres entiers (PLNE).
Pour la partie CSP, les étudiants doivent connaître les principales techniques de propagation et stratégies de résolution et se familiariser à travers les travaux pratiques avec des outils de programmation intégrant des algorithmes de propagation de contraintes et des stratégies générales de (ex d'outil : CPLEX).
Dans la partie modélisation SAT, les étudiants appliquent différentes techniques et heuristiques de propagation de contraintes sur des modèles SAT. Différents problèmes combinatoires classiques (coloration, affectation de ressources, ordonnancement) servent de cas pratiques pour s'entraîner sur l'encodage SAT.
Pour la partie PLNE, les étudiants doivent modéliser des problèmes industriels sous forme de programme linéaire en nombre entiers, et les résoudre via des algorithmes de branchement ou des méthodes de décomposition en utilisant des outils de programmation (CPLEX).

Pré-requis nécéssaires

Algorithmics & programming (I2MIIF11, I2MIIF21).
Fundamentals in Computer Science (I4IRIF11),
Intelligent Systems (I4IRSD11)

Infos pratiques

Lieu(x)

Toulouse

Software-defined communication infrastructure (SDCI)

ECTS
4 crédits

Volume horaire

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et capable d'expliquer :

- les concepts attenant à la virtualisation de fonctions de réseau (au sens NFV)
- les concepts attenant à la programmation des réseaux (au sens SDN)
- le modèle de l'autonomic computing défini (entre autres) par IBM
- les points de vue des acteurs du monde réel impliqués dans un projet d'ampleur (développeur d'application, opérateur middleware, opérateur réseau)

L'étudiant devra être capable de :
- utiliser un émulateur de réseau SDN (ContainterNET)
- utiliser un contrôleur SDN (Ryu)
- utiliser un MANO NFV standardisé (SON-EMU)
- développer une VNF standardisée
- architecturer et mettre en œuvre des solutions tirant partie des concepts de virtualisation de fonctions de réseau et de réseaux programmables, dans le contexte de la réalisation d¿une SDCI
- appliquer et mettre en œuvre le modèle de l¿autonomie computing à une problématique de gestion de QoS dans une SDCI

Pré-requis nécéssaires

Interconnexion de réseaux - TCP/IP (4IR)

Conception orientés objets - UML (4IR)

Programmation orientée objets - JAVA (4IR)

Concepts et techniques liés à la virtualisation (5SDBD)

Architectures orientés services (5SDBD)

Infos pratiques

Lieu(x)

Toulouse

Cloud Computing

ECTS
6 crédits

Volume horaire
69h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :
· Dans le domaine réseaux et télécommunication : conception et mise en oeuvre d'une infrastructure matérielle et de communication pour la virtualisation répondant aux contraintes de performance des solutions cloud.
· Dans le domaine des plateformes : conception et mise en oeuvre des plateformes pour l'intégration et la provision de services pour le développement d'applications métier et d'entreprise dans un environnement cloud.
· Dans le domaine de l'ingénierie logicielle: conception et mise en oeuvre de logiciels applicatifs intégrant les contraintes et les propriétés nécessaires pour leurs déploiements dans un environnement cloud.
L'étudiant devra être capable de :
Développer et mettre en place des solutions autonomiques afin d'assurer les besoins d'adaptation aux niveaux logiciel, plateforme et infrastructure du cloud computing.

Pré-requis nécéssaires

Programmation JAVA, Conception Orientée Objets (UML 2.0), Administration et Programmation réseau (TCP/IP), Service-Oriented Architectures (SOA)

Infos pratiques

Lieu(x)

Toulouse

Ingénierie des modèles

ECTS
6 crédits

Volume horaire

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :
L'approche IDM, la construction et l'exploitation des langues de modélisation et des techniques associées.
L'étudiant devra être capable de :
Sélectionner les modèles et les moyens technologiques appropriés à mettre en oeuvre.
Concevoir et réaliser techniquement une solution «IDM» sur un cas d'étude simple.

Pré-requis nécéssaires

Modélisation comportementale : Réseaux de Petri, Automates communicants
Programmation objet

Infos pratiques

Lieu(x)

Toulouse

Modélisation, évaluation et optimisation des réseaux et protocoles

ECTS
4 crédits

Volume horaire
78h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :
1. Les principes de mise en oeuvre, de gestion et d'évolution d'un réseau d'opérateur. Les notions de métrologie et d'analyse des caractéristiques du trafic.
2. Les problématiques de base de la planification des réseaux et quelques algorithmes d'optimisation du routage, de dimensionnement ou de conception de topologies des réseaux.
3. Les principaux concepts et formalismes permettant la description et la vérification formelle de protocoles.
L'étudiant devra être capable de :
1. Mesurer l'état d'un réseau, analyser les différents problémes et en déduire des correctifs.
2. Appliquer des algorithmes simples relatifs à : l'optimisation de la résilience des réseaux, au routage optimal, à l'optimisation des poids OSPF et du placement des LSPs et à la synthèse des réseaux.
3. Mettre en oeuvre les techniques de description et de vérification formelle pour réaliser une modélisation formelle de protocoles.

Pré-requis nécéssaires

Théorie des graphes, programmation linéaire et non-linéaire, processus stochastiques de base, protocoles de routage IP, TCP/IP, MPLS, logique propositionnelle, Automates et Langages.

Infos pratiques

Lieu(x)

Toulouse

Commande avancée et supervision

ECTS
6 crédits

Volume horaire

Toulouse

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :
Les principaux concepts et techniques de la commande des systèmes non linéaires et de la commande optimale.
Les signaux aléatoires et systèmes linéaires (Filtre de Kalman continu et discret).
L'étudiant devra être capable de :
Comprendre et mettre en oeuvre la commande des systèmes complexes : commande non linéaire et commande optimale.
Programmer un filtre de Kalman

Pré-requis nécéssaires

Systèmes à événements discrets - Systèmes linéaires continus : modélisation et commande - Signaux aléatoires - Analyse des systèmes non linéaires - Systèmes multivariables.

Infos pratiques

Lieu(x)

Projet physique PTP_ISS

ECTS
4 crédits

Volume horaire

Infos pratiques

Lieu(x)

Toulouse

Robotique de service

ECTS
6 crédits

Volume horaire
50h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra pouvoir expliquer devant un auditoire académique ou industriel ce qu'est la robotique de service et en quoi elle diffère de la robotique industrielle ; il aura également été initié aux bases de la robotique humanoïde et à la difficulté de contrôler un robot bipède. Ses connaissances techniques incluront les bases de la robotique des systèmes articulés : modèles cinématiques direct et inverse, modélisation dynamique du robot, génération de mouvements et stabilité de déplacement d'un robot bipède.

L'étudiant devra être en mesure de modéliser un robot articulé, de décrire ses composants technologiques et d'analyser le fonctionnement d'un robot de service dans son environnement domestique ou professionnel.

Pré-requis nécéssaires

Calcul matriciel, Automatique linéaire

Lieu(x)

Toulouse

Infos pratiques

Méthodes d'ingénierie

ECTS
4 crédits

Volume horaire
42h

Présentation

Objectifs

Présenter les grands principes de l'ingénierie système et de l'ingénierie logicielle. : concepts, méthodes et outils pour la définition et la maîtrise du processus de développement d¿un système embarqué critique

L'étudiant devra être capable de :
- appliquer ces connaissances génériques aux systèmes informatiques embarqués d'expliquer les différentes approches et choisir le bon type d'approche pour une application particulière.

Infos pratiques

Lieu(x)

Toulouse

Architecture informatique pour l'embarqué

ECTS
4 crédits

Volume horaire

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principes et spécificités des réseaux utilisés dans les systèmes embarqués des secteurs de l'automobile, l'avionique et des objets connectés,
- les spécificités des systèmes d'exploitation et leurs principaux services (ordonnancement, mémoire, privilèges, etc.) pour les systèmes embarqués,
- les avantages et inconvénients des différentes architectures informatiques utilisées pour les systèmes embarqués,
- les éléments impactant les performances (calcul, consommation d'énergie, etc.) d¿une architecture informatique et les méthodes pour les optimiser.

L'étudiant devra être capable de :
- choisir une technologie réseau répondant aux besoins d'un système embarqué,
- mettre en place le réseau support d¿un système embarqué,
- déployer un système d¿exploitation sur une architecture embarquée,
- développer un driver au sein d¿un système d¿exploitation,
- comparer deux architectures informatiques embarquées en terme de performances,
- choisir une architecture informatique adaptée aux besoins d'une application

Pré-requis nécéssaires

Programmation C, architecture des ordinateurs, réseau, système d'exploitation

Infos pratiques

Lieu(x)

Toulouse

Relations humaines et professionnelles, Ethique

ECTS
6 crédits

Volume horaire
78h

Présentation

Lieu(x)

Toulouse

Objectifs

L¿étudiant devra être capable de :
¿ Analyser des situations de groupe avec des concepts issus de la psychologie sociale
¿ Identifier les dimensions éthiques de ces situations et prendre position
¿ Repérer et comprendre des informations liées aux RH
¿ Analyser une situation de management d¿équipe en référence à un cadre théorique
¿ Formuler et argumenter des solutions managériales
¿ Agir dans un milieu naturel : analyser, décider, agir ; mettre en œuvre la sécurité, utiliser du matériel spécifique, découvrir un site.
¿ Respecter et s'intégrer dans un environnement différent de ses habitudes
¿ S'engager avec cohérence dans le projet d'activités
¿ Prendre part activement au collectif
¿ Valider son projet professionnel, construire une stratégie et s¿entraîner pour trouver un emploi

Pré-requis nécéssaires

Aucun

Infos pratiques

Projet interdisciplinaire

ECTS
5 crédits

Volume horaire

Présentation

Objectifs

A la fin de ce module, l'étudiant devra être capable de :
- mettre en œuvre et d'appliquer à son travail une démarche de gestion et de management agile selon la méthode agile scrum pour réaliser un produit,
- de mobiliser et d'articuler un ensemble de compétences techniques interdisciplinaires afin de réaliser un système embarqué critique,
- de rechercher de manière autonome et de porter un regard critique sur des solutions techniques pour lesquelles il ne dispose pas de connaissances au préalable afin de répondre à des exigences propres aux systèmes embarqués critiques,
- de réaliser un produit déployé sur une architecture hétérogène et communicante embarquée en garantissant des propriétés de performance,
- de définir les besoins, les exigences et l'architecture lors du développement d'un produit
- de communiquer dans un contexte interdisciplinaire et de travailler conjointement avec des acteurs aux compétences hétérogènes,
- d'adapter la rédaction et la présentation de résultats scientifiques en fonction du public visé (client, décideur, évaluateur, grand public) et à travers des supports variés (présentation, site web, rapport, synthèse, poster),
- de s'exprimer en anglais dans une langue correcte et dans un style concis et précis en respectant les conventions de genre à l'écrit comme à l'oral

Infos pratiques

Lieu(x)

Toulouse

Sûreté de fonctionnement

ECTS
5 crédits

Volume horaire
68h

Toulouse

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

Les concepts de base de la sûreté de fonctionnement et les grandes méthodes et techniques d'obtention et de validation de la sûreté de fonctionnement d'un système.

L'étudiant devra être capable de :
- appliquer ces connaissances génériques aux systèmes technologiques électroniques et logiciels.
- d'expliquer les différentes approches et choisir le bon type d'approche pour une application particulière.

Pré-requis nécéssaires

Systèmes à événements discrets, Logique Propositionnelle

Infos pratiques

Lieu(x)

Bases de la sécurité

ECTS
5 crédits

Volume horaire
77h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer :

- Les principaux concepts des systèmes d'exploitation, des réseaux TCP/IP, de la programmation en langage C et en assembleur. Il s'agit ici d'une mise a niveau de tous ces domaines scientifiques, pour être sûr que les étudiants aient les bases fondamentales pour suivre l'ensemble de la formation
- Les principaux concepts de la sûreté de fonctionnement
- Les principaux concepts de la cryptographie

L'étudiant devra être capable de :

- décrire le fonctionnement des éléments importants d'un système d'information.
- décrire les principes fondamentaux de la construction des protocoles réseaux, d¿analyser des traces réseaux et de comprendre l¿encapsulation des flux
- utiliser les techniques de base de la programmation avec le langage C et assembleur. Il sera capable de concevoir des programmes en utilisant ces techniques.
- différencier les domaines de la sécurité (sécurity et safety) et utiliser correctement le vocabulaire associé
- distinguer les différents outils cryptographiques, comprendre ce qu'ils peuvent apporter à la sécurité et ce qu'ils ne peuvent pas
- trouver les standards internationaux de la cryptographie, comprendre leur contenu et mettre en place une utilisation d'un outil cryptographique respectant les standards ;
- réaliser des déploiements à l'aide d'outils réels de haut niveau (PKI, VPN, IPSec) ou de bas niveau (openssl) en choisissant les algorithmes, les niveaux de sécurité, les modes de fonctionnement de façon raisonnée

Pré-requis nécéssaires

Infos pratiques

Lieu(x)

Toulouse

Sécurité du logiciel

ECTS
4 crédits

Volume horaire
47h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les différents types de vulnérabilités logicielles que l'on rencontre fréquemment, en particulier dans les programmes écrits en langage C ;
- Les contre-mesures usuelles de protections mémoires permettant de se protéger de ces différents types de vulnérabilités ;
- La théorie liée aux vers et virus, en particulier les algorithmes utilisés par les vers et virus pour infecter les systèmes informatique et se répandre, les protections contre ces malveillances et le fonctionnement des antivirus et des méthodes qu'ils emploient ;
- Les bonnes pratiques pour développer du logiciel de façon sécurisée.
- Les méthodes formelles permettant le développement de logiciel sécurisés

L'étudiant devra être capable de :

- Développer des logiciels en tenant compte des risques liés aux vulnérabilités logicielles ;
- Employer les méthodes formelles pour la détection de vulnérabilités logicielles ;
- Apprécier les enjeux de la protection virale, décrire les différents types d¿infection informatique, analyser les techniques virales et antivirales et réagir en cas d'infection

Pré-requis nécéssaires

De bonnes compétences en programmation en langage C et assembleur ;
- Un minimum de connaissances sur le fonctionnement des OS ;
- Des bases en algèbre et sur l¿utilisation de la théorie des automates

Infos pratiques

Lieu(x)

Toulouse

Sécurité système et matérielle, rétro conception

ECTS
4 crédits

Volume horaire
54h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux mécanismes de protection qui existent aujourd'hui dans les noyaux de systèmes d'exploitation ;
- Les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées ;
- Le fonctionnement des principaux composants matériels pour la sécurité tels que les hyperviseur et les IOMMU ;
- L'intérêt des dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset ;
- Le fonctionnement des attaques matériels et physiques principales qui ciblent les systèmes informatiques ;
- La rétro-conception de logiciels (reverse engineering) tout en étant capable d'expliquer la la chaîne de compilation avec les modèles utilisés par les compilateurs pour générer le code machine ;
- Les stratégies pour rendre la rétro-conception de logiciels plus difficile à réaliser.

L'étudiant devra être capable de :

- Identifier les composants logiciels les plus adaptés pour protéger un système d'exploitation vis-à-vis des attaques logicielles ;
- Identifier les menaces provenant des couches basses et les vecteurs d'attaques à considérer dans un système ;
- D'obtenir une vue globale des échanges entre le composants matériels d'un système pour identifier les composants critiques et déterminer les contre-mesures a intégrer dans le système d'exploitation ;
- Identifier les menaces sur les composants physiques d'un système ;
- De réaliser une rétro-conception de maliciels pour en comprendre le fonctionnement voire créer des signatures
pour les détecter

Pré-requis nécéssaires

De bonnes compétences en programmation en langage C et assembleur ;

- Un minimum de connaissances sur le fonctionnement des OS ;
- Des bases en algèbre et sur l¿utilisation de la théorie des automates.

Infos pratiques

Lieu(x)

Toulouse

Sécurité des réseaux et de leurs protocoles

ECTS
3 crédits

Volume horaire
40h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts):

- Les principaux concepts de la sécurité des réseaux filaires, les principales attaques ciblant ces réseaux et les mécanismes de protection associés
- Les principaux concepts de la sécurité des réseaux non filaires (Wifi, GSM, GPRS, LTE, UMTS)
- Les principales faiblesses des protocoles réseaux fragiles et comment les sécuriser.

L'étudiant devra être capable de :

- Reconnaître et mettre en place les attaques réseau classiques dans le cadre d'un test d'intrusion ; identifier et mettre en place les mécanismes de protection contre ces attaques ; utiliser et mettre en place des infrastructures de défense
- Choisir une solution de sécurité adaptée pour un pointenti d'accès Wifi ; réaliser un test d'intrusion sur un point d'accès Wifi
- Différentier les objectifs de sécurité dans les différents réseaux cellulaires ; décrire les mécanismes d'authentification et d'échange de clés et comparer les apports en sécurité de chacun ; décrire les attaques possibles dans le cadre de chaque technologie ; reconnaître les éléments architecturaux de la sécurité dans un réseau d'opérateurs
- Reconnaître les protocoles fragiles mis en place habituellement dans un réseau informatique ; sécuriser ces protocoles fragiles par l'utilisation de tunnels pour les applications lorsque ceci est nécessaire ; utiliser SSH et les fonctions associées (transferts de fichiers, proxys, etc.) ; décrire les bonnes pratiques pour la définition d'un protocole sécurisé

Pré-requis nécéssaires

De bonnes compétences dans l'informatique en général et dans la compréhension des protocoles réseaux qui régissent l'Internet (TCP/IP, protocoles de routage a minima) . En particulier, toute la terminologie doit être connue et lesprincipes fondamentaux de la cryptographie doivent être acquis

Infos pratiques

Lieu(x)

Toulouse

Architectures réseaux sécurisées

ECTS
4 crédits

Volume horaire
54h

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les principaux concepts associés à la conception et l'implémentation d'architectures réseaux sécurisées
- Les outils et techniques principaux permettant cette sécurisation et leur utilisation en fonction des différents contextes ainsi que des objectifs correspondants.
- Les vulnérabilités inhérentes aux architectures système et réseau et les grandes techniques d'intrusion ;
- Le fonctionnement des principales vulnérabilités du web.

L'étudiant devra être capable de :

- Distinguer les différents types de pare-feux ainsi que leurs capacités et limitations
- Définir et auditer une architecture de filtrage adaptée à un réseau informatique donné
- Choisir pour un tunnel IPsec les protocoles à utiliser, les modes de fonctionnement et un plan de routage adapté pour les passerelles associées
- Mettre en place et auditer un tel tunnel Ipsec
- Mettre en place ou auditer un VPN créé sur du IPsec manuellement ou en utilisant les outils tout-en-un du marché
- Mettre en place et auditer un système de détection d'intrusion éventuellement distribué avec des options de prévention
- Faire le design complet d'une architecture de sécurité pour un réseau complexe

- Identifier les limites et avantages de différentes solutions de détection d'intrusion ;
- Positionner les sondes de détection d'intrusion de manière efficace ;
- Analyse les évènements collectés par les sondes et corréler ces évènements pour identifier une menace réelle.
- Identifier les vulnérabilités dans les architectures web et proposer des solutions pour réaliser une protection efficace

Pré-requis nécéssaires

Une bonne connaissance des architectures Web, de la cryptographie et des réseaux.

Infos pratiques

Lieu(x)

Toulouse

Sécurité des systèmes embarqués critiques

ECTS
5 crédits

Volume horaire
31h

Toulouse

Présentation

Objectifs

A la fin de ce module, l'étudiant devra avoir compris et pourra expliquer (principaux concepts) :

- Les différentes techniques utilisées de nos jours pour sécuriser les communications sol/air dans le contexte satellitaire ;
- Les problématiques liées aux différents types de mission et les standards utilisés ;
- Les moyens pour la sécurisation des transmissions par étalement de spectre (TRANSSEC) ;
- Les principes du réseau informatique pour la gestion du trafic aérien (ATM) et les problématiques de sécurité associées ;
- Les principes et les problématiques de la gestion de la sécurité dans le contexte de la DGAC.

L'étudiant devra être capable de :
- Effectuer des choix pertinents vis-à-vis de la sécurité pour architecturer les moyens de communication sol/air ;
- Réaliser une analyse en boite noire d'un système embarqué critique

Infos pratiques

Lieu(x)

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

SHSJ

ECTS
5 crédits

Volume horaire
42h

Infos pratiques

Lieu(x)

Toulouse

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

UE commune M2 RT

ECTS
9 crédits

Volume horaire
45h

Infos pratiques

Lieu(x)

Toulouse