



Máster en Ingeniería de Telecomunicación 60944 - Sistemas electrónicos para control de acceso y seguridad

Guía docente para el curso 2015 - 2016

Curso: , Semestre: , Créditos: 5.0

Información básica

Profesores

- Carlos Miguel Orrite Uruñuela corrite@unizar.es

Recomendaciones para cursar esta asignatura

Teniendo en cuenta las titulaciones que dan acceso al master, para cursar esta asignatura no es necesario ningún conocimiento previo adicional al adquirido en las titulaciones de grado. Se requieren conocimientos básicos de MATLAB.

Actividades y fechas clave de la asignatura

Entre las principales actividades previstas se encuentran la exposición de los contenidos teóricos, el planteamiento y resolución de casos, la realización de prácticas de laboratorio y la realización de trabajos tutorados relacionados con los contenidos de la asignatura.

La asignatura se imparte en cuatrimestre de otoño; las fechas de inicio y fin de las clases, así como las fechas de las pruebas de evaluación global, serán fijadas por la Escuela de Ingeniería y Arquitectura (<https://eina.unizar.es/>) y serán publicadas en la página web del máster (www.unizar.es/mie/). Las fechas de las sesiones prácticas serán igualmente publicadas en la página web del máster antes del inicio de la asignatura. Las fechas de entrega y seguimiento de los trabajos prácticos tutorizados se darán a conocer con suficiente antelación en clase y en la página web de la asignatura alojada en la plataforma docente que se indicará.

A título orientativo:

- **Período de clases:** primer cuatrimestre (Otoño).
- **Clases teoría y problemas-casos:** cada semana hay programadas 2 horas de clases en el aula.
- **Sesiones prácticas:** el estudiante realizará 5 sesiones prácticas de 3 horas de laboratorio y entregará trabajos asociados a las mismas.
- **Entrega de trabajos de las prácticas:** se informará adecuadamente en clase de las fechas y condiciones de entrega.
- **Examen:** habrá un examen de 1ª convocatoria y otro de 2ª convocatoria en las fechas concretas que indique el centro.

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

- 1:**
R1. Conocer las distintas tecnologías existentes en la identificación automática de identidad, distinguiendo cual es la tecnología idónea según el campo de aplicación.
- 2:**
R2. Evaluar distintos algoritmos de verificación, proporcionando la tasa de falsa aceptación y falso rechazo.
- 3:**
R3. Saber diseñar y evaluar sistemas electrónicos para su aplicación en el control de acceso y/o identificación automática de personas y mercancías.
- 4:**
R4. Ser capaz de proseguir el aprendizaje de forma continuada y autónoma.

Introducción

Breve presentación de la asignatura

El objetivo de esta asignatura es formar al alumno en las técnicas y sistemas actuales en el control automático de acceso a espacios físicos y/o electrónicos. El control de acceso de personas y mercancías es una disciplina de enorme relevancia hoy en día, merced sobretudo, a los avances en los dispositivos electrónicos de localización de bajo coste y a las técnicas biométricas de reconocimiento de personas. En esta asignatura se contemplan tanto los dispositivos electrónicos existentes como los algoritmos y/o procesos necesarios para el reconocimiento del objeto o persona bajo inspección.

Se trata de una asignatura optativa del bloque de Electrónica para ambientes inteligentes, que consta de 6 créditos ECTS. Teniendo en cuenta las titulaciones que dan acceso al master, no es necesario ningún conocimiento previo adicional al adquirido en las titulaciones de grado para poder cursar esta materia. Se requieren conocimientos básicos de MATLAB.

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

La asignatura se estructura en tres grandes bloques.

El primero de ellos, es una breve introducción al reconocimiento de patrones, con especial énfasis en la presentación de métodos estadísticos. Los algoritmos presentados se dividen en dos grandes grupos: aquellos que requieren una supervisión humana, es decir, el etiquetado de un conjunto de entrenamiento y aquellos otros que no es necesario, utilizando técnicas de aprendizaje no supervisadas.

En una segunda parte se describen las diferentes tecnologías existentes para la identificación automática: códigos de barras, reconocimiento óptico de caracteres, RFID, tarjetas inteligentes y sistemas biométricos. Esta última tecnología se describe en profundidad presentando los dispositivos y algoritmos más representativos del reconocimiento de personas mediante técnicas biométricas. Se introducen distintas modalidades biométricas basadas en: reconocimiento facial, huella dactilar, iris, retina, morfología de la mano, firma, etc.

Por último, se presentan diversas aplicaciones de sistemas de seguridad y control de acceso como por ejemplo: control de acceso biométrico de personas, video-vigilancia, monitorización de tráfico, etc.

Contexto y sentido de la asignatura en la titulación

En el contexto de los entornos inteligentes, el control de acceso es uno de los aspectos claves a tratar. Podemos considerar un entorno inteligente como un espacio físico al que se desea tener acceso, pero también puede ser un entorno informático, como por ejemplo el acceso a Internet, o un terminal bancario. En ambos casos es muy importante la seguridad del usuario

mediante la identificación de la persona (o mercancía) que solicita el acceso.

Por otra parte, hoy en día existe una especial preocupación en todos los aspectos relacionados con la seguridad ciudadana. Seguridad para prevenir riesgos a personas o infraestructuras, pero también para proporcionar una mayor información y calidad de servicio a todo tipo de ciudadanos.

Esta asignatura aborda diversos campos de aplicación para el desarrollo en entornos inteligentes, que van desde el micro sistema formado por un terminal y un usuario, hasta entornos más complejos como una ciudad o una infraestructura vial.

Al superar la asignatura, el estudiante será más competente para...

1: COMPETENCIAS BÁSICAS

CB6: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

CB7: Los estudiantes sabrán aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

2: COMPETENCIAS GENERALES

CG11: Capacidad para saber comunicar (de forma oral y escrita) las conclusiones- y los conocimientos y razones últimas que las sustentan- a públicos especializados y no especializados de un modo claro y sin ambigüedades.

CG12: Poseer habilidades para el aprendizaje continuado, autodirigido y autónomo.

3: COMPETENCIAS ESPECÍFICAS

CE14: Capacidad para desarrollar instrumentación electrónica, así como transductores, actuadores y sensores.

CE15: Capacidad para la integración de tecnologías y sistemas propios de la Ingeniería de Telecomunicación, con carácter generalista, y en contextos más amplios y multidisciplinares como por ejemplo en bioingeniería, conversión fotovoltaica, nanotecnología, telemedicina.

CE17: Realización, presentación y defensa, una vez obtenidos todos los créditos del plan de estudios, de un ejercicio original realizado individualmente ante un tribunal universitario, consistente en un proyecto integral de Ingeniería de Telecomunicación de naturaleza profesional en el que se sinteticen las competencias adquiridas en las enseñanzas.

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

Las técnicas de control electrónico de acceso presentan numerosos campos de aplicación en el desarrollo de Entornos Inteligentes. Considerando que este es un campo que presenta una demanda cada vez mayor, debido a la complejidad de la nueva sociedad, la formación adquirida en esta asignatura permitirá al alumno situarse en una posición idónea para potenciar su carrera profesional, bien en el campo de la investigación, como en el del desarrollo de aplicaciones comerciales.

Evaluación

Actividades de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluación

1: E1: Prueba escrita presencial (30%).

Examen tipo test con penalización por fallos, con puntuación de 0 a 10 puntos. La calificación representará el **30%** de la nota final. Habrá un examen en cada convocatoria oficial.

2: E2: Evaluación de las prácticas de laboratorio (30%).

Las prácticas de laboratorio se valorarán tanto en la propia sesión de laboratorio como a partir del guion de la práctica que se deberá entregar. La calificación de las prácticas será de 0 a 10 puntos y representará el **30%** de la nota final.

Las prácticas son fundamentales para superar la asignatura. El estudiante que no realice una práctica en la sesión programada deberá realizarla por su cuenta y entregar el guion en la fecha correspondiente a la convocatoria oficial; el profesor ese día le realizará una prueba oral para comprobar que realmente dicho estudiante ha realizado la práctica y valorar su desempeño.

3: E3: Valoración de los trabajos dirigidos (40%).

Se realizará un trabajo de control de acceso y/o seguridad en el que el estudiante deberá mostrar el grado de adquisición de las competencias correspondientes a la asignatura. En la evaluación de los trabajos se tendrá en cuenta tanto la memoria presentada, como la idoneidad y originalidad de la solución propuesta. La **calificación global** de esta actividad será de 0 a 10 puntos, valorándose los siguientes conceptos: dificultad y desarrollo (hasta 3 puntos), resultados y simulaciones (hasta 3 puntos), calidad de la memoria (hasta 2 puntos), exposición oral y defensa (hasta 2 puntos). Todo ello supondrá un **40%** de la calificación del estudiante en la asignatura.

Se realizarán preferiblemente en grupos de dos estudiantes (aunque pueden hacerse de forma individual) en alguna de las 2 modalidades siguientes:

Tipo A. Consiste en la aplicación de algunas técnicas presentadas en la asignatura, utilizando el entorno de desarrollo de MATLAB, a la resolución de algún problema concreto. La temática puede ser propuesta por el propio alumno.

Tipo B. Implementación electrónica de alguna técnica de control de acceso, siendo el alumno quien la propone en función de la disponibilidad de material que él mismo disponga.

4: Prueba global (100%).

En aplicación de la normativa de evaluación de la Universidad de Zaragoza, en las convocatorias oficiales de examen, a realizar en las fechas y horarios determinados por la Escuela, el estudiante podrá alcanzar el 100% de la calificación, resultado de la contribución del examen tipo test (30%), trabajo de asignatura (40%) y prácticas (30%). Cada una de estas contribuciones se guardará hasta la última convocatoria del curso.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

El proceso de enseñanza se desarrollará en tres niveles principales: clases de teoría, problemas y laboratorio, con creciente

participación del estudiante.

- En las clases de teoría se expondrán las bases teóricas del diseño magnético en aplicaciones de potencia.
- En las clases de problemas se desarrollarán problemas y diseños representativos con la participación de los estudiantes.
- Se realizarán prácticas de laboratorio en grupos reducidos en las que se harán montajes con elementos magnéticos y simulaciones por elementos finitos.

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1: Actividades presenciales (1.8 ECTS, 45 horas)

A01 Clase magistral (20 horas)

En esta actividad se expondrán los contenidos fundamentales de la materia y se realizarán un conjunto de problemas representativos. Esta actividad se realizará en el aula de forma presencial. Los materiales que se expondrán en las clases magistrales estarán a disposición de los alumnos a través del Anillo Digital Docente.

Programa de la asignatura y calendario de sesiones presenciales

- T1: Revisión de técnicas de reconocimiento y clasificación.
- T2: Introducción a los sistemas electrónicos para el control de acceso
- T3: Sistemas biométricos de identificación
- T4: Sistemas de video vigilancia y seguridad
- T5: Análisis del comportamiento humano

A02 Resolución de problemas y casos (ECTS, 10 horas)

En esta actividad se resolverá un conjunto de problemas representativos. Esta actividad se realizará en el aula de forma presencial. Los materiales que se expondrán en las clases magistrales estarán a disposición de los alumnos a través del Anillo Digital Docente

A03 Prácticas de laboratorio (ECTS, 15 horas)

Las prácticas están estructuradas en 5 sesiones de 3 horas cada una. Los enunciados de las prácticas estarán a disposición de los alumnos a en el Anillo Digital Docente.

Programa de las sesiones de prácticas

Como se ha comentado anteriormente, las prácticas se estructuran en 5 sesiones de 3 horas

2: Actividades no presenciales (3.2 ECTS, 80 horas)

A06 Trabajos docentes (25 horas)

En esta actividad se realizarán los trabajos relacionados con las prácticas. Los trabajos se realizarán de forma individual o en grupos de dos personas como máximo.

A07 Estudio (53 horas)

Esta actividad comprende tanto el estudio personal encaminado a lograr el seguimiento adecuado de la asignatura, la realización de las prácticas, la preparación del examen y las tutorías.

A08 Pruebas de evaluación (2 horas)

La actividad de evaluación comprende la realización del examen y la revisión de las calificaciones del examen y de las prácticas.

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

Las clases magistrales y de problemas y las sesiones de prácticas en el laboratorio se imparten según horario establecido por el centro (horarios disponibles en su página web). El resto de actividades se planificará en función del número de alumnos y se dará a conocer con la suficiente antelación.

Referencias bibliográficas de la bibliografía recomendada

- Bishop, Christopher M.. Pattern recognition and machine learning / Christopher M. Bishop New York : Springer, cop. 2006
- Jain, Anil K.. Biometrics: Personal Identification in Networked Society / Anil K. Jain and others Kluwer Academic Publishers. 2002