Moduli di dottorato (anno 2018-19)

MODULO A

Titolo: *Tecniche di Analisi per la Valutazione di Performance e la Diagnosi di Guasti di Impianti Industriali*
Docente: Francesco Castellani
Contatto docenti*:* francesco.castellani@unipg.it
Periodo delle lezioni: gennaio - febbraio 2019 (gli studenti interessati sono pregati di prendere contatto con il docente per concordare il calendario delle lezioni).

ABSTRACT. I moderni impianti industriali sono ormai dotati di sofisticati sistemi di controllo e monitoraggio (SCADA - System Control and Data Acquisition). Tali sistemi sono in grado di generare una enorme mole di dati spesso scarsamente utilizzata a livello industriale. L'obiettivo del corso è quello di dimostrare le potenzialità dell'analisi dei dati di esercizio sia per migliorare l'affidabilità e la produttività degli impianti che per sviluppare nuovi interessanti filoni di ricerca applicata che coinvolge tutte le discipline tipiche dell'ingegneria industriale e dell'informazione.

PROGRAMMA

- **Modulo 1** - Architettura dei sistemi SCADA e logiche di accesso ai dati - 4 ore
- **Modulo 2** - Tecniche di filtraggio e analisi statistica dei dati grezzi - 3 ore
- **Modulo 3** - Metriche per la definizione delle performance di esercizio - 3 ore
- **Modulo 4** - Analisi dati a supporto della manutenzione preventiva - 2 ore
- **Modulo 5** - Tecniche innovative per la diagnosi precoce dei guasti - 4 ore
- **Modulo 6** - Analisi di casi reali - esercitazione pratica - 4 ore

MODULO B

Titolo: *Analisi Dinamica dei Sistemi Mediante l'Uso di Codici Multicorpo e l'Analisi in Frequenza*
Docente: Filippo Cianetti
Contatto docenti*:* filippo.cianetti@unipg.it
Periodo delle lezioni: gennaio-giugno 2019 (gli studenti interessati sono pregati di prendere contatto con il docente per concordare il calendario delle lezioni).

ABSTRACT. L'insegnamento si propone di descrivere e far apprendere le tecniche di modellazione e simulazione dinamica multicorpo nel dominio del tempo e della frequenza mediante l'adozione di un codice commerciale di riferimento e di affrontare l'analisi strutturale dei componenti che caratterizzano il sistema analizzato mediante l'analisi in frequenza dei risultati abbinando a questo approccio la modellazione "flessibile" di tipo modale dei componenti stessi.

PROGRAMMA

- **Modellazione dinamica.** Modellazione multicorpo.
- **Modellazione modale di componenti flessibili**. La sintesi modale di Craig e Bampton. Esempi di ottenimento del modello modale di un componente mediante l'adozione di un software FEM commerciale.
- **Analisi dinamica.** Simulazione dinamica multicorpo. Analisi dinamica transiente. Esportazione di rappresentazioni State Space MiMo del sistema. Tecniche di ottenimento di risposte espresse in termini di PSD a partire da ingressi sempre espressi in termini di PSD.
- **Durability**. Metodi di conteggio dei cicli nel dominio del tempo e della frequenza. Ricostruzione di spettri di carico a partire da funzioni PSD nel dominio della frequenza. Formula di Rayleigh e Dirlik.

TESTI CONSIGLIATI:

- Manualistica Matlab, ADAMS ed ANSYS (disponibile on line)
- Preumont A., "Twelve Lectures on Structural Dynamics", Universite Libre de Bruxelles (diponibile on line)

MODULO C

Titolo: *Bitcoin's Blockchain, Distributed Ledger Technologies and Smart Contracts*
Docente: Luca Grilli
Contatto docente*:* luca.grilli@unipg.it
Periodo delle lezioni: giugno-luglio 2019 (gli studenti interessati sono pregati di prendere contatto con il docente per concordare il calendario delle lezioni).

ABSTRACT. Bitcoin is the first and the most famous cryptocurrency. It was introduced in 2008 by an anonymous person, or by some unknown organization, under the pseudonym of Satoshi Nakamoto. Since then the Bitcoin's price is grown significantly, making this technology a very popular and controversial phenomenon. Anyway, regardless of the Bitcoin digital currency's future, the work by Nakamoto has already gained a fundamental result: the introduction of the blockchain technology.

A blockchain is a logical data structure consisting of a chain (or list) of immutable transaction blocks. It is physically memorized across multiple networked data stores - the blockchain network - each of which can be owned and handled by autonomous organizations with conflicting interests. Blockchains make strong use of cryptography and of (distributed) trustless consensus mechanisms to guarantee irreversibility, authenticity and integrity of their content (over time). In particular, suitably decentralized approaches are adopted to validate and authenticate transactions, without the necessity of intermediaries. In a typical scenario, each node in the network maintains its own copy of all transactions, and the nodes cooperate to verify the validity of the latest non-verified transactions through a specific consensus strategy. Each of such transactions is announced to all nodes within the network to be validated and grouped into transaction blocks marked with a timestamp.

To extend the idea behind the Bitcoin's Blockchain to wider application domains, and thus not only to develop other types of cryptocurrencies, more flexible and extensible data structures have been proposed, known as Distributed Ledger Technologies (DLT). A DLT may organize data even into non-linear structures such as trees or DAGs (i.e., Directed Acyclic Graphs) and may provide a programmable environment to execute smart contracts, which are essentially computer programs that actually control real-world assets, without the need for a third party that controls the release of such assets.

DLTs might become a fundamental infrastructure for reducing costs and improving reliability, security, transparency, and accessibility of many public services involving the legal registration of documents; such as notarial deed, business, cadastre, and protocol registers. Also, DLTs may play a relevant role in supply chain management and logistics, allowing for a more efficient, reliable and transparent tracking of data, and significantly reducing costs.

PROGRAMMA

1. **Fundamental Concepts of Information Security**
   - Confidentiality, Integrity, Availability
   - Assurance (Trust), Authenticity, Anonymity
   - Threats and Attacks
   - Security Principles
   - Identification, Authentication, Authorization
   - Access Control Models

2. **Fundamental Cryptographic Concepts and Primitives** [only a "black-box" description]
   - Pseudo-Random Number Generators
   - Secret Key Cryptography
   - Public Key Cryptography
   - Digital Signature and Multisignature
   - Cryptographic Hash Functions

- Merkle Tree

3. **Basic Concepts of Distributed Ledger Technologies (DLTs)**
   - The Problem of Trusting
   - Consensus Mechanisms
   - Overview of a Blockchain-Based DLT
   - Key Features of DLTs
   - Types of DLTs
   - Key Advantages of DLTs
   - Challenges and Risks Related to DLTs
   - Applications of DLTs
   - Smart Contracts
   - Existing Technologies

4. **Bitcoin's Blockchain**
   - Overview of the Bitcoin Cryptocurrency
   - Transactions and Chains of Transactions
   - Pseudonymity
   - Preventing Double Spending Attacks
   - P2P Distributed Timestamp Server (Network)
   - Blocks and Chain of Blocks (Blockchain)
   - Consensus Strategy - Proof-of-Work
   - Incentive - Mining and Fee
   - Wallets
   - Bitcoin as a State Transition System
   - Strategies for Improving Performances (Merkle Trees)
   - Scripting - Weak Version of Smart Contract

5. **Ethereum - A Decentralized Application Platform Supporting Smart Contracts**
   - Philosophy
   - Accounts
   - Messages and Transactions
   - Ethereum Virtual Machine (EVM)
   - Blockchain and Mining
   - Applications
   - Examples of Smart Contracts in Solidity

MODULO D

Titolo: *Data and Video Compression*
Docente: Fabrizio Frescura
Contatto docente*:* fabrizio.frescura@unipg.it (mobile: 348 - 15 16 466)
Periodo delle lezioni: maggio - giugno 2019 (gli studenti interessati sono pregati di prendere contatto con il docente per concordare il calendario delle lezioni).

PROGRAMMA

1. **Introduction**
   - 1.1 Introduction to data Compression
     - 1.1.1 Source and Channel Coding
   - 1.2 Compression Techniques
     - 1.2.1 Lossless Compression
     - 1.2.2 Lossy Compression
     - 1.2.3 Measures of Performance
   - 1.3 Modeling and Coding

2. **Mathematical Preliminaries for Lossless Compression**
   - 2.1 Overview
   - 2.2 A Brief Introduction to Information Theory
     - 2.2.1 Derivation of Average Information
   - 2.3 Models
     - 2.3.1 Physical Models
     - 2.3.2 Probability Models
     - 2.3.3 Markov Models
     - 2.3.4 Composite Source Model
   - 2.4 Coding
     - 2.4.1 Uniquely Decodable Codes
     - 2.4.2 Prefix Codes
     - 2.4.3 The Kraft-McMillan Inequality
   - 2.5 Algorithmic Information Theory
   - 2.6 Minimum Description Length Principle

3. **Huffman Coding**
   - 3.1 Overview
   - 3.2 The Huffman Coding Algorithm
     - 3.2.1 Minimum Variance Huffman Codes
     - 3.2.2 Optimality of Huffman Codes
     - 3.2.3 Length of Huffman Codes
     - 3.2.4 Extended Huffman Codes
   - 3.3 Non Binary Huffman Codes
   - 3.4 Adaptive Huffman Coding
     - 3.4.1 Update Procedure
     - 3.4.2 Encoding Procedure
     - 3.4.3 Decoding Procedure
   - 3.5 Golomb Codes
   - 3.6 Rice Codes

    - 3.6.1 CCSDS Recommendation for Lossless Compression
- 3.7 Applications of Huffman Coding
    - 3.7.1 Lossless Image Compression
    - 3.7.2 Text Compression
    - 3.7.3 Audio Compression

4. Arithmetic Coding

- 4.1 Overview
- 4.2 Introduction
- 4.3 Coding a Sequence
    - 4.3.1 Generating a Tag
    - 4.3.2 Deciphering the Tag
- 4.4 Generating a Binary Code
    - 4.4.1 Uniqueness and Efficiency of the Arithmetic Code
    - 4.4.2 Algorithm Implementation
    - 4.4.3 Integer Implementation
- 4.5 Comparison of Huffman and Arithmetic Coding
- 4.6 Adaptive Arithmetic Coding
- 4.7 Applications

5. Dictionary Techniques

- 5.1 Overview
- 5.2 Introduction
- 5.3 Static Dictionary
    - 5.3.1 Digram Coding
- 5.4 Adaptive Dictionary
    - 5.4.1 The LZ77 Approach
    - 5.4.2 The LZ78 Approach
- 5.5 Applications 133
    - 5.5.1 File Compression—UNIX compress
    - 5.5.2 Image Compression—The Graphics Interchange Format (GIF)
    - 5.5.3 Image Compression—Portable Network Graphics (PNG)

BOOKS

- David Salomon With Contributions by Giovanni Motta and David Bryant, “Data Compression The Complete Reference”, Springer
- Khalid Sayood “Introduction to Data Compression”, Elsevier

LAB ACTIVITES

- Main simulation tool: *Matlab* with *Image Processing Toolbox*
- Deepening and implementation of the Compression standards

PREREQUISITES

Probability and Random Processes	Mathematical Preliminaries for Transforms, Subbands, and Wavelets

• *Statistics and Probability*
  • Probability
  • Frequency of Occurrence
  • The Axiomatic Approach
  • Random Variables
  • Distribution Functions
  • Expectation
  • Mean
  • Second Moment
  • Variance
  • Types of Distribution
  ○ Uniform Distribution
  ○ Gaussian Distribution
  ○ Laplacian Distribution
  ○ Gamma Distribution
  ○ Stochastic Process
	• *Linear Algebra*
	  ○ Vector Spaces
	  ○ Dot or Inner Product
	  ○ Vector Space
	  ○ Subspace
	  ○ Basis
	  ○ Inner Product—Formal Definition
	  ○ Orthogonal and Orthonormal Sets
	• *Signal Theory / DSP*
	  ○ Fourier Series
	  ○ Fourier Transform
	  ○ Parseval's Theorem
	  ○ Modulation Property
	  ○ Convolution Theorem
	  ○ Linear Systems
	  ○ Time Invariance
	  ○ Transfer Function
	  ○ Impulse Response
	  ○ Filter
	  ○ Sampling
	  ▪ Ideal Sampling—Frequency Domain View
	  ▪ Ideal Sampling—Time Domain View
	  ○ Discrete Fourier Transform
	  ○ Z-Transform
	  ▪ Tabular Method
	  ▪ Partial Fraction Expansion
	  ▪ Z-Transform Properties
	  ○ Discrete Convolution