COURSE OVERVIEW IE0700
Cyber Security of Industrial Control System
(PLC, DCS, SCADA & IED)

Course Title
Cyber Security of Industrial Control System (PLC, DCS, SCADA & IED)

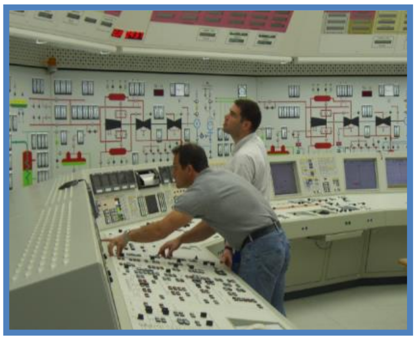
Course Reference
IE0700

Course Duration/Credits
Five days/3.0 CEUs/30 PDHs

Course Date/Venue

Session(s)	Date	Venue
1	February 04-08, 2024	Kizkulesi, Crown Plaza Istanbul Asia Hotels & Convention Center, Istanbul, Turkey
2	March 03-07, 2024	The Mouna Meeting Room, The H Dubai Hotel, Sheikh Zayed Rd - Trade Centre, Dubai, UAE

Course Description



This practical and highly-interactive course includes various practical sessions and exercises. Theory learnt will be applied using one of our state-of-the-art simulators.

The use of interconnected microprocessors in industrial systems has grown exponentially over the past decade. Deployed for process control in Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS) for many years, they have now moved into Intelligent Electronic Devices (IED) in applications such as substations, Motor Control Centers (MCC), and heat trace systems. The concern is that their connecting networks have grown as well, usually without much attention to the security ramifications. Intrusions, intentional and unintentional, can cause safety, environmental, production and quality problems.

The need for protecting Industrial Control Systems has grown significantly over the last few years. The combination of open systems; an increase in joint ventures; alliance partners and outsourced services; growth in intelligent manufacturing equipment; increased connectivity to other equipment/software; enhanced external connectivity; along with rapidly increasing incidents of network intrusion, more intelligent hackers, and malicious software, all lead to increased threats and probability of attack. As these threats and vulnerabilities increase, so does the need for protection of Industrial and Control Systems.

This course introduces several categories of electronic security technologies and discusses specific types of applications within each category, the vulnerabilities addressed by each type, suggestions for deployment, and known strengths and weaknesses, as well as some forms of mitigation for the mentioned risks.

The course provides participants with practical methods for evaluation and assessment of many current types of electronic security technologies and tools that apply to the Industrial Control Systems environment, including development, implementation, operations, maintenance, engineering and other user services. It provides guidance to manufacturers, vendors, and security practitioners at end-user companies on the technological options for securing these systems against electronic (cyber) attack.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain a comprehensive knowledge on security of industrial control systems including SCADA, DCS & PLC and recognize their characteristics, threats and vulnerabilities
- Identify different ISA security standards and determine industrial control system security program development and deployment
- Emphasize network architecture in industrial control system and list down the recommended firewall rules for specific services
- Determine the various industrial control system security controls including management, operational & technical controls and identify the SCADA vulnerabilities & attacks
- Employ SCADA security methods, mechanisms & techniques and explain SCADA security standards and reference documents
- Acquire knowledge on SCADA security management implementation issues & guidelines and determine the unique characteristics & requirements of SCADA systems
- Analyze the selected ISA technical papers of security issues including the physical protection of critical infrastructures & key assets, critical infrastructure protection, network security in the wireless age, etc

Who Should Attend

This course provides an overview of all significant aspects and considerations of cyber security of industrial control system (PLC, DCS, SCADA & IED) for a broad audience that includes asset owners from process, power and other critical infrastructures, control systems engineers, IT engineers, IT professionals, instrumentations engineers, instrumental & control staff, information and security officers and vendors, as well as security experts from government, industry associations and academia.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Certificates are accredited by the following international accreditation organizations:

- The International Accreditors for Continuing Education and Training (IACET - USA)

  Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

  Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

  Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

- British Accreditation Council (BAC)

  Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Mr. Anouar Dhifallah, MSc, BSc, is a **Senior Instrumentation & Control Engineer** with over **20** years of extensive experience within the **Power & Water Utilities** and other **Energy** sectors. His expertise widely covers in the areas of **Actuators & Valve Selection**, **Process Control & Automation**, **Batch Process & Sequential Control**, **Analog Control**, **Operator Interfaces**, **Data Communication**, **Networking Design and Configurations**, **Instrumentation & Control**, General **Instrumentation & Process** Control, **System Checkout & Testing**, **Advanced Control** with **PLC's**, **Ladder Logic**, **Process Instrumentation & Control**, **Control Valve Maintenance**, **Process Automation & Control Instrumentation**, **Foxboro**, **ABB**, **Rosemount**, **Yokogawa**, **Pneumatic & Electronic**, **Level Measurement, HV/LV Equipment**, **High Voltage Electrical Safety**, **LV & HV Electrical System**, **HV Equipment** Inspection & Maintenance, **HV Switchgear** Operation & Maintenance, **LV Distribution Switchgear & Equipment**, **Electrical Safety**, **Electrical** Maintenance, Inspection, Testing & **Risk** Assessment, **Electrical Generator** Protection, **Electrical Generator** Testing & Maintenance, Programmable Logic Controller (**PLC**), Distribution Control System (**DCS**), **Temperature**, **Flow & Level** Measurement, **Pneumatic & Hydraulic** Technologies, **Substation Automation** Systems & Application, Testing & Maintenance of **Electrical Substations**, **Electrical Substation 33/11KV** Design, Electrical **Power Substation** Maintenance, **Electrical Equipment** Inspection, Testing & Troubleshooting, **Lighting Installation** Design, **Electric Distribution** System, **Load Forecasting** Methods, **Transmission** & **Distribution** Analysis, **Circuit Breakers** Inspection & Maintenance, **Protective Relaying**, **Electrical & Control** System, **Switchgears**, **Transformers**, **Medium & High Voltage Equipment**, **Circuit Breakers**, **Cable & Overhead Line** Troubleshooting & Maintenance, **HV/MV Cable Splicing**, **High Voltage Circuit Breaker** Inspection & Repair, **Cable & Over Head Power Line**, **HV Cable** Design, **Cable** Splicing & Termination, **Cable** Jointing Techniques, **High Voltage Power** System, **Electrical Standards**, **Electrical Drawing & Schematics**, **Voltage Distribution**, **Power Distribution**, **Filters**, **Automation System**, **Electrical Variable Speed Drives**, **Power** Systems, **Power Generation**, **Diesel Generators**, **Power Stations**, Uninterruptible Power Systems (**UPS**), **Battery Chargers**, **AC & DC Transmission**, **CCTV** Installation, **Data & Fire Alarm** System, **Security** Systems, **Evacuation** Systems and **Electrical Motors & Variable Speed Drives**, Renewable Energy and Installation & Control of Electrical and Electronic devices.

During Mr. Anouar's career life, he has gained his practical experience through several significant positions and dedication as the **Electrical & Instrumentation Department Head**, **Technical Services Manager**, **Field Engineer**, **Electrical Engineer**, **Electrical Instructor/Trainer**, **Faculty Coach** and **Instructor/Trainer** from various companies, colleges and institutes like the Technical School of Zarzis, Ambatovy Training Center, Tunisian National Oil Co., Rancho Santiago College, Al Baha Technical College, **ARAMCO**, **PDO**, Tunisie Telecom Co., Al Seeb Institute, Russyal Institute and Technical College of Tunisia.

Mr. Anouar has a **Master's** degree in **Electronics & Telecommunication Engineering** and a **Bachelor's** degree in **Electrical & Instrumentation Engineering**. Further, he is a **Certified Instructor/Trainer**, a **Certified Coach** from the International Coaching Federation (ICF) and delivered numerous trainings, courses, workshops, seminars and conferences internationally.

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures
20% Practical Workshops & Work Presentations
30% Hands-on Practical Exercises & Case Studies
20% Simulators (Hardware & Software) & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Fee

Istanbul	**US$ 6,000** per Delegate + **VAT**. This rate includes Participants Pack (Folder, Manual, Hand-outs, etc.), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.
Dubai	**US$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 - 0930	***Overview of Industrial Control Systems*** *Overview of SCADA, DCS and PLCs • Industrial Control System Operation • Key Industrial Control System Components • SCADA Systems • Distributed Control Systems • Programmable Logic Controllers • Industrial Sectors and Their Interdependencies*
0930 - 0945	*Break*
0945 - 1030	***Industrial Control System Characteristics, Threats & Vulnerabilities*** *Comparing Industrial Control System and IT Systems • Threats • Potential Industrial Control System Vulnerabilities • Risk Factors • Possible Incident Scenarios • Sources of Incidents • Documented Incidents*
1030 - 1230	***ISA Security Standards*** *ANSI/ISA-TR99.00.01-2004 • ANSI/ISA-TR99.00.02-2004 • ANSI/ISA-TR99.00.01-2007*
1230 - 1245	*Break*
1245 - 1420	***ISA Security Standards (cont'd)*** *ANSI/ISA-TR99.00.02-2007 • ANSI/ISA-TR99.00.03-2007 • ANSI/ISA-TR99.00.04-2007*
1420 - 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2

0730 - 0900	***Industrial Control System Security Program Development & Deployment*** *Business Case for Security*
0900 - 0930	***Industrial Control System Security Program Development & Deployment (cont'd)*** *Developing a Comprehensive Security Program*
0930 - 0945	*Break*
0945 - 1230	***Network Architecture*** *Firewalls ● Logically Separated Control Network ● Network Segregation ● Recommended Defense-in-Depth Architecture ● General Firewall Policies for Industrial Control System ● Recommended Firewall Rules for Specific Services*
1230 - 1245	*Break*
1245 - 1420	***Network Architecture (cont'd)*** *Network Address Translation (NAT) ● Specific Industrial Control System Firewall Issues ● Single Points of Failure ● Redundancy and Fault Tolerance Preventing Man-in-the-Middle Attacks*
1420 - 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3

0730 - 0900	***Industrial Control System Security Controls*** *Management Controls ● Operational Controls*
0900 - 0930	***Industrial Control System Security Controls*** *Technical Controls*
0930 - 0945	*Break*
0945 - 1230	***SCADA Vulnerabilities & Attacks*** *The Myth of SCADA Invulnerability ● SCADA Risk Components ● Managing Risk*
1230 - 1245	*Break*
1245 - 1420	***SCADA Vulnerabilities & Attacks (cont'd)*** *SCADA Threats and Attack Routes ● SCADA Honeynet Project*
1420 - 1430	***Recap***
1430	*Lunch & End of Day Three*

Day 4

0730 - 0900	***SCADA Security Methods & Techniques*** *SCADA Security Mechanisms ● SCADA Intrusion Detection Systems*
0900 - 0930	***SCADA Security Methods & Techniques (cont'd)*** *SCADA Audit Logs ● Security Awareness*
0930 - 0945	*Break*
0945 - 1230	***SCADA Security Standards & Reference Documents*** *ISO/IEC 17799:2005 and BS 7799-2:2002 ● ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems ● ISA-TR99.00.02-2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment ● GAO-04-140T Critical Infrastructure Protection, Challenges in Securing Control Systems*

1230 - 1245	*Break*
1245 - 1430	***SCADA Security Standards & Reference Documents (cont'd)*** *NIST, System Protection Profile for Industrial Control Systems (SPP ICS) ● Federal Information Processing Standards Publication (FIPS Pub) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004 ● Additional Useful NIST Special Publications*
1420 - 1430	***Recap***
1430	*Lunch & End of Day Four*

Day 5

0730 - 0900	***SCADA Security Management Implementation Issues & Guidelines*** *Management Impressions of SCADA Security ● SCADA Culture ● Unique Characteristics and Requirements of SCADA Systems*
0900 - 0930	***SCADA Security Management Implementation Issues & Guidelines (cont'd)*** *Limitations of Current Technologies ● Guidance for Management in SCADA Security Investment ● NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems*
0930 - 0945	*Break*
0945 - 1230	***Selected ISA Technical Papers on Security Issues*** *The Physical Protection of Critical Infrastructures and Key Assets ● Critical Infrastructure: Control Systems and the Terrorist Threat ● Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems ● The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems ● Network Security in the Wireless Age*
1230 - 1245	*Break*
1245 - 1345	***Selected ISA Technical Papers on Security Issues (cont'd)*** *Remote Method Security in a Distributed Processing Architecture Supporting Generic Security Objects ● Current Status of Technical Issues Concerning Cyber Security of Control Systems for Water and Wastewater Industries ● Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks ● 21 Steps to improve Cyber Security of SCADA Networks*
1345 – 1400	***Course Conclusion***
1400 – 1415	***POST-TEST***
1415 - 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Simulator (Hands-on Practical Sessions)

Practical sessions will be organized during the course for delegates to practice the theory learnt. Delegates will be provided with an opportunity to carryout various exercises using one of our state-of-the-art simulators "Allen Bradley SLC 500", "AB Micrologix 1000 (Digital or Analog)", "AB SLC5/03", "AB WS5610 PLC", "Siemens S7-1200", Siemens S7-400" "Siemens SIMATIC S7-300", "Siemens S7-200" "GE Fanuc Series 90-30 PLC", "Siemens SIMATIC Step 7 Professional Software", "HMI SCADA" and "PLCLogix 5000 Software".

Allen Bradley SLC 500 Simulator

Allen Bradley Micrologix 1000 Simulator (Digital)

Allen Bradley Micrologix 1000 Simulator (Analog)

Allen Bradley SLC 5/03

Allen Bradley WS5610 PLC Simulator PLC5

Siemens S7-1200 Simulator

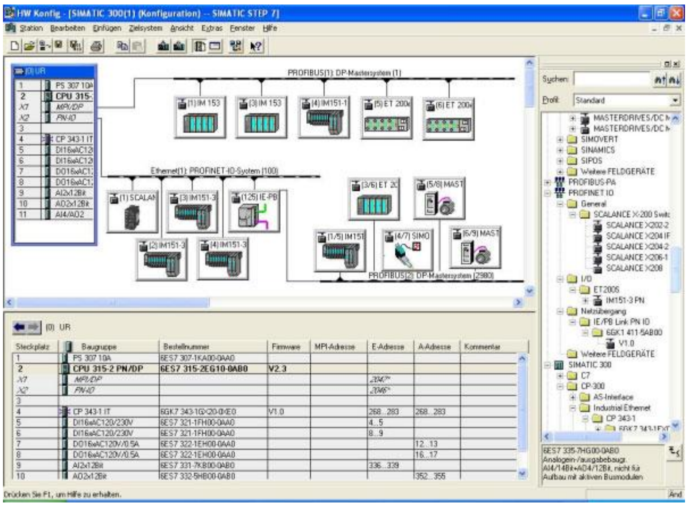
Siemens S7-400 Simulator

Siemens SIMATIC S7-300

Siemens S7-200 Simulator

GE Fanuc Series 90-30 PLC Simulator

Schneider Electric Magelis HMISTU



HW Konfig - [SIMATIC 300(1) (Konfiguration) -- SIMATIC STEP 7]

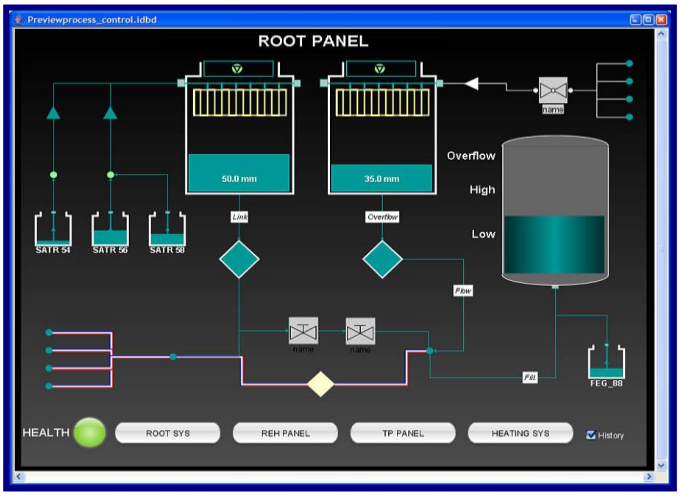
(0) UR

Steckplatz	Baugruppe	Bestellnummer	Firmware	MPI-Adresse	E-Adresse	A-Adresse	Kommentar
1	PS 307 10A	6ES7 307-1KA00-0AA0					
2	**CPU 315-2 PN/DP**	**6ES7 315-2EG10-0AB0**	**V2.3**				
X7	*MPI/DP*				*2047**		
X2	*PN-IO*				*2046**		
3							
4	CP 343-1 IT	6GK7 343-1GX20-0XE0	V1.0		268...283	268...283	
5	DI16xAC120/230V	6ES7 321-1FH00-0AA0			4...5		
6	DI16xAC120/230V	6ES7 321-1FH00-0AA0			8...9		
7	DO16xAC120V/0.5A	6ES7 322-1EH00-0AA0				12...13	
8	DO16xAC120V/0.5A	6ES7 322-1EH00-0AA0				16...17	
9	AI2x12Bit	6ES7 331-7KB00-0AB0			336...339		
10	AO2x12Bit	6ES7 332-5HB00-0AB0				352...355	

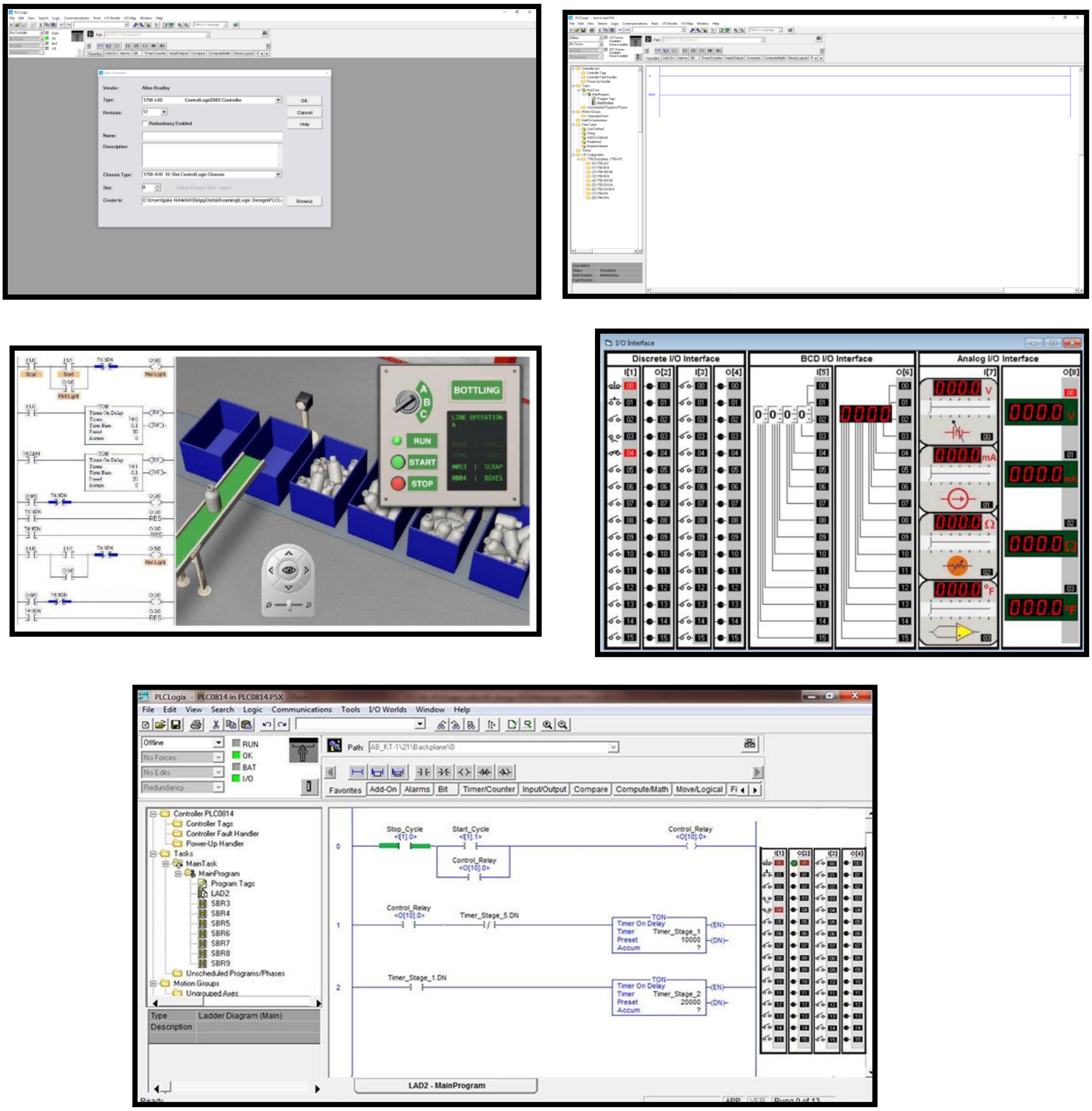
6ES7 335-7HG00-0AB0
Analogein-/ausgabebaugr.
AI4/14Bit+AO4/12Bit, nicht für
Aufbau mit aktiven Busmodulen

Drücken Sie F1, um Hilfe zu erhalten.

Siemens SIMATIC Step 7 Professional Software



HMI SCADA



PLCLogix 5000 Software

Course Coordinator
Kamel Ghanem, Tel: +971 2 30 91 714, Email: kamel@haward.org