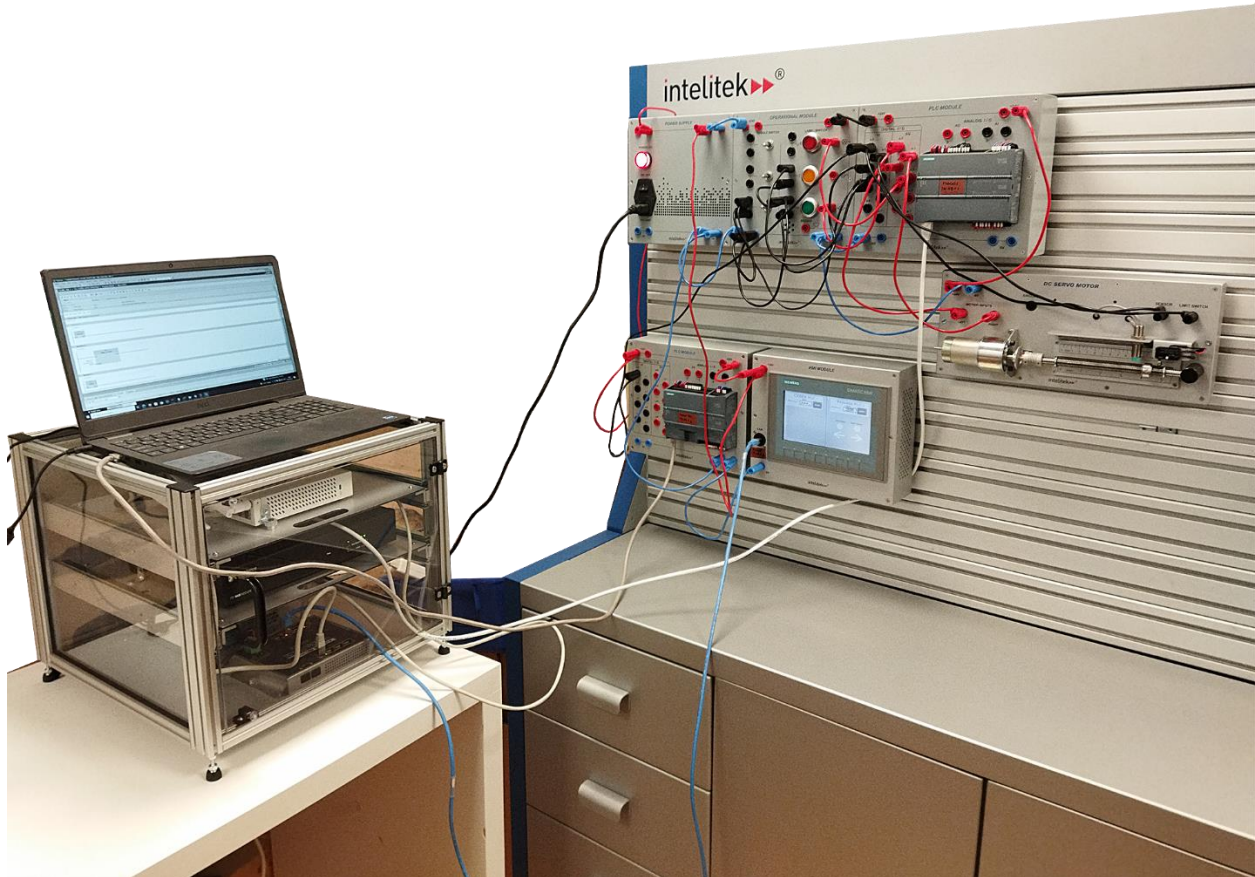


Industrial Cybersecurity Experimentation Package



LAB ACTIVITY GUIDE

Catalog #34-8000-0019 Rev. A

intelitek▶▶[®]

INDUSTRY 4.0 

Copyright © 2022 Intelitek Inc.

Tel: (603) 625-8600

Industrial Cybersecurity Lab Activity Guide

Fax: (603) 437-2137

Cat. # 34-8000-0019 Rev. A

September 2022

website: <http://www.intelitek.com>

email: info@intelitek.com

Intelitek software and documentation are available at <http://intelitekdownloads.com>.

All rights reserved. No part of this publication may be stored in a retrieval system, or reproduced in any way, including but not limited to photocopy, photography, magnetic, or other recording, without the prior agreement and written permission of the publisher. Program listings may be entered, stored, and executed in a computer system, but not reproduced for publication.

Every effort has been made to make this book as complete and accurate as possible. However, no warranty of suitability, purpose, or fitness is made or implied. Intelitek is not liable or responsible to any person or entity for loss or damage in connection with or stemming from the use of the software, hardware and/or the information contained in this publication.

Intelitek bears no responsibility for errors that may appear in this publication and retains the right to make changes to the software, hardware, and manual without prior notice.

Table of Contents

1. Getting Started.....	4
1.1. Overview	4
1.2. Prerequisites.....	4
1.3. Where are the Lab Activities?.....	4
2. Materials	5
3. Navigating the Lab Activities.....	6
3.1. Overview and Preparation.....	6
3.2. Videos and QR Codes.....	6
4. List of Lab Activities (Course Outline)	7

1. Getting Started

1.1. OVERVIEW

Thank you for purchasing the Intelitek *Industrial Cybersecurity Experimentation Package* for use in your classroom or laboratory. In a world where cyberthreats are ever-present, a manufacturing enterprise must do everything in its power to protect its valuable assets and information from external attack. The Intelitek *Industrial Cybersecurity Experimentation Package with the JobMaster Mechanical Training Bench* is meant to provide a scaled-down, smart factory network coupled with an accompanying informational technology (IT) network equipped with various cybersecurity features. The experimentation kit is usable in an educational setting, while still providing would-be technicians and factory managers authentic, industry-recognized hardware and software.

This guide is meant to help you get started with the laboratory curriculum and provide you with access to the various lab activities.

1.2. PREREQUISITES

It is strongly recommended that you complete Intelitek's Level 1 and Level 2 Industry 4.0 courses before performing these lab activities.

1.3. WHERE ARE THE LAB ACTIVITIES?

You can find the lab activities on the course page. A summary of each activity is found in Section 4, List of Lab Activities, on page 7. All lab activities are available on downloadable and printable PDF documents.

2. Materials

Materials required for each lab activity are also listed at the beginning of each activity. Make sure all materials are ready before the beginning of each lab period.

Individual lab activity exercises contain hyperlinks to download any required software. All software should be downloaded and installed before starting a lab activity.

Intelitek software and documentation are available at <http://intelitekdownloads.com>.

The following materials are necessary for completion of the course.

		Quantity	Note
Hardware	Intelitek Cybersecurity Cabinet (includes data diode, switch, and firewall server)	1	
	Power Supply Module	1	
	Operational Module	1	
	PLC Module	2	One controller acts as the process PLC, the other as the cyber PLC
	Cybersecurity laptop computer	1	
	DC Servo Motor Module	1	
	HMI Module	1	
	Electrical connectors		Banana plugs
	Ethernet cables		
	JobMaster Training System (JMST) Panel	1	
Software	Software and firmware are accessed from the individual lab activities.		
Other	Personal Computer		
	Ethernet/Network switch		

3. Navigating the Lab Activities

3.1. OVERVIEW AND PREPARATION

Lab activities include tasks that must be performed using the Intelitek *Industrial Cybersecurity Package*.

Participants are assigned with reading the lab activity PDFs (see Section 4, List of Lab Activities, below) and performing the tasks. Both participants and instructors are encouraged to read through the activities ahead of each lab period as preparation.

All activities require instructor verification to ensure that the work of the participants meet the requirements in the performance objectives. Performance objectives are listed at the beginning of each lab activity.

3.2. VIDEOS AND QR CODES

Lab activities may contain QR codes like the one below. Click these codes or scan them with your smartphone to watch instructional or illustrative videos that are relevant for the specific lab activity task.

An example QR code is given here:



4. List of Lab Activities (Course Outline)

Below is a list of lab activities in the *Industrial Cybersecurity Experimentation Package*. Ctrl + click the name of each activity to navigate to that lab activity.

Note: Lab activities may be password protected. Contact support@intelitek.com if you have not received passwords for the activities.

Lab Activity	Description
Activity 1: Exploring the Factory Network	Explore the main components of the OT (Operational Technology) and IT (Information Technology) networks of the smart factory. Identify the main components of the IT and OT networks and test your knowledge about cybersecurity concepts.
Activity 2: The Switch	Install and configure the network switch.
Activity 3: The Data Diode	Install and configure the data diode.
Activity 4: The Firewall	Install and configure the firewall.
Activity 5: Testing the IT Network	Perform various tests on the cybersecurity components to ensure their proper configuration.
Activity 6: Setup and Activation of the Smart Factory	Physically connect each component of the Operational Technology Kit to set up your smart factory network. Observe how each device functions according to the PLC logic.
Activity 7: Simulated Attack on the Process PLC	Simulate a cyber-attack on the process PLC. Observe how the attack affects the process and how the parallel reference system (PRS) identifies it.
Activity 8: Simulated Attack on the Cyber PLC	Simulate an attack on the cyber PLC. Observe how the attack affects the process and how the parallel reference system (PRS) behaves under such an attack.
Activity 9: Threat Prevention	Critically analyze the vulnerability of the system by identifying the various weak points that could have led to its exploitation.