Cyber Security for Automation Systems
Training Manual

Unity Pro v8.0

Schneider Electric

DISCLAIMER

Schneider Electric Limited makes no representations or warranties with respect to this manual and, to the maximum extent permitted by law, expressly limits its liability for breach of any warranty that may be implied to the replacement of this manual with another. Furthermore, Schneider Electric Limited reserves the right to revise this publication at any time without incurring an obligation to notify any person of the revision.

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric Limited nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information that is contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric Limited software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Cyber Security for Automation Systems Training Manual

INTRODUCTION AND LEGAL NOTICE

Your purchase of this official Cyber Security for Automation Systems Training Manual entitles you to undertake the Cyber Security for Automation Systems training course.

Satisfactory completion of the course evaluation is mandatory for you to obtain a Schneider Electric Limited certificate of completion of the training course.

Schneider Electric Limited will not accept any liability for action taken in reliance on this training manual.

TRADEMARKS (Cyber Security)

Schneider Electric Limited has made every effort to supply trademark information about company names, products and services mentioned in this manual. Trademarks shown below were derived from various sources.

Unity Pro is a trademark owned by Schneider Electric or its affiliated companies. All other trademarks are the property of their respective owners.

Microsoft Windows®, Windows® XP, Windows® 7 and Excel are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

General Notice:

Some product names used in this manual are used for identification purposes only and may be trademarks of their respective companies.

Validity Note

The present documentation is intended for qualified technical personnel responsible for the implementation, operation and maintenance of the products described. It contains information necessary for the proper use of the products.

About Us

Members of Schneider Electric's team of Instructional Designers have tertiary qualifications in Education, Educational Course Development and are also experienced Instructors. Currently, the team is supporting a range of Schneider Electric courses in multiple languages and multiple software environments.

Authors

Antony Saunders and Tristan Powell

August 2015 Edition for Unity Pro v8.0
Manual Release 1.0

Safety Information

Important Information

PLEASE NOTE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety alert messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Safety Information (cont.)

Important Information (cont.)

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Before the Course Begins

Scope of this Training Manual

This training manual is a supplement to the authorised training. In order to make proper use of the software students should also refer to the documentation that has been provided with the product such as the Help Files, User Guides or Knowledge Base.

The graphics displaying screen captures were taken using the Windows® XP and Windows® 7 operating systems using Classic mode display properties. If students are running a different version of Windows then screen images may differ slightly from those shown in the training manual.

Some screen captures may have been taken from beta versions of the software and may vary slightly from release screen captures.

Product Related Information

⚠ DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the unit.
- Use only the specified voltage when operating this equipment and any associated products.

Failure to follow these instructions will result in death, serious injury, or equipment damage.

Product Related Information (cont.)

⚠ WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines[1].
- Each implementation of this equipment must be individually and thoroughly tested for a proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

[1] For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Safety Information (cont.)

User Responsibilities

The products specified in this document have been tested under actual service conditions. Of course, your specific application requirements may be different from those assumed for this and any related examples described herein. In that case, you will have to adapt the information provided in this and other related documents to your particular needs. To do so, you will need to consult the specific product documentation of the hardware and/or software components that you may add or substitute for any examples specified in this training documentation. Pay particular attention and conform to all safety information, different electrical requirements and normative standards that would apply to your adaptation.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The use and application of the information contained herein require expertise in the design and programming of automated control systems. Only the user or integrator can be aware of all the conditions and factors present during installation and setup, operation, and maintenance of the machine or process, and can therefore determine the automation and associated equipment and the related safeties and interlocks which can be effectively and properly used. When selecting automation and control equipment, and any other related equipment or software, for a particular application, the user or integrator must also consider any applicable local, regional or national standards and/or regulations.

Before the Course Begins (cont.)

User Responsibilities (cont.)

Some of the major software functions and/or hardware components used in the examples described in this training document cannot be substituted without significantly compromising the performance of your application. Further, any such substitutions or alterations may completely invalidate any proposed architectures, descriptions, examples, instructions, wiring diagrams and/or compatibilities between the various hardware components and software functions specified herein and in related documentation. You must be aware of the consequences of any modifications, additions or substitutions. A residual risk, as defined by EN/ISO 12100-1, Article 5, will remain if:

- it is necessary to modify the recommended logic and if the added or modified components are not properly integrated in the control circuit.
- you do not follow the required standards applicable to the operation of the machine, or if the adjustments to and the maintenance of the machine are not properly made (it is essential to strictly follow the prescribed machine maintenance schedule).
- the devices connected to any safety outputs do not have mechanically-linked contacts.

⚠ CAUTION

EQUIPMENT INCOMPATIBILITY

Read and thoroughly understand all device and software documentation before attempting any component substitutions or other changes related to the application examples provided in this document.

Failure to follow these instructions can result in injury or equipment damage.

Safety Information (cont.)

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

⚠ CAUTION

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters and debris from equipment.

Failure to follow these instructions can result in injury or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Safety Information (cont.)

Startup and Test (cont.)

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Safety Information (cont.)

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

Course Overview

Course Instructor

Please write the name of the Instructor here: ☞ _____

The course Instructor will be spending the next One Day with the class, and will guide the students through this training course. The Instructor is an experienced **Unity Pro** user so please feel free to ask questions.

Course Objectives

By the completion of this training course the student will be able to:

- Identify the importance of **Cyber Security**
- Configure aspects of **Unity Pro** to enhance **Cyber Security**

Target Audience

This Cyber Security for Automation Systems training course is an integral part of the complete Schneider Electric Educational Services curriculum. This course is designed for:

- Users who are new to **Cyber Security**.
- Users who already have programming experience with **Unity Pro**.
- Existing users of **Unity Pro**.
- Users who understand **Networking** and **Industrial Communications**.

Further Training:

This course is specifically designed for experienced programmers who may also find they are able to complete the content in this course before the designated One Day.

More complex programming techniques using Cicode and its use within the **Unity Pro** design environment are covered in the **Unity Pro** Customization and Design Course.

Prerequisite Knowledge

It is expected that trainees will:

- Be familiar with the concepts of **PLCs**
- Be familiar with the concepts of **Industrial Automation**
- Be familiar with the concept of **Ethernet Networking**
- Be familiar with **Unity Pro**
- Be familiar with **Microsoft Windows®**

Course Overview (cont.)

Course Program

The training course will take One Day to complete. The following program outlines the topics that will be covered on each day:

Day	Topics
1	➢ What is Cyber Security ➢ Cyber Security Defence ➢ Password Management ➢ Source Code Access ➢ Unsolicited Connections ➢ Change Management ➢ HTTP and FTP Servers ➢ Unity Pro Integrity Check

Support

If support or additional information about any concepts or products in the course is required, students should ask the Instructor who will either address the question or obtain additional technical assistance as required.

Conventions Used in this Manual

Objectives

These are the skills to be achieved by the end of each chapter. An overview providing a brief synopsis of the topic begins each section. Often, examples are given to illustrate the conceptual overview.

Example -

The configuration environment consists of several toolbars, browser windows and programming editors. This chapter introduces the user to the configuration environment using an example project with pre-defined elements.

This Chapter Covers These Topics:

- Topic A 1-2
- Topic B 1-3
- Topic C 1-5

Exercises

After a concept is explained students will be given exercises that practice the skills just learned. These exercises begin by explaining the general concept of each exercise and then step-by-step procedures are listed to guide students through each exercise.

Example -

Paste an object from a library onto a test page called **Utility**.

1 Run the Milk_Upgrade project then trigger and view some alarms.

i. Use the following template settings:

User Input

Whenever information is to be typed into a field or dialog box it will be written in this font:

```
KETTLE_TEMP/25
```

Note that some exercises will show a fragment of information already typed into a Unity Pro screen and then ask students to add extra lines of configuration. In this instance, the previously entered material will be given to the student as light grey italic text.

KETTLE_TEMP/25

```
OVEN_TEMP/5
```

Conventions Used in this Manual (cont.)

Hints & Tips

This heading will provide students with useful or helpful information that will make configuring the project easier.

Example -

 **Hints & Tips:**

To go to the next field, use the mouse cursor or press the **TAB** key.

Note

A note will refer to a feature which may not be obvious at first glance but something that should always be kept in mind.

Example -

 **Note:**

Any events named **GLOBAL** are enabled automatically when events are enabled.

Menus and Menu Options

Text separated by the double arrow symbol "**»**" indicates that students are to select a menu.

Example -

File » New…

Open a menu "**File**" then select the menu option "**New…**"

Horizontal and Vertical Tabs

Text written this way indicates the **Horizontal** then the **(Vertical)** tab is to be selected.

Example -

Appearance (General)

Conventions Used in this Manual (cont.)

See Also

Text written in this way indicates further references about the current topic.

Example -

See Also:

For further information about **Templates,** see U*nity Pro Help - Using Page Templates*.

Further Training

This heading describes topics that are covered in more advanced courses.

Example -

Further Training:

Trend Table Maths is a topic in the **Customisation and Design Course**.

Table of Contents

Table of Exercises

	Description	> Chapter-Page
Exercise:	**PLC Code Transfer Denial**	> 3-2
Exercise:	**PLC Variable Security**	> 3-3
Exercise:	**Unsolicited Unity Pro Connections**	> 3-4
Exercise:	**Unsolicited Modbus or EIP Connections**	> 3-5
Exercise:	**Unity Pro XL v8.0 - Integrity Check**	> 3-7

CHAPTER 1: CYBER SECURITY FOR AUTOMATION SYSTEMS 1-1

Overview 1-1
What is Cyber Security? 1-2
Cyber Security Defence 1-6

CHAPTER 2: CYBER SECURITY CONFIGURATION 2-1

Overview 2-1
Password Management 2-2
Services Control 2-7
Access Control 2-8
Change Management 2-11

CHAPTER 3: CYBER SECURITY PRACTICALS 3-1

Overview 3-1
Source Code Control 3-2
Unsolicited Connections 3-4
Unity Pro Integrity Check 3-6

Chapter 1: Cyber Security for Automation Systems

Overview

Introduction

This chapter provides guidelines and practical tips to help users secure an existing automation system.

Some of these features are independent of each other but it is recommended that they are combined together to improve the security level of the system architecture depending on the needs of each user.

Chapter Objectives

By the completion of this chapter you will be able to:

- Understand the definition of and reasons for **Cyber Security**

This Chapter Covers These Topics:

- What is Cyber Security? 1-2
- Cyber Security Defence 1-6

What is Cyber Security?

Definitions of Cyber...

- **Cyber -** Is derived from the word **Cybernetic,** meaning control of speech and function**,** which itself comes from the Greek adjective meaning *skilled in steering or governing*.

  It is a common, often overused, prefix used for Internet, Computer and Information Technology (IT) terms. To the extent that it should only be used to denote control (electronic or remote) of the thing represented by the word it precedes, but instead it has become synonymous with anything related to computing and in particular to the Internet.

- **Cyberspace -** An unregulated network of computers and systems, such as the Internet, which is at risk of being infiltrated by unwanted actions or persons.

- **Cyber Risks** - Are vulnerabilities present in a computerised system or network that exposes the system to possible threats or crime.
- **Cyber Threats** - Are actions or accidents that can disrupt the normal operation of a computerised system and its networks.

  These actions can be initiated from within the physical facility or from any external location if the system is connected to the Internet.

- **Cyber Crime** - Is the deliberate and criminal use of these treats, by individuals or organised groups, intent on extracting money, data or causing disruption to a system or network.

  Cyber Crime can take many forms; including the acquisition of intellectual property and impairing the operations of a website or utility service, up to the worst levels of Cyber War and Cyber Terror.

  - **Cyber War -** A nation state conducting sabotage and espionage against another nation or state in order to cause disruption or to extract data.
  - **Cyber Terror -** An organisation, working independently of a nation state, conducting terrorist activities to commit Cyber War

- **Cyber Security** - Securing against these risks, threats and possible crime is the ongoing challenge of **Cyber Security**.

What is Cyber Security? (cont.)

Malicious Software (Malware)

Cyber criminals operating locally or remotely can use many methods of attacking a system or network. These methods fall broadly under the term of Malicious Software or Malware.

The types of Malware include:

- **Spyware and Adware :** A software program hidden inside an e-mail attachment, web page, link or software download that collects personal or corporate information with the intent to bombard the individual or corporation with unwanted e-mails (Junk Mail) and/or advertising. This can reach such levels as to inhibit network traffic.

  The user may be requested to acknowledge or accept installation, describing this behaviour in loose terms so that it is easily misunderstood or ignored, with the intention of deceiving the user into installing it without the supplier being technically in breach of the law.

- **Virus :** A software program that attaches itself to or mimics another software file and replicates itself across a computer network with the intent to; gain access to, steal, modify and/or corrupt information and files from a targeted computer system.

- **Worm :** Another self-replicating software program which doesn't need to mimic or attach itself to another file.

  These often carry a payload intent on damaging networks and providing the worm author exclusive access to the infected computer(s), whilst continually looking for further vulnerabilities and reporting back to the author when and where these weaknesses are found.

- **Trojan :** A software program disguised as part of or an entire valid software package whilst carrying out a malicious act.

  These commonly mimic anti-virus tools to avoid being shut down, detected or deleted, whilst corrupting user accounts or files and/or installing rootkits and backdoors in order to download further Malware without detection.

- **Rootkit :** A software package that modifies a computer's Operating System so that Malware files are hidden from the user and/or the system processes.

  Other rootkits defend themselves another other malware against removal by halting the deletion process and copying themselves and the malware to a new location, milliseconds before the original files are removed.

- **Backdoor :** A software tool that computer manufacturers and software companies use to bypass normal security and authentication procedures in order to gain access to computer systems over a network or the Internet for valid support and recovery reasons.

  Unfortunately these can also be used by cyber criminals for malicious reasons.

What is Cyber Security? (cont.)

Sources

The best practise of **Cyber Security** is to implement a security plan that accounts for various potential sources of cyber attacks and accidents, including:

Source	Description
Internal	➢ inappropriate employee or contractor behaviour ➢ disgruntled employee or contractor
External opportunistic (non-directed)	➢ script kiddies* ➢ recreational hackers ➢ virus writers
External deliberate (directed)	➢ criminal groups ➢ activists ➢ terrorists ➢ agencies of foreign states
Accidental	➢ Non specific
* slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding of how the script works or its potential impact on a system	

What is Cyber Security? (cont.)

Challenges

The **Cyber Security** challenges that exist for **PlantStruxure** control systems include:

- Diverse physical and logical boundaries
- Multiple sites and large geographic spans
- Adverse effects of security implementation on process availability
- Increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open
- Increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network
- Direct impact of control systems on physical and mechanical systems

Impact

A deliberate cyber attack on a **PlantStruxure** control system may be launched to achieve a number of malicious results, including:

- Disrupt the production process by blocking or delaying the flow of information
- Damage, disable, or shut down equipment to negatively impact production or the environment
- Modify or disable safety systems to cause intentional harm

How Attackers Gain Access

A cyber attacker bypasses the perimeter defences of a network to gain access to the control system.

Common points of access include:

- Dial-up access to remote terminal unit (RTU) devices
- Supplier access points (such as technical support access points)
- IT-controlled network products
- Corporate virtual private network (VPN)
- Database links
- Poorly configured firewalls
- Peer utilities

Cyber Security Defence

Network Administration

Cyber Security is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions.

The objective of **Cyber Security** is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

The basic components of **Cyber Security** within network administration are:

- Risk assessment
- A security plan built on the results of the risk assessment
- A multi-phase training campaign
- Physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- System Access Control
- **Device Hardening**
- Network monitoring and maintenance

The remainder of this document focuses mainly on item 6 - **Device Hardening**

See Also:

One method of **System Access Control** is to use software that restricts access to only a known list of applications rather than attempt to keep an updated list of known threats to protect against. This method is called **Whitelisting** (rather than Blacklisting). **Schneider Electric**, working closely with renowned virus protection experts **McAfee** has produced a suite of whitelisting control software solutions.

For general information on this access control software solution refer to the **McAfee Whitelisting Paper http://www.schneider-electric.com/products/ww/en/8200-cybersecurity-solutions/80041-application-whitelisting/62397-mcafee/:** available on the Internet.

Cyber Security Defence (cont.)

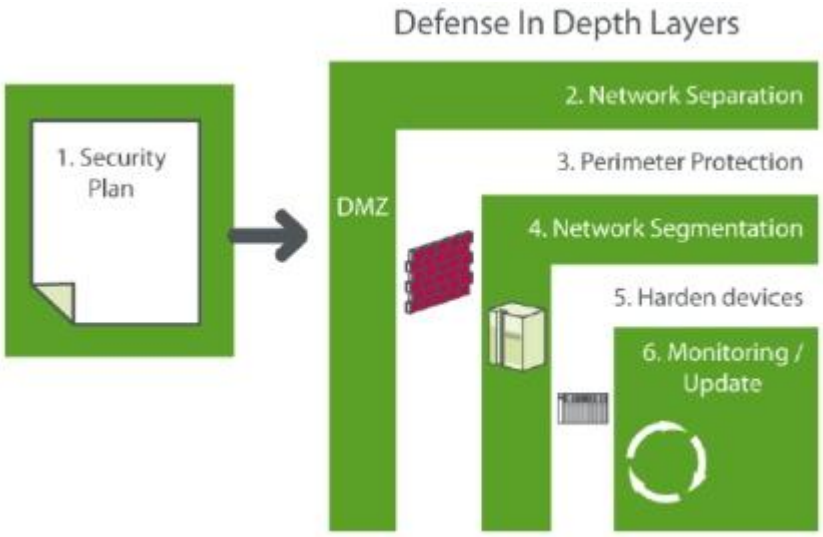
Schneider Electric Defence in Depth (DiD)

No single solution can provide adequate protection against all cyber attacks on a control network.

Schneider Electric recommends employing a "**Defence in Depth**" (**DiD**) approach using multiple security techniques to help mitigate the risks.

Conceived by the **National Security Agency (NSA),** this approach layers the network with security features, appliances, and processes.

The defence in depth approach utilises six layers of defence for a **PlantStruxure** network:



Schneider Electric Cyber Security Defence (cont.)

1.	**Security Plan**	Creating the security plan is the first step to secure the control system network. Policies and procedures must be defined, implemented and most importantly updated and maintained. The planning process involves perform a vulnerability assessment, mitigating the risk and creating a plan to reduce or avoid those risks.
2.	**Network Separation**	Physically separating the control system network from other networks, including the enterprise, by creating demilitarised zones (DMZs).
3.	**Perimeter Protection**	Preventing unauthorised access to the control system through the use of firewall, authentication and authorization, VPN (IPsec) and anti-virus software. This includes remote access.
4.	**Network Segmentation**	Use VLANs to sub-divide the network providing containment in the event of a security breach within a subnet. It can be further enhanced using the concept of communication zones. Each zone would be buffered from other zones by use of a security firewall to limit access, monitor communications and report incidents.
5.	**Device Hardening**	**Device hardening is the process of configuring a device to protect it from communication based threats. It involves password management, access control and disabling all unnecessary protocols and services.**
6.	**Network Monitoring**	No network is 100% secure due to the constant evolution of new threats. Constant monitoring for control network system is necessary to block intruders before damage is done.

The remainder of this document focuses mainly on item **5** - the **Device Hardening** elements of this approach to configure a **PlantStruxure** system that is less susceptible to cyber attacks.

See Also:

For detailed information on the **Defence-in-Depth** approach, refer to the **TVDA**: *How Can I Reduce Vulnerability to Cyber Attacks in the Control Room* which is available from the **Schneider Electric Virtual Campus http://industry.vcampus.schneider-electric.com/psx/resource-centre/tvdas-and-stns/download-tvdas:** (requires a User Name and Password) [Search for '**Cyber**']

See Also:

For general information and further free advice on **Cyber Security** refer to the **Schneider Electric Blog http://blog.schneider-electric.com/cyber-security/:** (requires a User Name and Password) [Search for '**Cyber Security**']

Cyber Security Defence (cont.)

Certifications

Schneider Electric developed its **Cyber Security** guidelines based on the following recommendations:

- Achilles
- ISA Secure

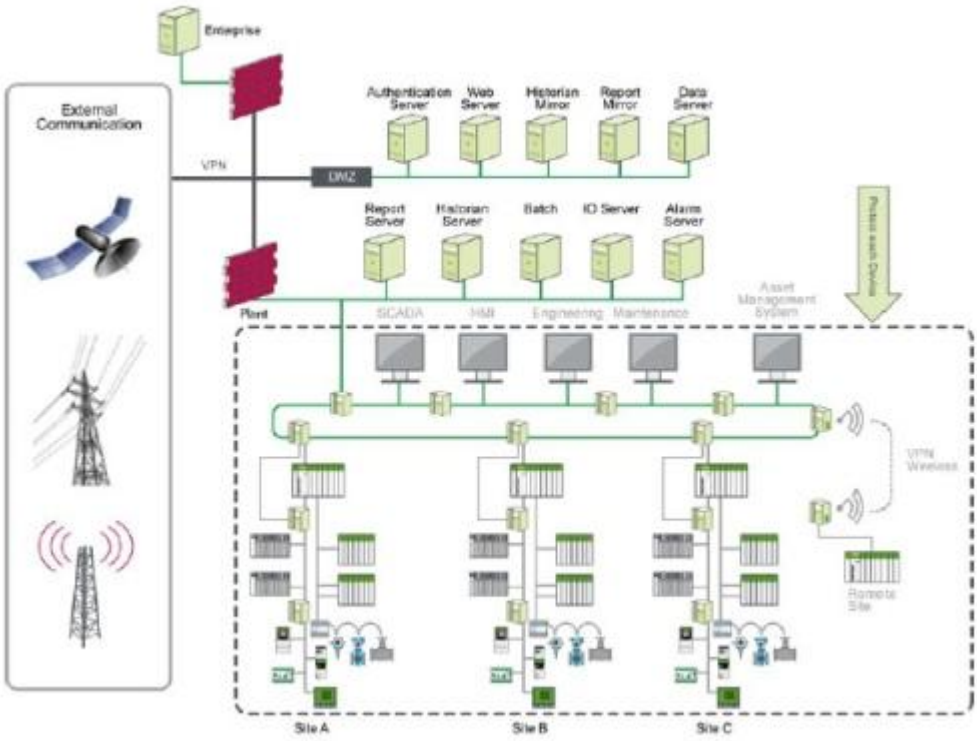
Note:

To submit a **Cyber Security** questions, report security issues, or get the latest news from **Schneider Electric**, visit our website: **www.schnedier-electric.com**.

Cyber Security Defence (cont.)

Device Hardening

Device hardening is a process that reconfigures a device's default settings in order to strengthen security.



Device hardening applies to routers, firewalls, switches and other devices on the network of SCADA and PAC systems.

Examples of device hardening are:

- **Password Management** including encryption
- Disabling of unused **Services**
- System **Access Control**
- Network intrusion detection systems (NIDS)
- Strong authentication

The following chapter describes how to configure the first three of these aspects namely **Password Management, Services Control** and **Access Control** together with specific **Change Management** for **Unity Pro**.

Chapter 2: Cyber Security Configuration

Overview

Introduction

This chapter provides guidelines on configuring some of the **Unity Pro** parameters in order to optimise the overall security of an existing system based on simple features or programming rules.

Some of these parameters can be configured independently of each other but it is recommended that they are combined together to improve the security level of the system architecture.

Chapter Objectives

By the completion of this chapter you will be able to:

- Review aspects of **Unity Pro** in order to harden security against unauthorised actions

This Chapter Covers These Topics:

- Password Management 2-2
- Services Control 2-7
- Access Control 2-8
- Change Management 2-11

Password Management

Introduction

Password Management is one of the fundamental tools of device hardening. It is the simplest process of configuring a device against communication-based threats.

It can be easily and quickly implemented but is often neglected in a control system network, where password policies and procedures are often lacking or missing entirely.

However, caution must also be taken when considering security requirements and the potential ramifications (i.e. performance, safety or reliability could be adversely impacted).

Schneider Electric Limited recommends the following password management guidelines:

---

1 Enable password authentication on all email and Web servers, CPUs, and Ethernet interface module**s.**

2 Change all default passwords immediately after installation, including those for**.**

- User and application accounts on Windows, SCADA, HMI, and other systems.
- Scripts and source code.
- Network control equipment.
- Devices with user accounts.
- FTP servers.

---

1 Grant passwords only to people who require access**.**

2 Prohibit password sharing**.**

3 Do not display passwords during password entry**.**

- Require passwords that are difficult to guess. They should contain at least 8 characters and should combine upper and lower case letters, digits, and special characters when permitted.

---

1 Require users and applications to change passwords on a scheduled interval**.**

2 Remove employee access accounts when employment has terminated**.**

3 Require different passwords for different accounts, systems, and applications**.**

4 Maintain a secure master list of administrator account passwords so they can be quickly accessed in the event of an emergency**.**

5 Implement password management so that it does not interfere with the ability of an operator to respond to an event such as an emergency shutdown**.**

6 Do not transmit passwords via email or other manner over the insecure Internet**.**

Password Management (cont.)

Password Setting (cont.)

Some general guidelines are:

- Default passwords must be changed immediately after installation:
  - User and Application passwords
  - Scripts & source code
  - Network Control equipment
  - All user accounts must have passwords.
- Limit passwords to people that need access.
- Passwords should not to be shared and be difficult to guess.
- Passwords should contain at least 8 characters and contain:
  - Upper and lowercase letters
  - Numbers
  - Non-alphanumeric characters (e.g. !, $, #, %)
- Passwords should be changed regularly.
- Remove employee's access account when employment has terminated.
- Use different passwords for different accounts, systems and applications.
- There needs to be a master of all passwords at all times in the plant that can quickly be accessed in the event of an emergency that is secured.
- Password implementation must never interfere with the ability of an operator to respond to a situation (e.g. emergency shut-down).
- Passwords should not be transmitted electronically over the insecure Internet, such as via e-mail.

Password Management (cont.)

Unity Pro Passwords

When an application in **Unity Pro** is configured, a viable password should be created.

1 Choose a password that contains alphanumeric characters, and is case-sensitive. **Unity Pro** encrypts the password, and stores it in the application.

2 Choose a password that contains a minimum of 8 characters.

3 Choose a password that is difficult to guess.

- **The password should combine upper and lower case letters, digits, and special characters.**
  - When the user opens an existing application, the **Application Password** dialog box opens.
  - Type in the password, and click **OK**.

Application Password Amendments

To create or change the **Unity Pro** application password, follow these steps:

1 **Right-click** the ***project name*** **Properties** in the **Project Browser.**

Result: The **Properties of Project** dialog box opens**.**

2 **Click** the **Protection** tab**.**

3 In the **Application Field**, click **Change Password.**

Result: The **Modify Password** dialog box opens**.**

4 To enter a **New** password, type the password in the **Entry** field. Retype the password in the **Confirmation** field, and click **OK.**

5 To change an ***existing*** password, type the current password in the **Old** password field. Type the **New** password in the **Entry** field. Retype the **New** password in the **Confirmation** field, and click **OK.**

6 In the **Properties** of **Project** dialog box, click **Apply** to save the changes, or click **OK** to save and close.

Password Management (cont.)

Removing Application Passwords

To remove the **Unity Pro** application password, follow these steps:

1	Right-click the **project name >** Properties **in the** Project Browser**.** Result: **The** Properties **of** Project **dialog box opens.**
2	Click **the** Protection **tab.**
3	**In the** Application **field, click** Clear **password.** Result: **The** Access Control **dialog box opens.**
4	**Type the password in the** Password **field, and click** OK**.**
5	**In the** Properties **of** Project **dialog box, click** Apply **to save the changes, or click** OK **to save and close.**

Password Management (cont.)

Auto Lock Feature

Follow these steps to establish the amount of time that a password is required to activate a locked application.

1 Right-click on the `Project Name > Properties` in the Project Browser.

Result: **The Properties of Project dialog box opens.**

2 Click the Protection tab.

3 In the Application field, select the Auto-lock check box.

4 Click the up / down arrows to select the desired number of minutes before a password is required to unlock a locked application.

5 In the Properties of Project dialog box, click Apply to save the changes, or click OK to save and close.

Resetting Passwords

A **maximum** of *3* attempts is allowed for correct entry of **Unity Pro** or **PAC Application Passwords**.

Follow these steps to reset a forgotten password:

1 When the **Application Password** dialog box opens, press **Shift + F2.**

Result: A ***greyed number*** (e.g.: 57833) appears in the dialog box**.**

2 Contact the local **Schneider Electric** customer support.

Give this ***greyed number*** to the support representative.

3 Type the **Temporary Password** in the **Application Password** dialog box that customer support provides**.**

4 **Modify** the **Temporary Password.**

5 Click **Build > Rebuild All Project.**

6 Click **Save.**

Services Control

Unused Service Deactivation

One method of device hardening is to implement **Services Control** on the Schneider Electric devices.

In any application it is good practise to deactivate any service that is not needed for a particular system, since these unused running services are prone to mimicking from malware as they are relatively hidden within a system.

- **How To:** Deactivate and Activate Services in a Unity Pro application.

1 When the FTP, TFTP and HTTP services are not required at run time.

Disable these services within **Unity Pro** as shown below.

Note:

The only way to reactivate these services is to load a new **Unity Pro** configuration.

2 When the FTP, TFTP and HTTP services are required at run time.

As these services are required for web pages, Faulty Device replacement, data storage or firmware upload load.

Configure the required service(s) as 'Enabled' in **Unity Pro**.

Hints & Tips

The status of a service can be controlled via an input or via an unlocated variable (**No located variable**).

Services can also be run only when needed using the '**EthPort_Control_MX**' function block.

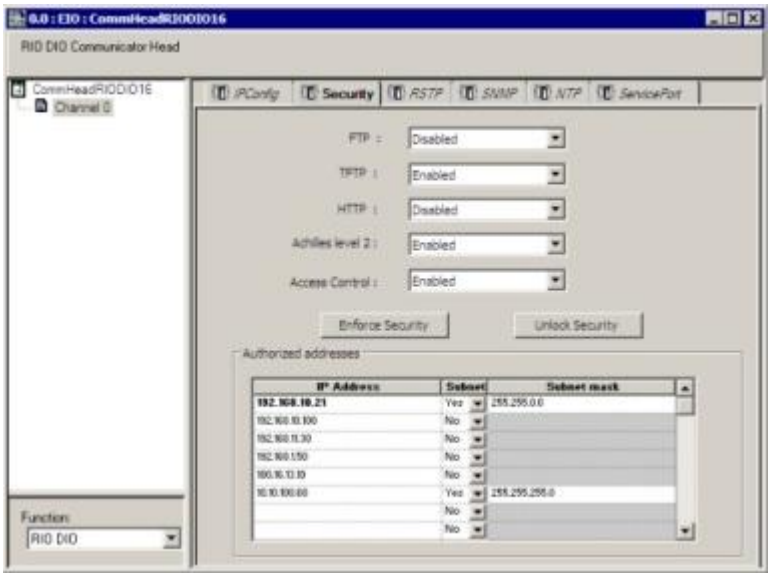
Access Control

Device Access Control

Another method of device hardening is to implement access control on the Schneider Electric devices.

Access control is similar to IP packet filtering in a firewall. Only permitting access to the addresses entered in the access table. It is useful to prevent access from one plant area to another.

- **How to:** Configure Access Control to determine whether or not a device is allowed to open a TCP connection to the module.

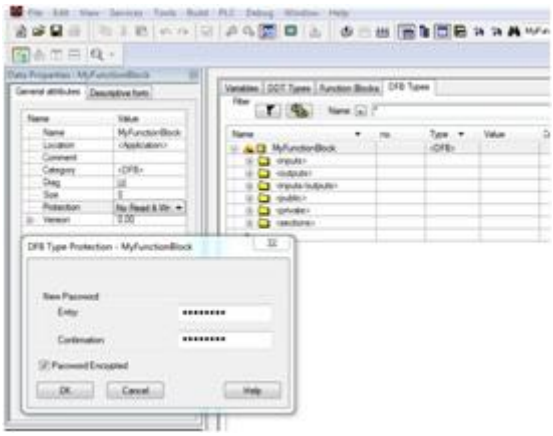


Access Control (cont.)

Function Block Protection

A further method of device hardening is to restrict access to the **Read** and **Write** actions of the **Source Code.**

- **How To:** In **Unity Pro** any Function Block, section or event task can be password protected.



The options are as follows:

- **No Read & Write** - Source Code is NOT visible without authentication.
- **No Write** - Source Code is visible but cannot be modified.

Note:

This functionality requires a password per DFB and a **Global Password** if enabling all sections.

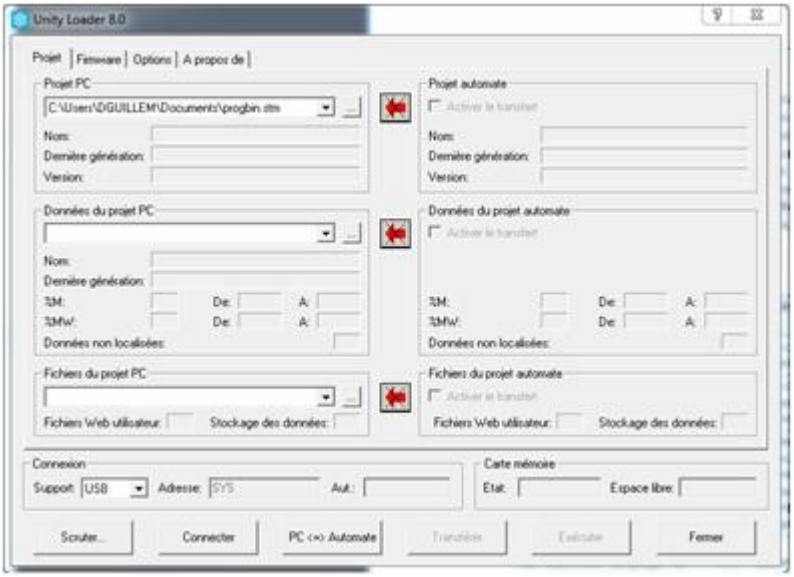
These passwords can also be encrypted.

Access Control (cont.)

Unity Loader

A final method of device hardening the **Unity Pro** application is to use the **Unity Loader** tool.

This tool manages raw binary files (called STM Files) , without the use of **Source Code**.



STM files contain only binary files required for execution in a PLC and do not contain any source code and hence cannot be read by any application software including **Unity Pro**.

Note:

This tool is available to all platforms.

Change Management

Security Editor

The **Security Editor** options of **Unity Pro** configure the access rights of **Users**.

These control who is authorised to carry out actions such as **Adjust, Debug and Operate**.

The **Audit** feature enables the tracing and logging of **User** actions.

Note:

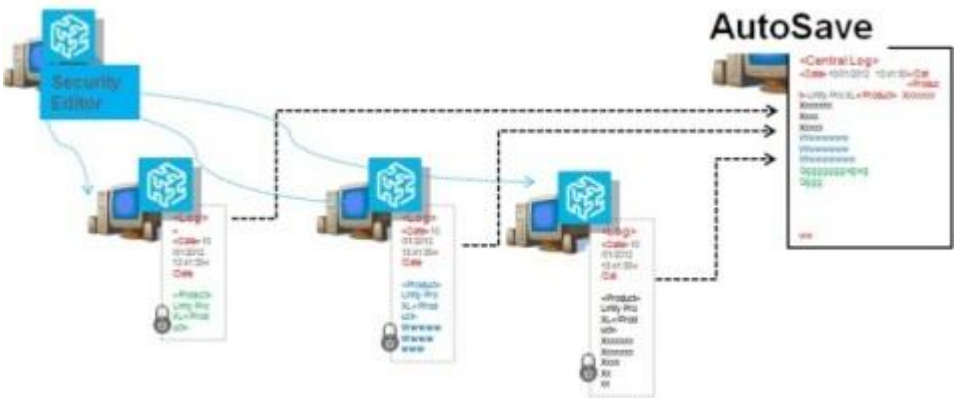
Security Editor enables the centralisation of **User Actions** into syslog databases.

Change Management (cont.)

Server Security

A flexible and more secure system for the traceability of **PLC** application updates is to use encrypted textual Log files.

Security Editor on Server



Note:

These features are only available as a global solution for **Unity Pro v8.0** and require the **AutoSave** software package from our CAPP partner MDT Software.

Please contact the **Schneider Electric** sales representative for more information.

Change Management (cont.)

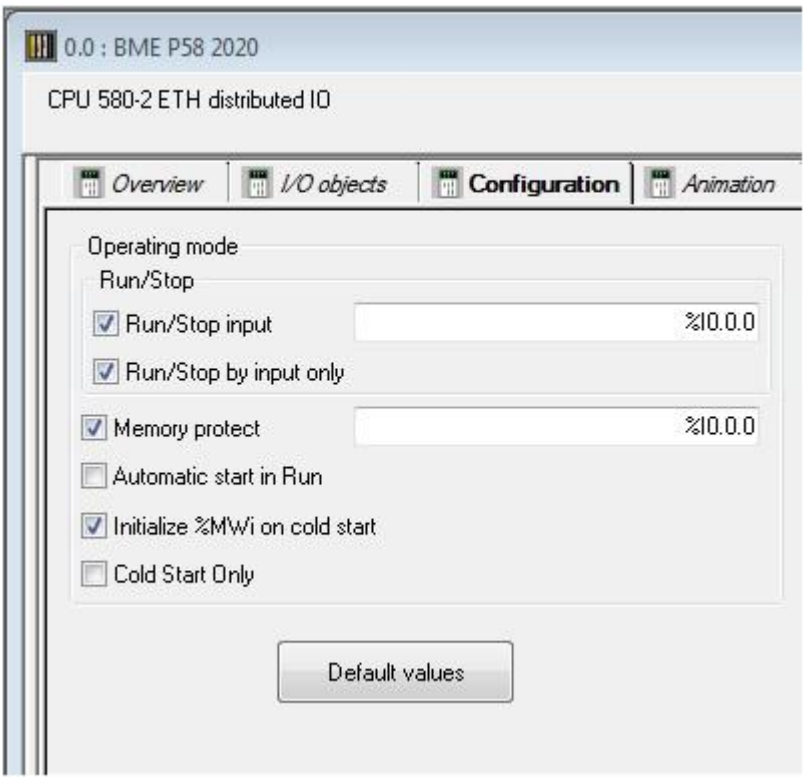
Run/Stop Replay Prevention

The goal is to protect against unauthorised **RUN/STOP** replay attacks

The following three steps are recommended to enable Run/Stop Replay prevention:

- Check '**Run/Stop input**'
- Check '**Run/Stop by input only**'
- Configure the input which will prevent **RUN/STOP** requests

Any remote **RUN/STOP** request will be rejected.

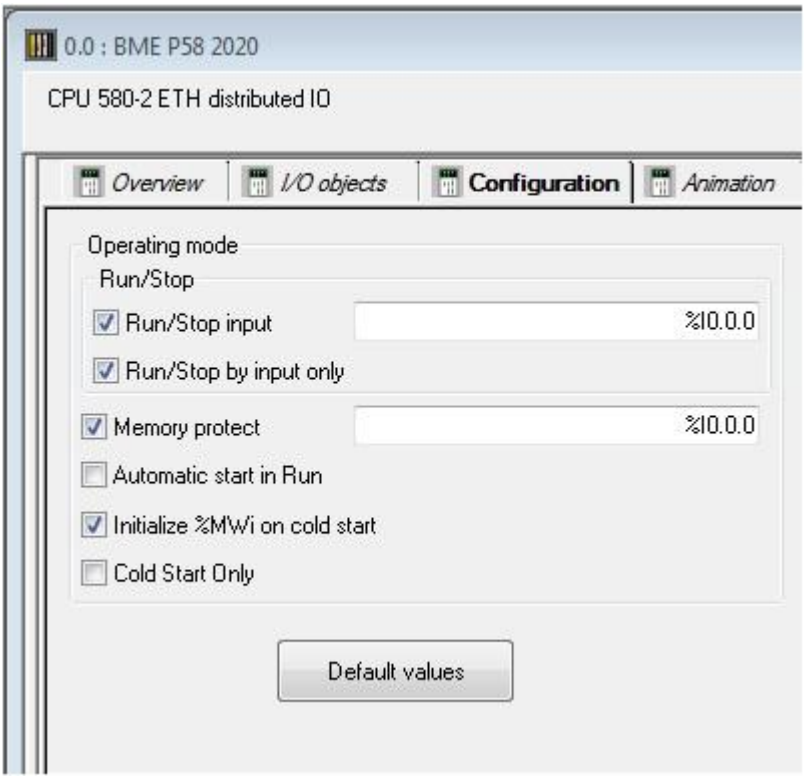


Change Management (cont.)

Memory Protect

The Memory Protect option controls the authorisation of changes within the PLC, dependent upon the value of the configured input.

Any requests other than Read/Write are rejected.



To configure ‘Memory Protect’ features

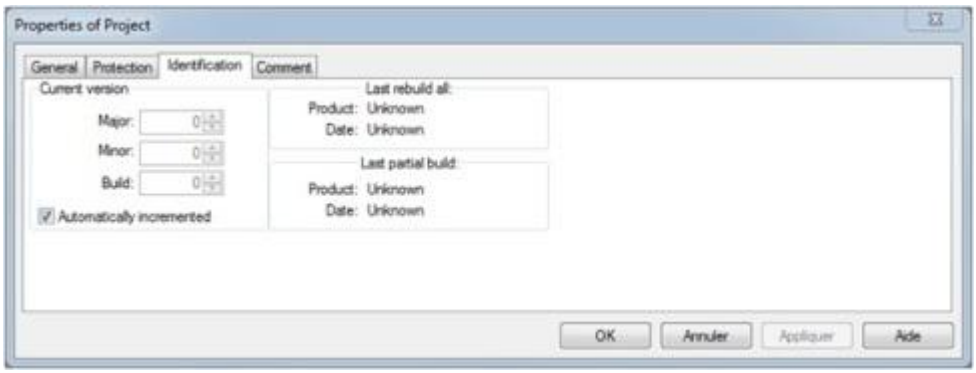
- Check '**Memory protect**'
- Associate memory protect feature with a input

Change Management (cont.)

Application Version Control

Configure automatic incrementation of application version.

This allows any modifications of the application to be traced.



Select '**Automatically incremented**' checkbox.

Hints & Tips

It is possible to get the version of the project in the SCADA using the predefined OFS variable 'Appliversion'.

Note:

This applies to all versions of **Unity Pro**.

Chapter 3: Cyber Security Practicals

Overview

Introduction

This chapter provides exercises to configure **Unity Pro** parameters in order to optimise the overall security of an existing system.

Some of these parameters can be configured independently of each other but it is recommended that they are combined together to improve the security level of the system architecture, depending on the needs of each user.

Most of the items within this document apply to any of the **Unity Pro** hardware platforms. It will be mentioned when this is not the case.

Chapter Objectives

By the completion of this chapter you will be able to:

- Configure aspects of **Unity Pro** in order to harden security against unauthorised actions

This Chapter Covers These Topics:

- Source Code Control 3-2
- Unsolicited Connections..... 3-4
- Unity Pro Integrity Check 3-6

Source Code Control

Exercise - PLC Code Transfer Denial

➢ **How to:** Restrict unauthorised users gaining access to source code files from within the **PLC**

The following is recommended to prevent source code files being transferred from the **PLC** to the host computer (PC).

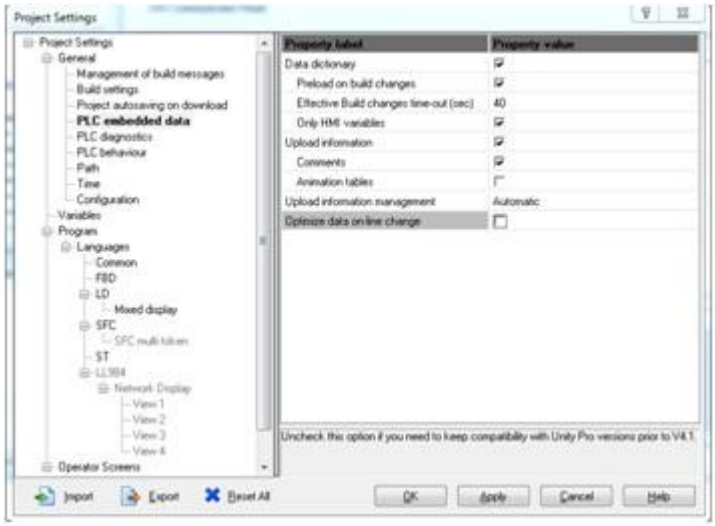
1 In `Project Settings » General » PLC embedded data`

The tick box '**Unload information**' can be enabled or disabled.

Hints & Tips

Here the term '**Upload information**' refers to **PLC Source Code**.

When '**Upload information'** is unchecked, only executables are stored in the **PC**.



Hints & Tips

To connect to a PLC from Unity Pro requires having program file (*.STU . . .) on the PC.

Note:

This applies to all **Unity Pro** platforms.

Note:

The **Program Viewer** web page requires **Upload** information to be enabled.

Exercise - PLC Variable Security

- **How to:** Restrict users' access to **PLC** data at run time.
- **How to:** Protect **PLC** data at run time against illegal read / write access.

The following is recommended to prevent data being accessed from within the **PLC** during run time.

---

1 In **`Project Settings » General » PLC embedded data`**

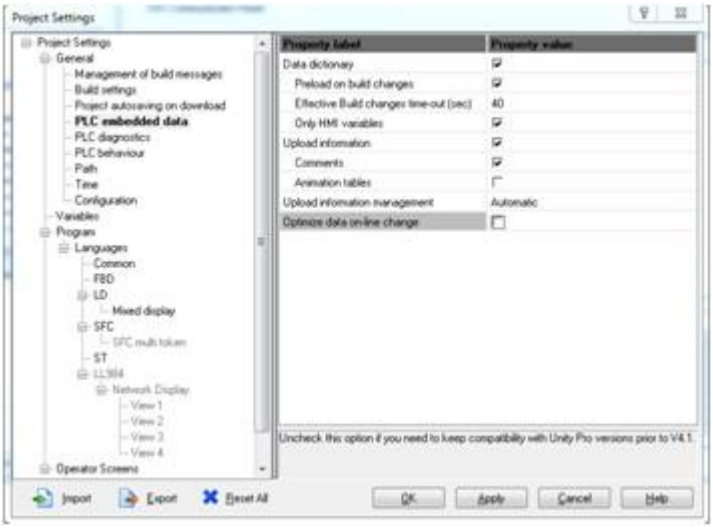
Whenever possible, use unlocated data.

---

2 Configure **Unity Pro** to store only **HMI** tagged variables.

3 Tag as HMI PLC variables which must be accessible from HMI or SCADA.

4 Connection with **SCADA** must rely on **OFS**.



Note:

Non tagged **PLC** variables are not accessible from external clients.

Unsolicited Connections

Exercise - Unsolicited Unity Pro Connections

- **How to:** Protect a **PLC** against unsolicited connections from **Unity Pro:**

An **Application Password** can be configured within **Project Properties**.

These passwords are stored within the **PLC**.

Any attempts to modify the **PLC** requires password authentication.

- No Application in PLC / Application without password in PC - **OK**
- Application with password in PLC / Application with password in PC (same password) - **OK**
- Application with password in PLC / Application with password in PC (different password) - **Not OK**
- Application with password in PLC / No Application in **Unity Pro** - **Not OK**

Unsolicited Connections (cont.)

Exercise - Unsolicited Modbus or EIP Connections

- **How to:** Protect from unsolicited Modbus or EIP remote requests

- Enable **Access Control**

  Result: Restricts access to PLC at run time, only from authorised IP addresses

Note:

The **Access Control** is only for **Ethernet IP** and **Modbus TCP** ports.

Unity Pro Integrity Check

About Unity Pro XL

Unity Pro v8.0 and above runs an integrity check of all of its required **.exe** and **.dll** files on startup.

This check can also be manually performed from the `Help » About` drop down menu.

Exercise - Unity Pro XL Integrity Check

Learning Outcomes

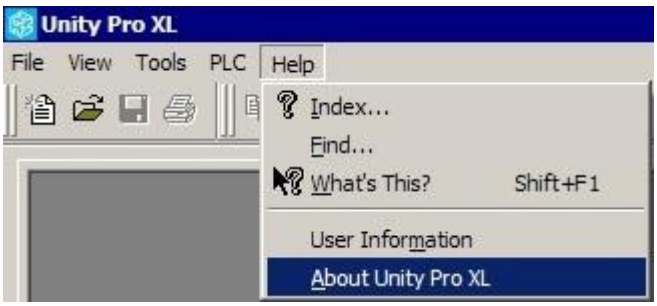
By the completion of this exercise you will:

- Learn how to check the integrity of the **.exe** and **.dll** files within **Unity Pro XL**.

1 Once **Unity Pro XL** has been launched, carry out the following:

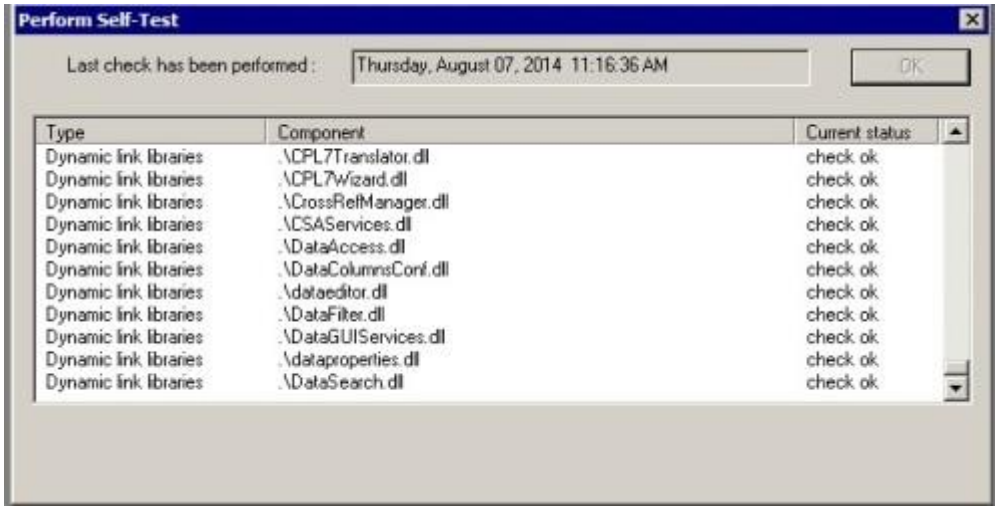
a Select the drop down **Help** menu.

b Select **About Unity Pro XL.**



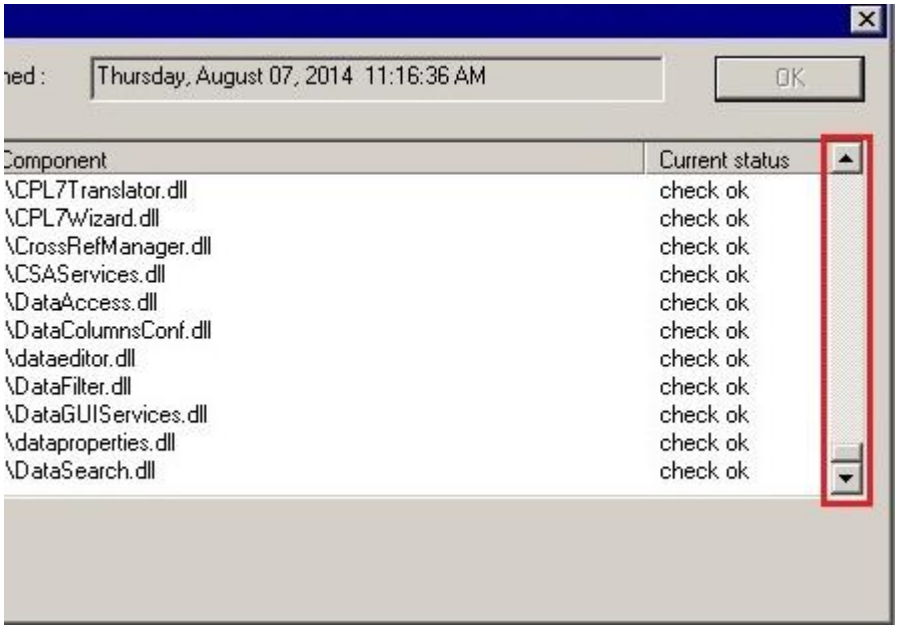
c In the **About Unity Pro XL** message window, select **Perform self-test.**

d The **Self-Test** output window is then seen and the list of files being tested populates the centre section of the window.

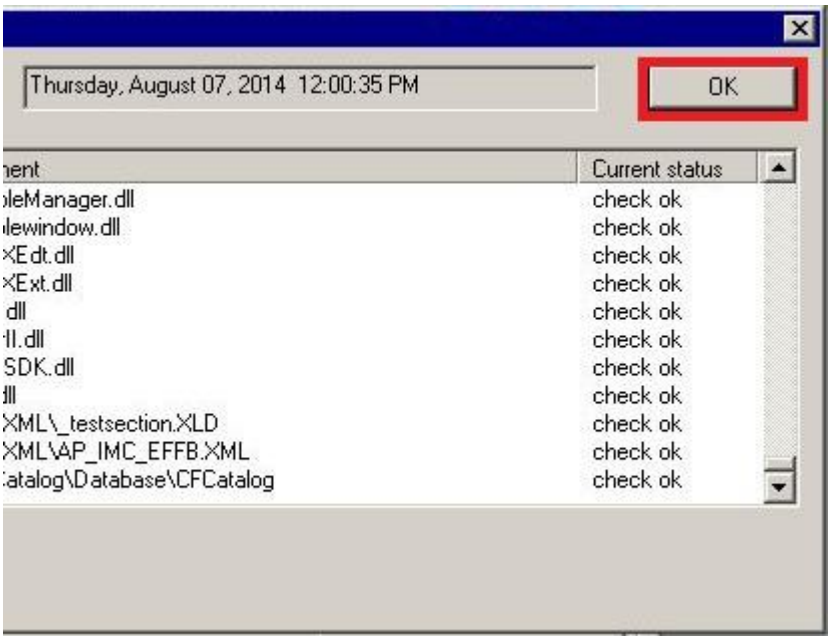


Integrity Check (cont.)

e The list of tested **.dll** and **.exe** files can then be scrolled to verify that their status has been set to **check ok**.



f Once this list has been verified then the **Self Test** output window can be closed by selecting the **OK** button.



Exercise - Unity Pro XL (cont.)

Integrity Check (cont.)

g Finally the **About Unity Pro XL** window can also be closed by selecting the **X** in the top right hand corner.

Further Training:

An eLearning module entitled **Unity Pro XL v8.0 Integrity Check** is also available explaining this procedure**.**