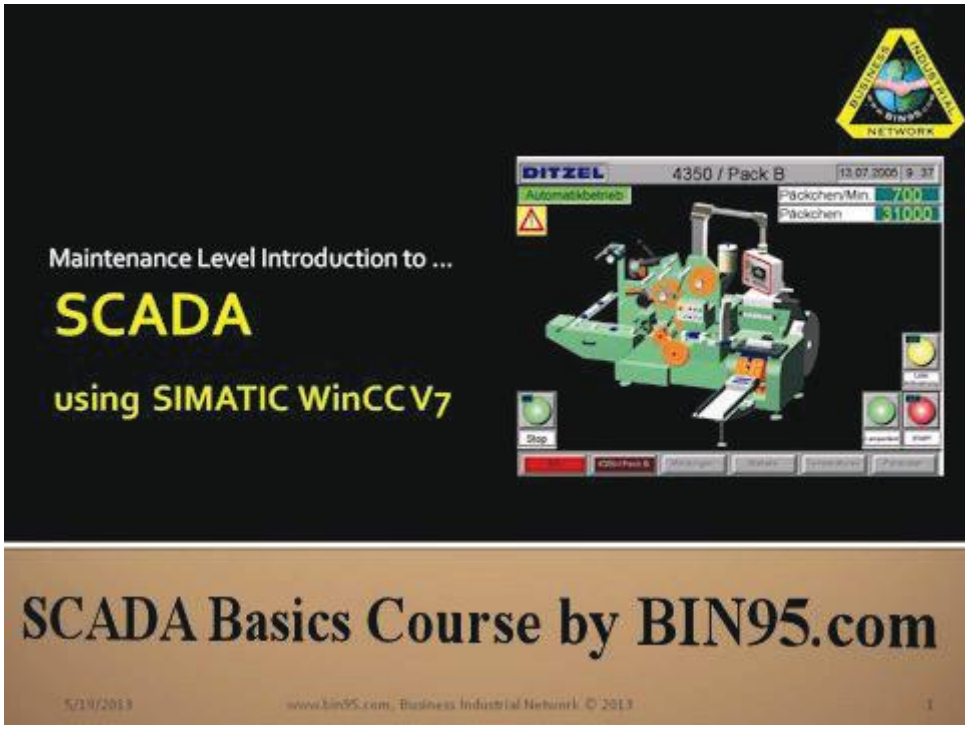
To download this SCADA course, please visit …

http://bin95.com/scada_tutorial_siemens_automation.htm

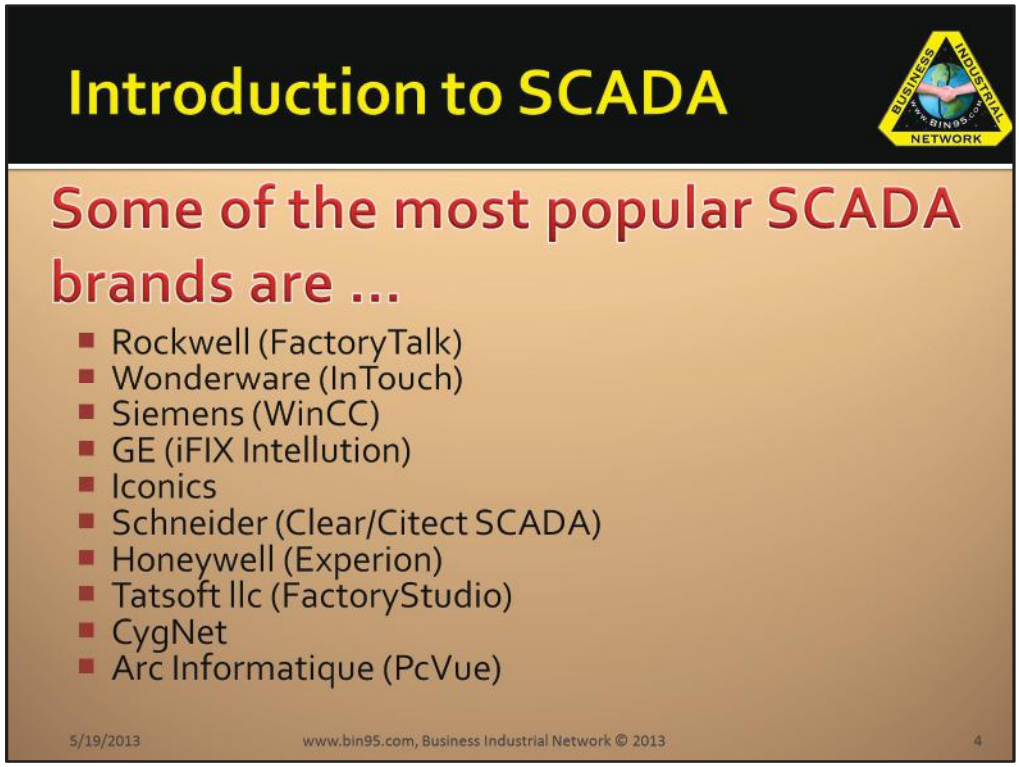


BY

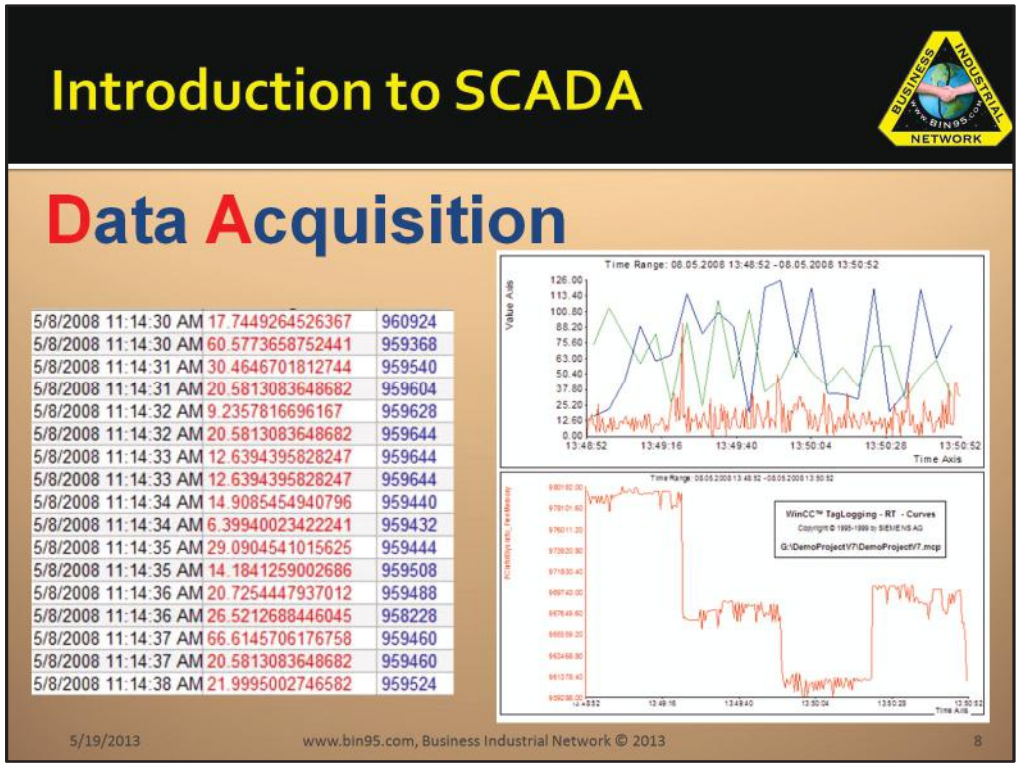
Business Industrial Network

- Introduction to SCADA
- What is WinCC?
- Creating a new project in WinCC on a single standalone PC
  - Creating tags
  - Creating a connection to a PLC (using S7-PLCSIM simulator)
  - Using the Graphics Designer
- Configuring alarms and displaying them
- Industrial Network Security

SAMPLES BELOW



These brands are the 10 most popular we found from our survey. But it should be noted depending on what industry and what country the brand popularity varies due to sales focus of each individual SCADA vendor. Some examples, FactoryTalk is most popular in USA manufacturing where WinCC is more popular in UK and in refinery processes. Intellution is popular in building and facility control. (*In addition to this training course, it is advised you get training on particular brand you believe you will be working with from the vendor of that SCADA too. So you can get more familiar with specifics to the particular brand of SCADA before attempting to navigate the software and work with that particular brand of SCADA software*. As SCADA is not just another software package, it connects to real-world equipment and mistakes have real world safety consequences.)



Data Acquisition is the taking of values from the process and storing them on the computer's hard drive. The date and time that a value is read from the process are also stored. In this way, old data history can be viewed at a later time as a table of values, or as graphs that can display the history of the values, making it easier to see and interpret.

Other terms for data acquisition are trending and logging. WinCC is capable of Data Logging, which is the saving of data to the hard drive, and Alarm logging, which is the saving of alarm messages to the hard drive.

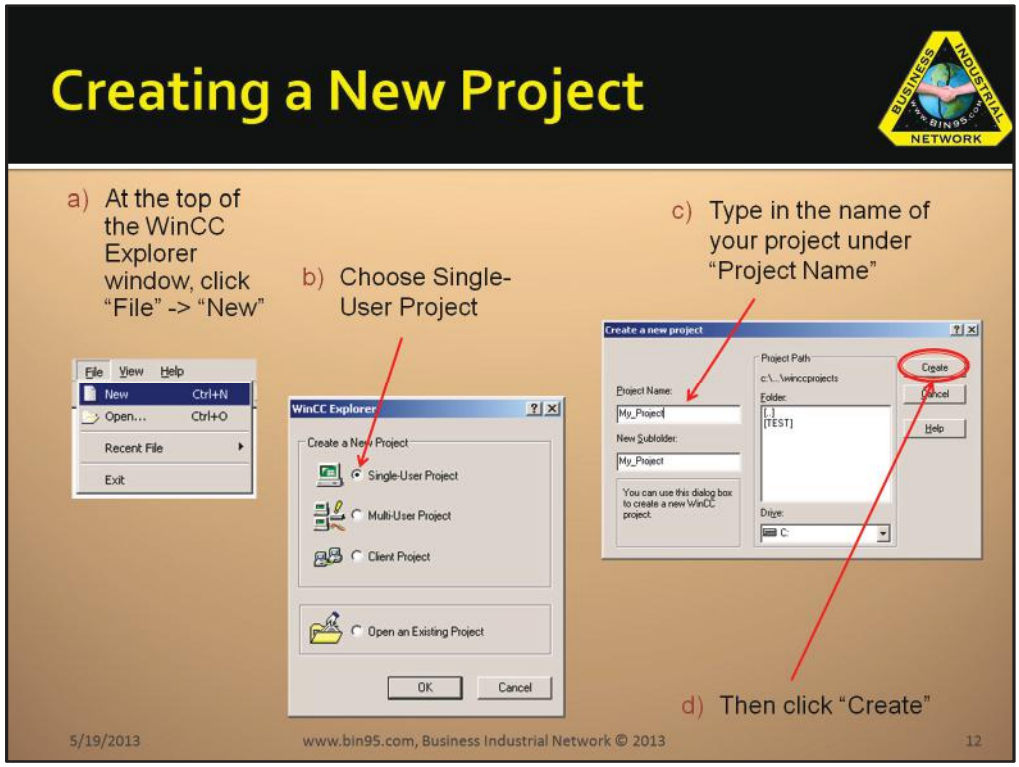
There are generally 3 types of logging: cyclic driven, event-driven, and a hybrid of both.

Cyclic driven logging means that every specified amount of time (ex: per second), the value of a tag is saved into a file as a record (ex: saved into a database or CSV, Comma Separated Values file).

Event-driven logging mean that a value is recorded on a change of another value or command (ex: when another tag value changes to 1).

A hybrid of both cyclic and event-driven logging can be that the value is recorded cyclically while another bit value is on (ex: while the burner is on, record the temperature every minute).

[Now is a good time to take a break] and next do the online ***SCADA Training Test 1*** *at* http://bin95.com/plc-scada-training-online.htm



After WinCC Explorer has started, you will create a WinCC project. The types of projects possible are:

Single-User Project	– a standalone project on a single computer
Multi-User Project	– a project on several computers (a server(s) with clients)
Client Project	– a project for a client computer, connecting to server(s)
Open an Existing Project	– to open a project already created

WinCC independently creates a unique project folder for each project created, and uses the MSSQL Server 2005 database as its storage of configuration information about the project.

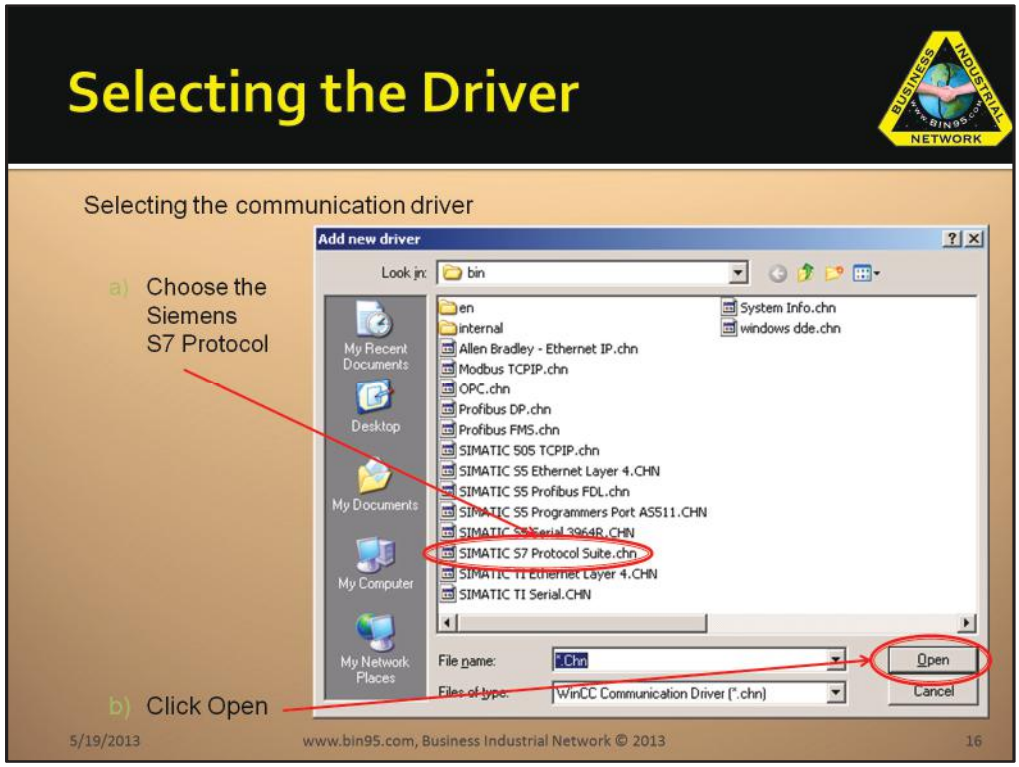
Whenever WinCC Explorer is opened again, the project last edited is called up.

The name of the project will also be the name of the new subfolder by default. You may leave this to be the same.

The default project path is:

C:\Documents and Settings\All Users\Documents\Siemens\winccprojects\<project path>\<project_name>.MCP

Where <project path> is your project subfolder, and <project name> is the name of your project. MCP is the file extension of the WinCC project.

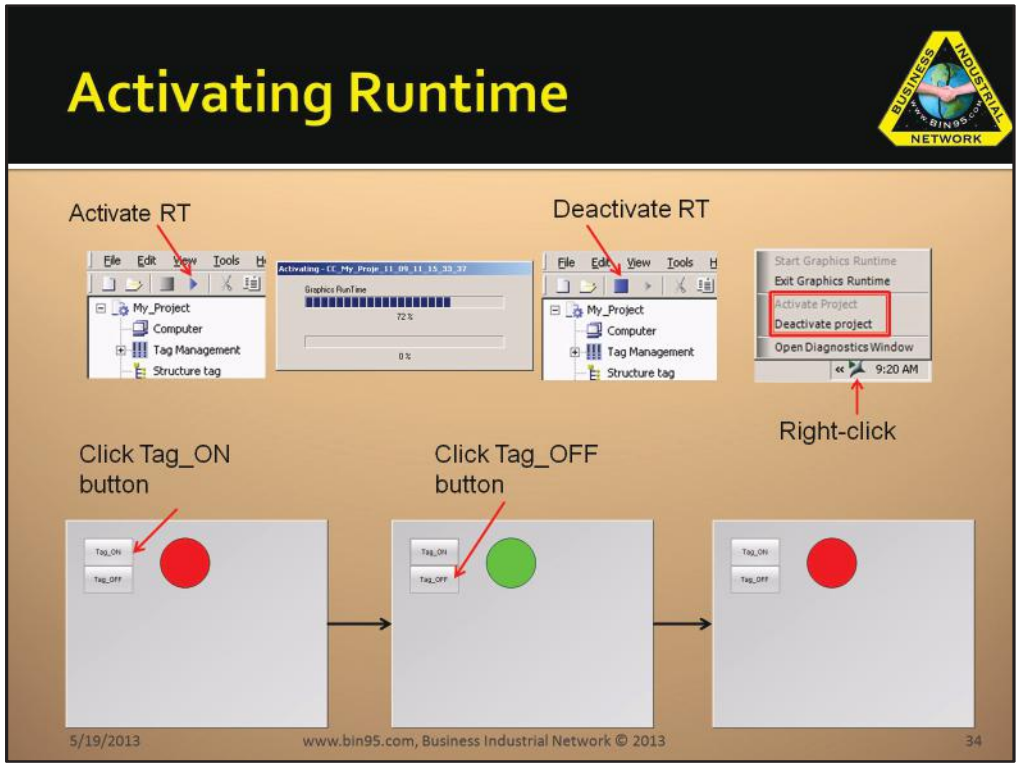


Select the **SIMATIC S7 Protocol Suite**, and click **Open**.

You can see here that there are other drivers available as well:

- Allen Bradley Ethernet/IP
- Modbus/TCP
- OPC (client – can be connected to an OPC server)
- Etc...

OPC is **O**LE for **P**rocess **C**ontrol, and OLE stands for **O**bject **L**inking and **E**mbedding. In basic terms, if there is a controller for which WinCC does not have a driver, an OPC server for the controller which has the driver can be purchased. WinCC has the OPC client driver built-in, and therefore can communicate to the OPC Server, which in turn communicates to the controller. Tags would normally be created in the OPC Server, then those names would be referenced as tags in WinCC.



Runtime is the execution engine of the developed project.

There are a couple of ways to activate the current project runtime.

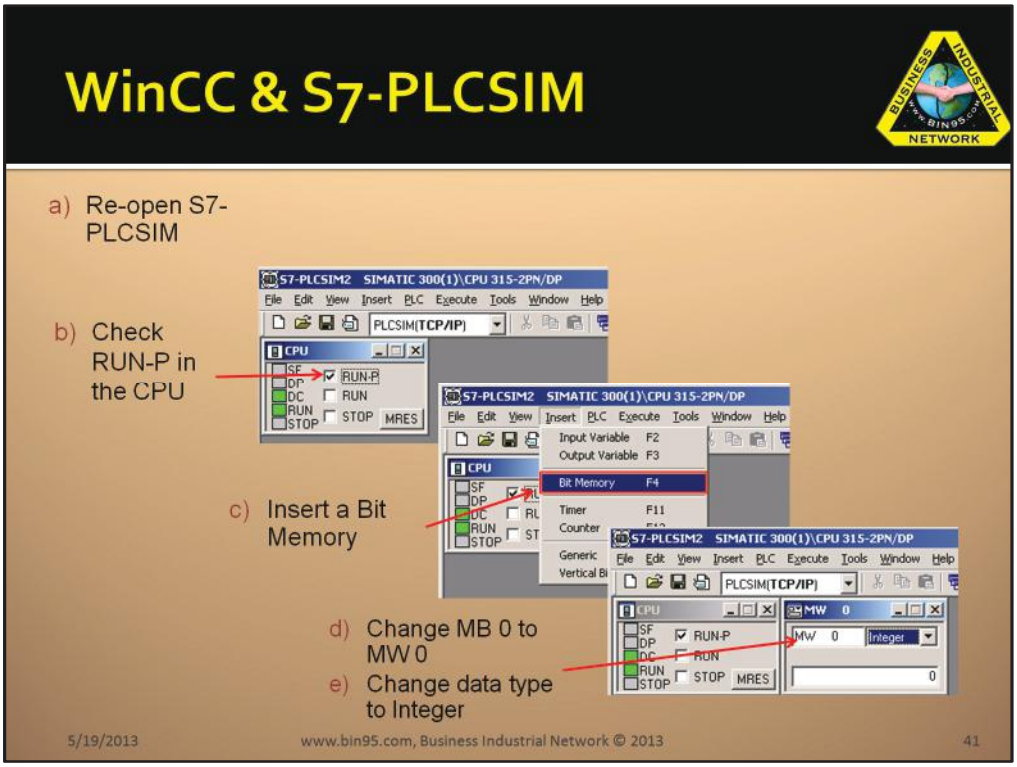
1) Click the “play” button (with a blue triangle – see above)
2) Right-click on the WinCC icon beside the Windows clock, and Activate Project

To deactivate:

1) Click the “stop” button (with a blue square – see above)
2) Right-click on the WinCC icon beside the Windows clock, and Deactivate Project

After activating the runtime, the runtime window appears, and the graphics picture you developed is displayed, because it is defined as the start picture. Initially the circle is red in color. When you press the Tag_ON button, the action defined on the button is told to make the value of Internal_Tag1 equal to 1. Consequently, the dynamic display property set for the background color of the circle tells it to change to green when Internal_Tag1 is equal to 1.

Thus control is achieved by the pushbuttons, and supervision (visualization) is displayed by the circle.



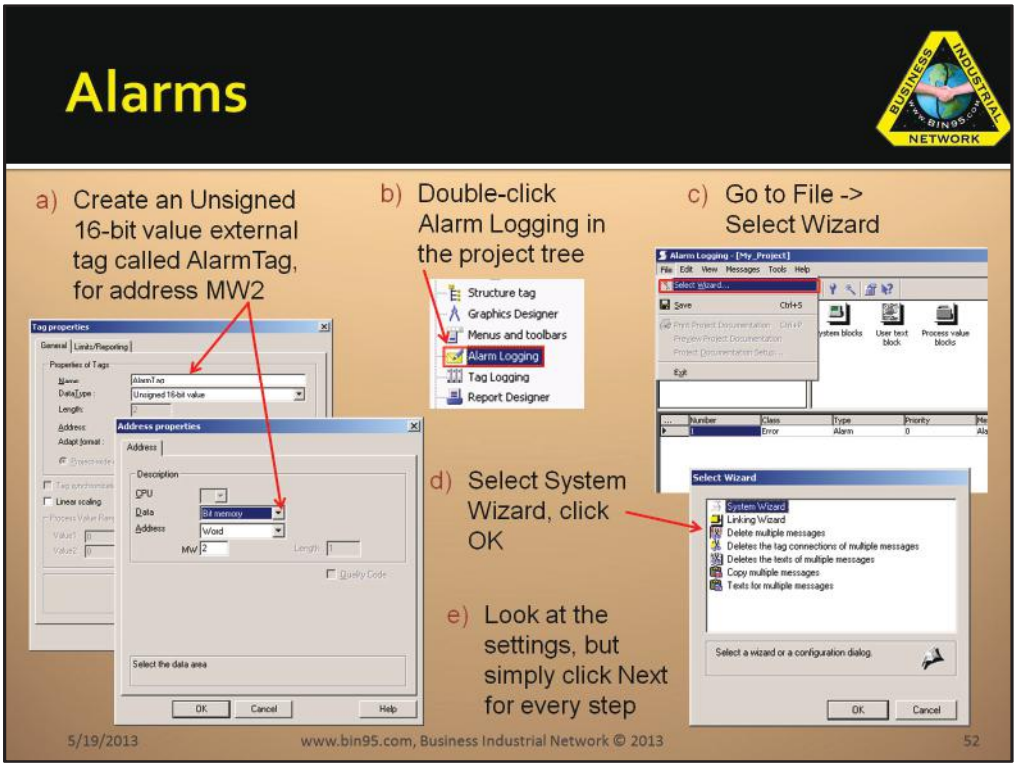
Re-open the S7-PLCSIM window, and place the CPU in RUN-P mode. This is the same as toggling the RUN-STOP switch on an S7 PLC. If you wish to monitor and modify values in the S7-PLCSIM, you insert variables using the Insert menu. The options are:

Input Variable (I)
Output Variable (Q)
Bit Memory (M)
Timer (T)
Counter (C)
Generic (can be any of the above, or peripheral input (PI) or output (PQ), or data block (DB))

Vertical Bits field (the above variables display bits horizontally)

In our case, we created a WinnCC Tag called "My_Tag1" with the address MW 0. This Means we can set up WinnCC to communicate to the S&-PLCSIM, and test the runtime with the PLC simulator now.

[Now is a good time to take a break] and next do the online ***SCADA Training Test 6*** *at* http://bin95.com/plc-scada-training-online.htm

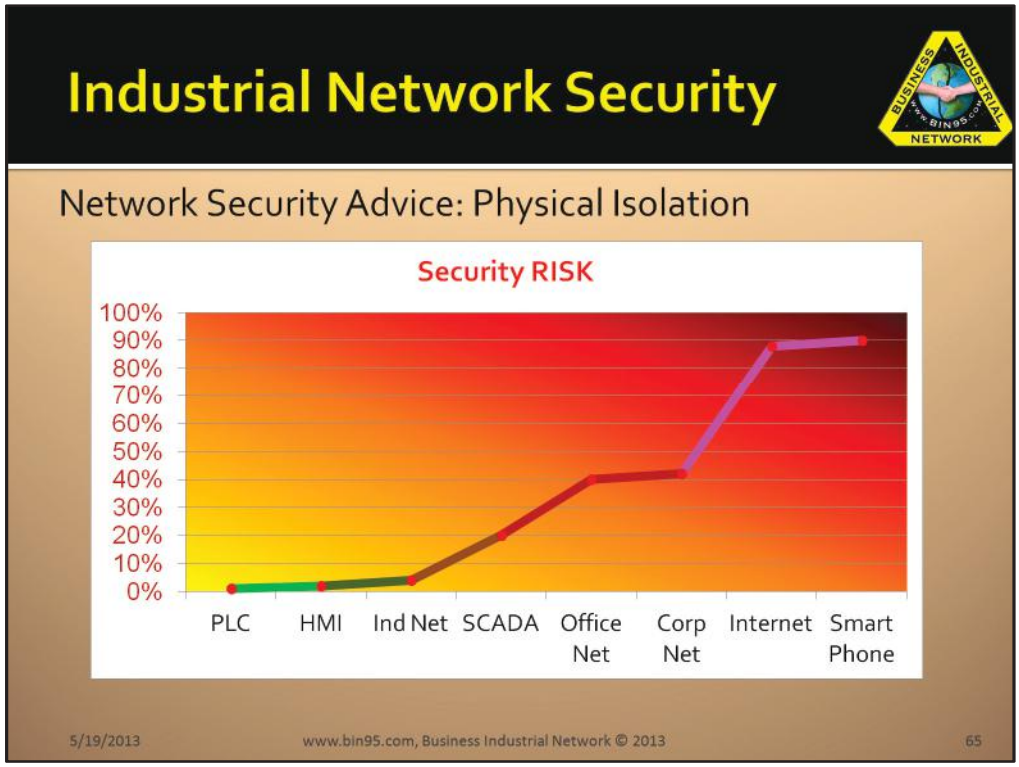


Alarms are used to signify to the operator that there is something in the process that requires attention.

What is typically done, is that the PLC code will set a bit based on the logic preceding this bit. For example, the temperature of an oven is measured to be above 300 degrees Celsius. So a comparison instruction is used in the PLC to compare the current temperature of the oven to 300 degrees Celsius. When this happens, a bit is set. In WinCC, we define an external tag to read a word (which is 16-bits), and the bit described in our example will be inside these 16-bits. Therefore, WinCC will read the 0 or 1 value of this bit. If the value is a 1 in our case, the oven temperature is too high, and this is an alarm condition, and the operator needs to be alerted.

The Alarm Logging feature in WinCC is used to define the tag(s) that causes the alarm condition, and the text to be displayed for the alarm.

First, a tag is defined for the alarm bits, as shown above. Then the Alarm Logging Wizard is started to apply settings.



Security risk is greatly reduced by isolation. Within software and operating systems, the isolation methodology is used, but with minimum effectiveness, thus we still get viruses and hacked. But physical isolation can result in near 100% secure industrial equipment at the cost of reduced networking capabilities. Below is some *arbitrary* percentages to make a clear picture of exponential risk increase as we network our industrial equipment and as those networks grow. One should always first weigh out the Risk/Benefit comparison before networking or expanding networks.

<1% Risk **PLC Only** (Lacking best practice PLC training and management virtually only risk. No network, virtually no risk)
<5% Risk **HMI** (With no networked HMI, like local touch screens. Risk increases if HMI on commercial PC with standard consumer operating .....system like Windows. Greater risk of person connecting infected laptop to HMI.)
>8% Risk **Industrial Network** (even less if proprietary network protocol like Allen Bradley DH+, but still risk mentioned above under PLC/HMI)
>20% Risk **SCADA** (Same risk as home PC as SCADA is just a software program on a PC. Some say a little more risk because hacker would be more interested in an industrial system than your personal computer. Includes all risk above too including management policies that would otherwise limit access and educate employees of safe computer practices.)
>40% **Office Network** (Double the risk above as it opens network access to a larger physical location and number of people. Especially if office network knowingly or not gets connected to a larger network. Commonly the Internet would be an example, but also seen office employee set up wifi to access network at home near plant. Best to have industrial network physically separated from office network.)
>42% **Corporate Network** (A little more riskier than stand alone network, only because risk are more commonly known and mitigated on corporate networks. It increases slightly because number of people who can access and greater risk some may not be properly training on industrial controls. And it increases a little bit more because of access points between to physical locations can be infinite.)
>88% **Internet** (Obviously access becomes world wide, but also visibility becomes greater which increases risk slightly. Satellite private network should be used if authorized global access is needed.)
>90% **Smart Phones** (The riskiest of all because of portability of physical device, accidental operation and ease of theft. If the benefits outweigh the risk in rare occasions, only monitoring functionality should available and strict control by management of smart phone with application installed should be enforced. Don't allow someone to vacation in a foreign country with SCADA app on their personal phone. Remove it and reinstall when they return.
NOTE: *All of the above networks can be implemented and managed with minimum risk if above considerations are taken and they are constantly re-evaluated and effectively managed.*

PLC and SCADA course Certificate (*Recommended 4.2 CEUs*)

REQUIRMENTS:

- Email copy of PLC Training Certificate
- Complete all test at https://bin95.com/plc-scada-training-online.htm
- Complete training task on slide 70