Troubleshooting PLCs & SCADA Systems

By

Steve Mackay
Recognition, endorsement and/or accreditation from:

- National Recognised Training
- Training Accreditation Council
- IET
- ACPET
- SAIMC
- Engineers Ireland
- IEEE
- Project Management Institute
- Institute of Measurement and Control Computer Company

Welcome to the Engineering Institute of Technology (EIT)

The Engineering Institute of Technology (EIT) provides endorsed engineering Diplomas and Certificates (Masters Degrees accreditation pending), designed for students working in industry who need a practical, relevant education that is delivered efficiently. Our students work in the fast-moving engineering and technology fields where time is precious. They choose the EIT online delivery because it provides many of the benefits of live classroom based study without the inconvenience of travel. EIT courses are run by expert instructors who present in a friendly, interactive manner.

The EIT offers engineering Diplomas and Certificates (Masters Degrees accreditation pending) in the areas of:
Start recording!
EIT MicroCourse Series

- Every two weeks we present a 45 minute interactive course
- Practical, useful with Q & A throughout
- PID loop Tuning / Arc Flash Protection presented, so far
- Upcoming:
  - Functional Safety
  - Troubleshooting Conveyers and much much more.....
- Go to http://www.eit.edu.au/free-courses
- You get the recording and slides
"We are proud to present our new video-based eLearning platform designed for engineers and technicians."

Electrical Engineering (8 courses)

Electrical engineering is the science that studies the use of electricity and the equipment used to generate, distribute, and control it.

The short course videos form part of a professional development series and are designed to provide you with critical knowledge and practical tools that can be immediately applied to the workplace. They include lectured recordings and practical online materials that can be studied at your own pace.

"Complete professional development courses with ease, thanks to our brand new user-friendly platform."

Dr Steve Mackay, Dean of Engineering
The brand new, user-friendly IDC Video platform gives you exclusive access to high demand courses and offers you the following benefits:

- Self-Paced video courses with no completion deadline
- Try-before-you-buy: Free introductory course videos
- Achieve a ‘Certificate of Completion'
- Courses from US$99
- Track your course progress
- Lectured by industry experts
- Includes associated technical eBook and quizzes
- Complete professional development courses with ease
Objectives

• Quickly interpret, isolate and fix common hardware problems related to PLC input/outputs
• Troubleshoot PLC software
• Identify data communications problems
Topics

- Introduction to PLC
- Internal or External Problem
- Internal Problems
- External Problems - I/O and Comms
- Applications
- SCADA Troubleshooting
- Conclusion
Industrial Automation Skills

“Today’s Industrial Automation engineer and technician should be able to troubleshoot, identify, prevent and fix common PLC and SCADA problems.

If you have worked in industry, you are probably familiar with PLCs and SCADA systems and understand their basic operation.

You want to be able to quickly diagnose problems using your PLC software; know how to connect to the right PLC processor online, make minor changes to get the machine running and have the know-how to test new ideas and hardware components. In addition, you want to be able to do troubleshooting and problem solving of your associated SCADA system”.
Introduction to the PLC
Introduction to the PLC

• “PLC” means “Programmable Logic Controller”. The word “Programmable” differentiates it from the conventional hard-wired relay logic

• The PLC as a unit consists of a processor to execute the control action on the field data provided by input and output modules

• In a programming device, the PLC control logic is first developed and then transferred to the PLC

• PAC or Programmable Automation Controller
What can a PLC do?

• It can perform relay-switching tasks.
• It can conduct counting, calculation and comparison of analog process values.
• It offers flexibility to modify the control logic, whenever required, in the shortest time.
• It responds to the changes in process parameters within fraction of seconds.
• It improves the overall control system reliability.
• It is cost effective for controlling complex systems.
• Trouble-shooting becomes simpler and faster.
• An operator can easily interact with the process with the help of the HMI (Human-Machine Interface) computer.
Basic block diagram of the PLC
Ladder program execution

Scan1:

START P.B.

STOP P.B.

Scan2:

START P.B.

STOP P.B.

K

K
Internal or External Problem
Internal or External Problem?

• Over 80% of malfunctions are with I/O modules and field equipment
• Problems related to specific I/O module or I/O device are external problems
• Large groups of failures – internals of PLC
Internal Problems
Internal Problems

- Check earthing/grounding is correct
- Check power supply to PLC is within correct range and ac ripple on dc supplies is not excessive
- Batteries on PLC are OK
- PLC program hasn't been corrupted
- Examine internal diagnostics for a crash of PLC program
External Problems
External Problems – digital Inputs

• Check Power supply to module
• Look for where power to digital Input comes from
• Check fuses/breakers
• Adequate changes of voltage to Input
• Digital input fine ===> PLC program problem
Discrete DC input module

24 Volts P/S

+VE

Field I/P's

CH.7

CH.6

CH.5

CH.4

CH.3

CH.2

CH.1

CH.8

COMMON

24 V DC

8 CH.DI Module

Terminals

CH.1 Internal Circuit

Opto-Coupler

5 v dc

To processor

Field I/P

24 v dc

D

ZD
External Problems – digital outputs

- Check Power supply to module
- Check power output from PLC
- Check fuses
- Force digital outputs on and off
- Use test load rather than open circuit – why?
Discrete DC output module
External Problems – analog inputs

• Move field device through full range of current – 4-20mA
• Hook up signal transmitter if you need to be absolutely sure.
External Problems – analog outputs

- Force output to specific value and observe
- Check external wiring
Remote troubleshooting

• Be careful with remote troubleshooting about industrial network security
• Hackers are about 24x7
Thorny transients

- Fiber Optics where possible
- Good earthing/grounding for data comms
The purpose of the shield is to reduce the magnitude of the noise coupled into the low-level signal circuits by electrostatic or magnetic coupling. This has brushed up the above-mentioned concepts up to some extent.
Opto-electric coupler circuit
When in doubt - disconnect

- Test with dummy equipment not 1MW ball mills
Troubleshooting of SCADA Systems
SCADA
Supervisory Control And Data Acquisition

– SCADA is not just Software or Hardware

– But a complete control system including communications systems
SCADA
Supervisory Control and Data Acquisition
Remote Terminal Unit

• The complete assembly of equipment at an end point of the control system in the field, factory or industrial site.

• This can be a Programmable Logic Controller (PLC).
Typical SCADA System
Industrial Communications
Protocols
RS-232 Connections (DB25)

Microcomputer (DTE)

1. Chassis Ground
2. Transmit Data (TxD)
3. Received Data (RxD)
4. Request to Send (RTS)
5. Clear to Send (CTS)
6. Data Set Ready (DSR)
7. Signal Ground (Common)
8. Data Carrier Detect (DCD)
20. Data Terminal Ready (DTR)
22. Ring Indicator (RI)

23. Data Signal Rate Selector (DSRS) (not supported by most PCs)

Modem (DCE)
RS-485 Review
EIA-485 interface standard

- Distances of up to 1200m
- Data Rates of up to 10Mbps
- 32 Line Drivers
- 32 Line Receivers

NOTE: Total of 32 devices on same line
Two Wire Multidrop RS-485

1200M (4000 FT)

TERMINATION RESISTORS AT BOTH ENDS ONLY

G - Generator
R - Receiver

- Circuit ground or circuit common
- Protective ground or frame ground
GWG - Green wire ground or power system ground

Note: The RS-485 standard documentation leaves out the inverters for the receiver
Modbus PLC Notation

Master Node

Slave Node

110 VAC Coil (Digital Output)

Digital Input 5 VDC

16 Bit Input Register

16 Bit Output Register

ADC

DAC

4-20mA Analog Input

4-20mA Analog Output

www.eit.edu.au
Troubleshooting and Maintenance
• Ensure that components are not removed on line whilst the system is powered up unless the manufacturer specifically indicates that this is permissible.
• Damage to components and modules can occur when removing whilst the system is still powered up.
• Ensure that the antenna system is not disconnected from the system unless a dummy load has been installed, otherwise the radio power amplifier may be damaged.
The RTU and component modules

Check:

- Analog input modules
- Digital input module
- Interface from RTU to PLC (RS-232 / RS-485)
- Privately owned cable
- Switched telephone line
- Analog or digital data links
The master sites

- The master sites will generally consist of a more complete telemetry unit and higher quality radio equipment.
- The same troubleshooting techniques can be applied to the master site as are used at the RTUs.
- Additional equipment would include links to other master sites, to the central site and computer control facilities.
The operator station and software

There is not much that can be done here if a system fails or has intermittent problems except to systematically replace each connected unit to identify the faulty module

- Operator terminal (normally a personal computer)
- Local area network card(s)
- Bridge unit to radio, microwave or landline system
- Printer connected to operator terminal
There are however a few problems which can be examined:

• Operator terminal locks up intermittently
• Throughput of the operator station and associated system drops off dramatically
"We are proud to present our new video-based eLearning platform designed for engineers and technicians."

Electrical Engineering (8 courses)

Electrical engineering is the science that studies the use of electricity and the equipment used to generate, distribute, and control it.

The short course videos form part of a professional development series and are designed to provide you with critical knowledge and practical tools that can be immediately applied to the workplace. They include lectures, recordings, and practical online materials that can be studied at your own pace.

Instrumentation (2 courses)

Instrumentation is the art and science of measurement and control of process variables within a production or manufacturing area. It can involve control valves, SCADA, PLCs, process plant layout, piping design, boiler control, hazardous areas, industrial data communications, networking, deviceNet, and Fieldbus, radio telemetry systems, safety, and much more.

"Complete professional development courses with ease, thanks to our brand new user-friendly platform."

Dr Steve Mackay, Dean of Engineering

www.video.idc-online.com

enquiries@idc-online.com
The brand new, user-friendly IDC Video platform gives you exclusive access to high demand courses and offers you the following benefits:

• Self-Paced video courses with no completion deadline
• Try-before-you-buy: Free introductory course videos
• Achieve a ‘Certificate of Completion'
• Courses from US$99
• Track your course progress
• Lectured by industry experts
• Includes associated technical eBook and quizzes
• Complete professional development courses with ease

www.video.idc-online.com  enquiries@idc-online.com