Automation Software Support Recommendations for End-Users

Specification, programming and support of automation software for end-users

Specifying, sub-contracting & support issues, when procuring electrical design and software design for programmable logic controllers and associated hardware.

Author:

Jan Hemper, Technical Director at InControl Systems Ltd.

Document:

Reference - ICSLWP02
Version - 01 issue 01

1. Who this white paper is written for:

Managing Directors, Technical directors, Engineering Directors, Operations Directors, Control Managers, Electrical Managers, Engineering Managers of end-users such as manufacturing and process factories, plants and facilities.

2. What are the 'take-aways':

This paper is intended to provide insight into the specification, procurement and support of software for machine and equipment control systems. Although this paper specifically refers to PLC application software, it is equally relevant to other components of the programmable automation system such as HMIs and SCADA.

- Insights - asking the right questions of your business and its suppliers
- Understanding the current state of your machines and control software within them
- Appreciation of the hardware controls within your machines, processes and control cabinets
- The top 4 risks facing manufacturing and process industries, and mitigating against those risks
- Recommendations for best practise and protecting your business operationally
- An executive summary

3. Introduction:

One of the most under-appreciated challenges facing manufacturers, process industries and other end-users, is the knowledge and up-keep of software systems inside critical items of plant and machinery throughout their site.

Most manufacturing factories or process plants rarely consist of brand new, single-sourced equipment. In most cases, the site processes have been developed over the years, with additional machinery and equipment being brought in from different suppliers over the last 2 or 3 decades.

Companies have changes in their own personnel, and their suppliers of equipment & plant may have ceased trading or may no longer provide long term support for the installed equipment. With these issues, it is easy to see how records, information and knowledge of the systems that their business relies on may have been lost.

This white paper sets out to explain many of these challenges and the recommendations for protecting your company against them.

4. Insights:

Most manufacturers are experts in how best to manufacturer their unique product. They are however reliant on the specialist equipment and processes designed to make their product as quickly and efficiently as possible. However, this reliance is a contributory cause of some of the biggest risks and challenges to their continued and sustainable production and productivity.

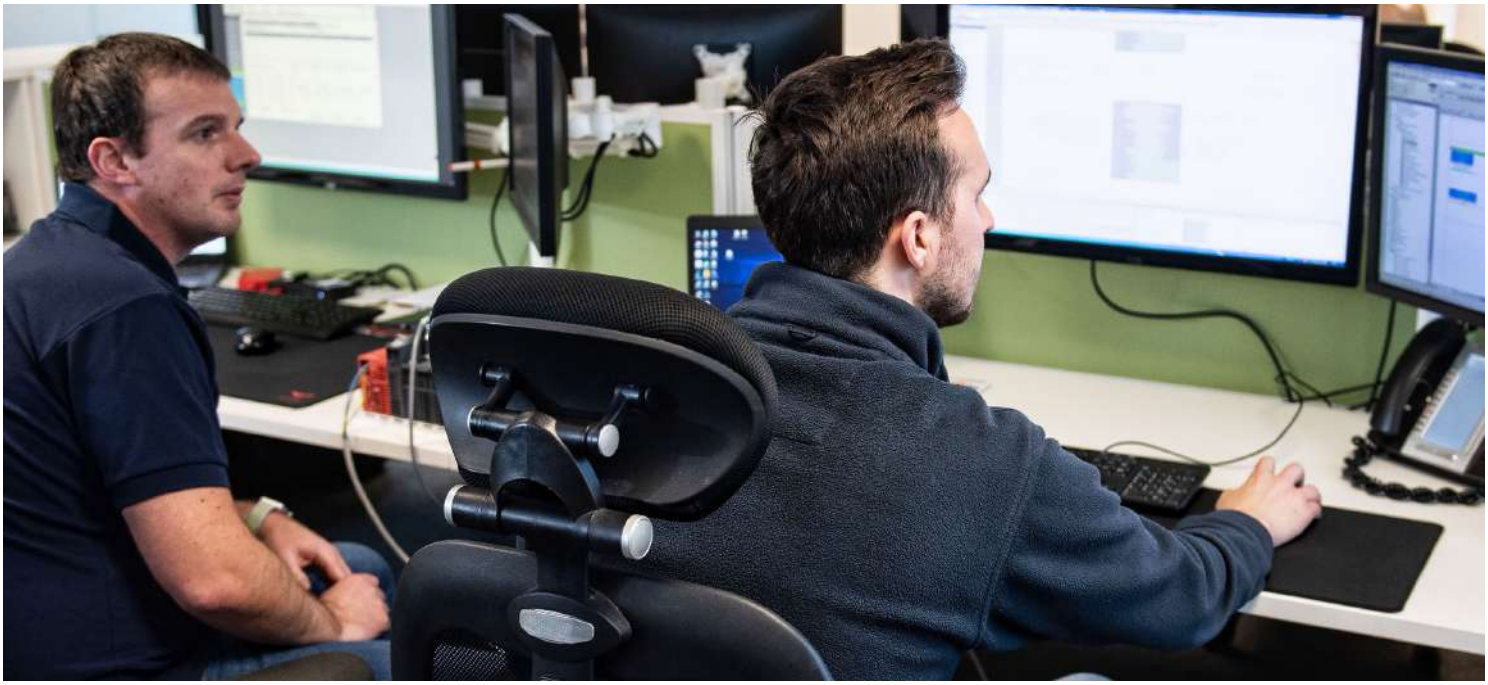
The following insights pose questions that you may need to ask of your own business in order to understand the level of risk and preparedness for the future upkeep of your facility:

#1 Who owns and who keeps copies of software that runs on each and every machine you have?

Invariably, the software on semi-standard machines is owned as the IP (intellectual property) of the original equipment manufacturer. This is understandable, but where does that leave you towards the end of life of that machine? When the machine may need upgrading, refurbishing or just basic functionality changes.

#2 Do you have adequate documentation for all machinery new and old?

Often drawings are located inside control panel doors, and as a machine gets older and more frequently maintained, those drawings may become modified, damaged and out of date. Do you have a digital copy (with back-ups) for these electrical drawings? and who is responsible for the upkeep of the data?



#3 How well is the software documented for any machines you have on-site?

For older machines, the challenge will be finding the software files and viewing the documentation, and that assumes you have someone on site who can make a judgement on the quality of this, even if you can locate it.

For newer machines under service contracts or new machines you are about to buy, the machinery supplier may be reluctant to provide copies of this software, but should always be prepared to let you view the software and you will need to make plans for the support of this in 5, 10 or 20 years' time.

#4 What are the big challenges and trends facing your business and the market it operates in?

Invariably, at the time a new machine is or was specified, the only focus is to the specified operational needs of that machine. End-users are unlikely to be able to guess what changes are likely in their business in the next ten years or so. But, we all know that changes will come, and it will be essential to have access to the software of those machines in order that modifications to operational process or connectivity can be made.

#5 Who's making modifications to the software on your machines?

Whether this an internal PLC/electrical controls engineer, sub-contractor systems integrators or the original equipment manufacturer, you need to know where the revised code is kept, how well it is documented and that you have adequate version control in place.

5. Understanding and supporting the software in your machines, equipment & plant:

Typically, if there is a control cabinet attached to a machine or process, or piece of equipment, there is a high chance that there will be a process computer, HMI or PLC inside it. It doesn't need to have a screen and keyboard for software to be running inside it.

If a process, equipment or machine is essential for the daily operational success of your business, you need to perform some level of audit to assess where any risk may lie.

Consider the following types of equipment when performing an audit of your machinery and plant:

- Any suites of floor standing cabinets connected to your production line
- Control cabinets integrated into machines
- HMI, screens and basic displays connected to the operation of machines
- Small electrical cabinets connected to important equipment
- Control room, or control desk systems
- Cabinets connected to handling, warehousing and conveyor systems
- Operator workstations
- Dedicated computer systems in 19” cabinets
- Any systems above that are used in critical single-sourced supply chains

6. Consider also, the hardware in the control cabinets:

Whilst assessing the availability and quality of software inside your machinery and processes, you may also wish to conduct an obsolescence review of the equipment that the software is running on.

For example, having access to the source code of a particular PLC, may not help you if the PLC has been made obsolete 10 years ago.

Whilst electronic systems (note that PLCs and drives are electronics) when looked after, are highly reliable. Temperature, humidity, vibration and dust can significantly shorten their lifetime. Many similar pieces of equipment, when run in similar circumstances, will have the same lifetime. For example, if 3 drives fail after 8 years, there’s a good chance the others will be failing soon.

As a ‘rule of thumb’ control cabinets, with an internal temperature (which is often 15-30 degrees higher than the building temperature) of say 50 degrees, will halve the lifetime of internal components, compared with a cabinet of 40 degrees.

In short, ageing equipment, in hot cabinets will invariably have shorter lifetimes. Sometimes, electronics which could have a lifetime of 10 years in a temperature-controlled cabinet, can see its lifetime reduced to 1 or 2 years, purely because a lack of adequate cabinet cooling.

Being prepared and having a plan of action for upgrading and improving these control panels is therefore essential.

7. Risk management:

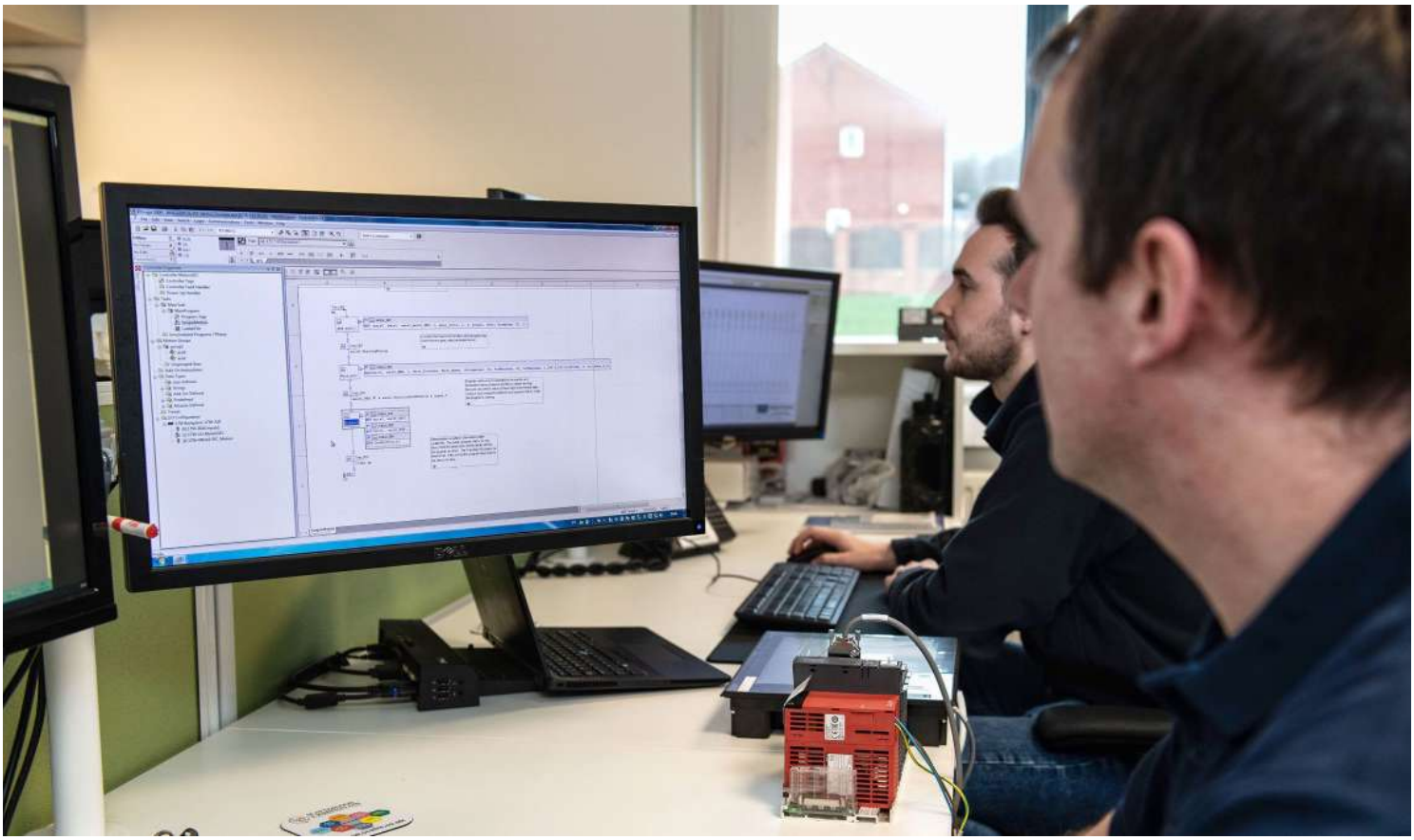
Having a good understanding of the current state and having asked the right questions of your business is only the first step. The next step is to be aware of those risks and to start planning a strategy to mitigate those risks in order of priority:

Risk	Mitigation
Software and or documentation is not available for an important machine or process Risk: **Medium** Impact: **Medium**	Get your PLC engineer or contractor to extract the raw PLC code or machine software from the device: • Archive the software and have secure back-ups • Ensure future procurement of machines includes software access within the contract • Understand if the hardware is still in current supply • Consider reverse engineering for documentation and future support
Electrical drawings unavailable for the machine Risk: **Medium** Impact: **Medium**	Speak to the original equipment manufacturer to obtain drawings and speak to contractors and electrical engineers to obtain any revision updates: • Archive digital copies of the drawings, with back-ups • Conduct a control panel audit to decide firstly, if the controls wiring is adequate or needs refurbishing, and secondly if the controls hardware is of current supply and not obsolete • Consider a long-term refurbishment plan for this panel
Reliance on a single controls contractor or a single employed controls engineer Risk: **Low** Impact: **High**	Perform a review of the methods and records used by your engineers: • Ask for copies of all software source code • Agree levels of documentation provided • Use independent advice on reviewing the above • Have back-up resources for when your preferred engineer is sick or unavailable for work
Ageing equipment, that could fail or regularly needs rework Risk: **High** Impact: **High**	Often the mechanics of a machine are part of the maintenance schedule and can have a long lifetime when well maintained, yet the control cabinet is ignored, consider: • A control cabinet review or audit, software & hardware • Quality of wiring, repairs and recent upgrades • Internal temperature of the cabinet & improved cooling • Age and availability of PLC controls • Spares provision for hard to find components • Plan for complete refurbishment of the cabinet

8. Recommendations:

We hope you will find this document has given you enough questions to ask and enough answers to the risks that your business finds during any reviews or audits, below we summarise our recommendations to protecting your business:

- Consider software access and documentation as part of your disaster recovery plans
- Ensure that future machinery, equipment or automation purchases include access to software and adequate documentation
- Conduct a site wide audit using your own staff or competent professionals to review all electrical and control cabinets, covering; software, documentation, obsolescence, safety & reliability
- Ensure that electrical drawings are available as digital copies and are kept archived and backed-up
- Ensure that all source code for PLCs and machine computer systems has documentation, keep both source code and documentation archived and backed-up
- Consider writing a company, site or group controls specification, which can help with standardisation of controls methods and equipment as well as being part of future machine procurement contracts



9. Executive summary:

Using the adage of 'if it isn't broken, don't fix it' is fine to a degree, but do you know which machines in your business are either close to breaking or, if they did break, would be very difficult to fix?

Furthermore, if your business changes and you need to restructure your processes or modify your machine operations (think 'Made Smarter' or Industry 4.0), do you know if you have access to the control software inside those machines, or even if the companies that delivered those machines are still able to support you?

The recommendations above should cover most of the risks faced by your business in relation to machine, equipment and process automation software. (and to a degree the hardware)

You will know the costs of downtime by the hour or day of your plant. The risks identified in this document are not unique and relate to every manufacturing or process business. But the risk of occurrence and the severity or impact vary from case to case, from machine to machine and site to site.

At the lowest impact, could be the need to reprogram a new device and replace a failed one, which might have your line down for 1-2 hours. At the most extreme, could be an obsolete PLC which may not be available anymore, or a control panel that needs to be rebuilt and reverse engineered to replace a system that just cannot be repaired. At best several days, at worst weeks of machine downtime.

Creating a plan to review your risks and plan for mitigating those risks by order of priority is therefore of paramount importance.

10. Sources:

Contacting the author: Jan Hemper

The author can be contacted on jan.hemper@incontrol.co.uk or by calling +44 (0) 333 313 0006.

InControl Systems Ltd are an independent Systems Integrator with over 20 years of experience in producing control and automation solutions in a wide range of industries.

InControl Systems Ltd
Coney Green Business Centre
Clay Cross, Chesterfield S45 9JW