Systematic approach to maintain safety performance in the service of CANopen systems

Dr. Heikki Saha, TK Engineering Oy, Pertti Vilenius, Cloudfield Operations Oy

Safety standards require, that manufacturers are responsible for maintaining safety level of systems throughout their life cycle. Traditionally the implementations have been designed and validated design time only. Despite of the requirements, little extra attention has been paid for guaranteeing assembly, maintenance and service of the systems without degradation of safety performance. Experience has shown, that safety performance after assembly is lower than designed and further, maintained level gradually decreases from assembled one.
More systematic approach for reliable spare part orders, logistics and assembly is presented. Main enabling thing is adding machine understandable identifications for components, transportation means, systems and target positions. Then, information may be accessed by consumer devices so, that error prone manual typing of identifiers and information searching are not required. Consistent identification enables automated information collection in the background, without intentional human effort.
Main results include order of correct and valid spare parts, including second sources, up-to-date product documents and configuration packages in the field. Status in the field is continuously up-to-date, including errors. In addition to the automated live reports, most serious exceptions trigger notifications, including links to corresponding reports. With the presented concept, it is possible to maintain the designed safety level in practice.

Introduction

Requirements for functional safety performance of control systems is continuously increasing. Simplified view to functional safety is, that as long as a failure can be detected in a reliable way, control system can perform safety reaction and no danger will result.

CANopen is never the only system integration technology in systems, also other technologies – e.g. mechanics, hydraulics and electrics – exist and are coupled with CANopen in both designs and implementations.
There are some design traditions, which need to be updated. The first tradition is understanding, that increased safety performance is only an additional cost and does not provide any advantages. Functional safety performance is based on mean time to dangerous failure (MTTFd) and diagnostics coverage (DC) of the system. MTTFd is mainly a sum of the corresponding values of components and it is not so easy to improve that, except the use of lower number of or more reliable components. But, improving DC may be performed in many levels. One shall notice, that improving DC results improved diagnostics – achieving more accurate detection of failure modes and locations, which provides not only improvement in safety performance, but also valuable improvement in system maintenance performance.

Second design tradition is, that degradation of safety in assembly and maintenance procedures have not been seriously considered. Despite of the fact that cabling and wiring failures are dominating the failure statistics, discrete instrumentation is widely used instead of field buses. It is well known and proved fact, how much better DC may be achieved by replacing discrete wiring by field bus, e.g. CANopen [1]. From diagnostics point of view, main problem with discrete instrumentation is, that each signal needs to be accessed separately by persons and corresponding documentation and drawings typically exist in human understandable format only.

Third tradition is, that information transfer strictly follows organizational barriers. As a result, assembly and service departments work according to the design documents, but there does not exist systematic information sharing mechanism towards design departments. In other direction, fixes to documents and drawings are not systematically distributed to the field, because design departments don‘t have any systemtics, where and how to distribute.

Fourth tradition is, that it has had to be possible to e.g. change spare parts without any systematic checks and configuration downloads. Such has been the way of working with discrete sensors and actuators, which don‘t support machine readable identity. Furthermore, configurations have been mounting or dismounting physical parts or manual adjustments, instead of automated sequence of download, store and verification. Due to a need for intentional reporting, majority of the problems have not been reported and thus “not officially occurred”.
Main objectives of this paper are the overall dependability and functional safety in wider scope, not only how to meet certain SIL or PL level by the design. This paper begins with a brief introduction of prerequisites and review of design time issues, which provide complete and consistent information for the assembly and service operations. Next, troubleshooting is considered, followed by spare part logistics. Preparing for assembly and system assembly related issues are covered as last topics, because same actions apply for both assembly of new and spare parts.

Prerequisites

There are some prerequisites for successful further steps. Major cornerstone of multidisciplinary information management is a uniform mechanism for linking the different disciplines together via the natural interfaces. Typically sensors and actuators have interfaces for mechanics, electrics and control system. There is often interface also for hydraulics or other power source. Linking mechanism already exist in the form of reference designators, which are based on the higher level architecture. Common problem with existing higher level architectures and reference designation systems is, that they are applied only partially, typically in electrics and hydraulics schematics containing components with electric interface. Such leads into partial connectivity between the disciplines, applications and documents.

All the information to be distributed, shall be semantically complete enough. In practice, each linked artefact shall have both machine understandable meta information and human understandable, visual appearance. Without a defined meta information, information content cannot be linked.

Design time

CANopen enables reliable, standardized methodology for communication of device capabilities and even optional configuration management GUI tools from device vendors to system integrators [2] [3]. For application program development, CANopen provides standardized way for managing SW component interfaces as library components [4] [5] and interaction with system models [6]. Based on the standardized configuration file formats, 2nd source management may be included [7] with dependable device configuration re-use [7] [5] and system design tools may also generate entire communication abstraction layers for SW development [8] [9] [10], for which there exists a standardized format for PLCs [11]. Connection to the system architecture may be implemented simply by picking target position information from a central repository [5].

Despite of the various vendor specific formats of CAD programs, integration of electric design into system- and SW-design has been implemented [12] [13].

Standardized format for storing configuration of each CANopen device enables seamless information transfer from system design into assembly and service [2] [14]. Furthermore, system design tools create communication description for system analysis.

It can be concluded, that there exist, up to some extent, standardized design practices and information sharing interfaces in design tools. Utilization of such results consistent information for system assembly and service.

Troubleshooting

Due to the lack of centralized access to the discrete instrumentation, also information transfer has been based on human understandable documents only. Thus, the troubleshooting has been labor intensive and prone to human mistakes in each phase.
The first problem with human understandable only documentation is, that finding each artefact from the drawings cannot be automated, service technicians shall read the artefact identification and search it from the drawings manually.

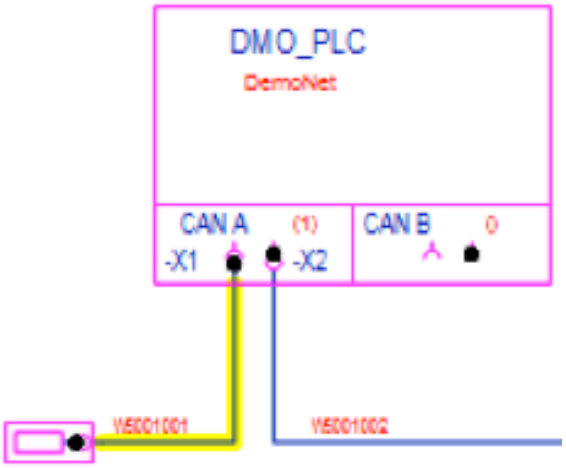


Figure 1: An example of schematics with highlighted CAN cable shown based on reading the cable identification tag

Such procedure may be easily improved by supplementing the human understandable markings in the system into machine understandable tags. Thus, the technicians need not to manage the artefact identifiers manually, because they can just read the tags by their terminal devices. As illustrated in Figure, drawings corresponding with the tagged artefact may be accessed with tagged artefact highlighted by a single click. Main results are significantly improved access time of the correct drawings and practically no space for human mistakes. Further advantage is, that updates need to be uploaded as files to a single server, instead of distributing hard copies worldwide.

The second problem has been measurement of the instrumentation as part of troubleshooting. Troubleshooting of discrete instrumentation requires reading schematics and measuring individual points by multimeter or implementing a massive HW setup for logging multiple points simultaneously. There does not exist any standardized approach for improving the information transfers regarding the measurements.

With CANopen based systems, it is always possible to access each network from single point for analyzing the entire network. Furthermore, there exists a de-facto format for describing the conversion of communication from raw data into human understandable format. The format is supported by majority of the corresponding tools in the market, enabling the use of generic work flow.

```
From:     QFL <qfl@cloudfield.fi>
To:       Alarms <alarms@customer.com>
Date:     14.05.2016 13:46:44
Subject:  10000001 - ABCD1234 - Y1000A -
Repetitive Issues...

Repetitive Issues Notification
Date: 14-05-2016
Time: 13:46:44
Customer: 10000001
System: ABCD1234
Position: Y1000A
Severity: 2
URL: http://qfl.fi/cgi-bin/rm.py?
c=10000001&...
```

Figure 2: Example alarm email triggered by repetitive issues

The third problem has been, that feedback from the field operations has not been available without heavy and intentional reporting by the service technicians. Often they have not had sufficient information for traditional reporting systems, why feedback has not been systematically available.

The new approach has been designed for not only sharing the product documentation, troubleshooting projects and configuration packets, but also including follow-up of field status and automated alarms in the case

of exceptions in target systems and in the used analysis tools and projects. With such supplements, status in the field is always up-to-date, more comprehensive and available for all consuming organizations.

Spare part logistics

Spare parts may be ordered traditionally, based on component ID-code. Human mistakes may be avoided, when the information is read from a tag, instead of typing it manually. There is still a risk of an unsupported existing part or missing part information leading into problems. With parts without a need of configuration this is significant, because additional identity check does not exist.

Order may also be based on combination of target system and position information. No matter if there exists obsolete, unknown, unapproved or valid part, the approach results always an order of a correct part. There is a minimum risk of missing information, because the position tag is attached close to the part, but not on the part.

Follow-up of the part logistics based on combination of part ID-codes and serial number over the entire delivery makes it easy to reveal logistics problems. Especially intended or accidental recycling of discarded parts back to the field may be efficiently detected.

Automated process helps in recording and analysis of the orders. Unexpected increase in number of orders may indicate quality problems or decrease potential use of unapproved parts or reduced maintenance. Especially position based orders help in determining the root causes for the consumption. If spare parts are needed evenly distributed in many positions, a potential problem may be in the component. But if spare parts are needed only in one or few positions, there may be a design problem in such positions.

Preparing for assembly

Devices have been required various kinds of configurations also in more traditional systems without networked control system, but not as numeric parameter values. Changing spools, springs and washers as well as manual adjustment of screws, potentiometers and jump wires have been used instead. Main problems with such traditional parametrization are constrained accuracy and repeatability of the settings and a need of special competence by the involved technicians.

In modern, distributed systems, configuration downloads are supported in a managed way with information systematically produced in the design. Moreover, there exists an integrated support for alternative devices. Device identification may be utilized in order to stop proceeding forwards with installation of an invalid part [15]. Errors in parameter sets, download and saving the changes may be revealed by a managed procedure following a sequence of write, store, reset and verify.

```
From:     QFL <qfl@cloudfield.fi>
To:       Alarms <alarms@customer.com>
Date:     14.05.2016 13:46:44
Subject:  10000001 - ABCD1234 - Y1000A -
Download aborted

Configuration Download Notification
Date: 19-05-2016
Time: 10:44:48
Customer: 10000001
System: ABCD1234
Position: Y1000A
Failure: Download aborted
URL: http://qfl.fi/cgi-bin/pm.py?
c=10000001...
```

Figure 3: An example alarm email triggered by aborted configuration

Integrated tool execution and download process status transfer back to the server have been presented earlier [16]. Automated alarm email – as show in Figure – is sent in the case of any exception. Aborted download may indicate e.g. the use of unsupported part or constrained competence of the involved technician. Download error may indicate a missing download tool or its license, a problem in a configuration package or constrained competence in the case of e.g. missing supply power or unsuccessful network access to the device.

System assembly

Recorded document accesses may be used for proving, that technicians have read the instructions before assembly in order to ensure safe and error free installation procedure.

And vice versa, missing document reads may indicate unapproved service procedures, further indicating constrained competence of the technicians, as well as randomly repetitive access of various documents.

Removed and installed parts may also be recorded. Removed parts may be defined as discarded, which enables preventing them coming back to the use without a notice. Removed parts may also be used as spare parts for other systems or sent for repair. The detailed follow-up enables maintenance of a technical file for each system, which is required for many kinds of systems.

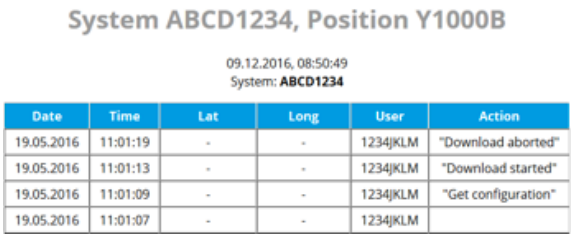
Marking service done

Traditionally service actions have been reported mainly for invoicing purposes, but not for continuous follow-up of the systems production and safety performance or structural consistency.

Service actions may also be acknowledged in a managed way. In addition to the target system and position, each acknowledge consists of time, location and user information. Such enables full traceability of the performed actions. It is also possible to limit the capability of marking services done by license level. Thus, only authorized persons may officially acknowledge the services done.

Reporting

Main problem of reporting is a tradition of considering reports massive and regularly generated static historical overviews. Such kind of reports are practically always out of date and indicating status over each period. Major disadvantage is, that if something significant happened during between the generation times, the indication is included in the next report, after a delay. In the developed approach essential is, that separate heavy reporting is not used – assembly line and service technicians shall just be able to do their work with state-of-the-art tools and information is accumulated into server, where the required reports may be generated and updated on-demand.

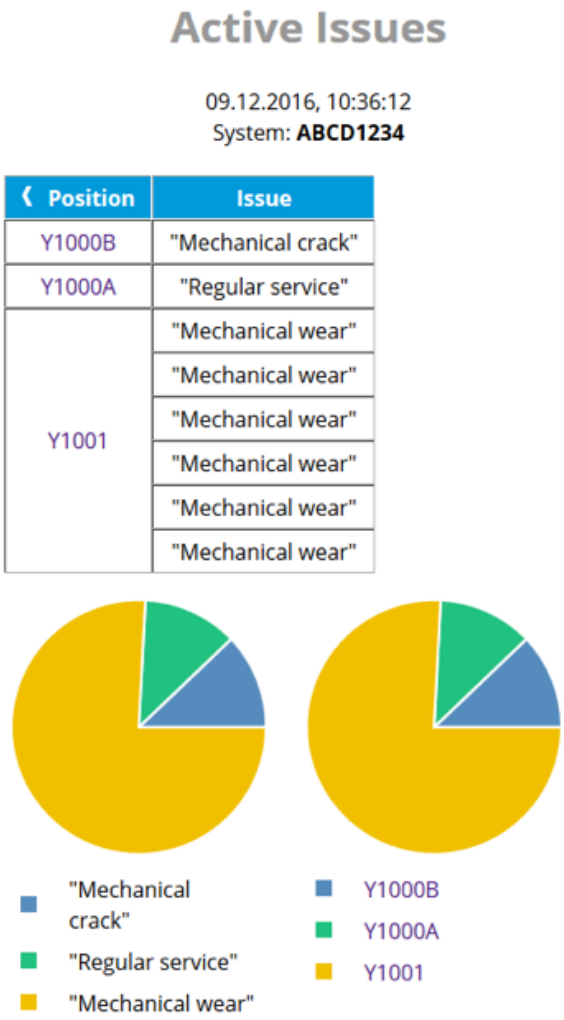


System ABCD1234, Position Y1000B

09.12.2016, 08:50:49
System: **ABCD1234**

Date	Time	Lat	Long	User	Action
19.05.2016	11:01:19	-	-	1234JKLM	"Download aborted"
19.05.2016	11:01:13	-	-	1234JKLM	"Download started"
19.05.2016	11:01:09	-	-	1234JKLM	"Get configuration"
19.05.2016	11:01:07	-	-	1234JKLM	

Figure 4: An example log of aborted configuration download



Active Issues

09.12.2016, 10:36:12
System: **ABCD1234**

Position	Issue
Y1000B	"Mechanical crack"
Y1000A	"Regular service"
Y1001	"Mechanical wear"
	"Mechanical wear"
	"Mechanical wear"
	"Mechanical wear"
	"Mechanical wear"
	"Mechanical wear"

"Mechanical crack"
"Regular service"
"Mechanical wear"
Y1000B
Y1000A
Y1001

Figure 5: A report providing spatial and categorical summary of pending issues

Due to the holistic approach, reporting may serve all consuming organizations, without extensive workload. Reports contain strictly focused, manageable size, on-demand and most recent information instead of massive off-line reports generated at regular interval. The most common and severe known problems may be detected by checker plug-ins, which send email alerts on exceptions. Such alerts typically contain a brief notification supplemented by a link into corresponding report in order to both optimize the use of

communication bandwidth and keep the information up-to-date despite of the moment of reading.

First example is show in Figure, where a history of aborted configuration download exists. Such view may be opened via a link included in the alarm email shown in Figure. Second example is show in Figure, where a list of burst mode pending failures are listed. Such overview may be opened via a link included in the example alarm email shown in Figure. Third example in Figure shows an overview of pending failures, which supports important information for strategic management of the entire product line.

Discussion

Functional safety is a global topic and such requirements cannot be fulfilled by the plain control system components and design. Also each supporting process shall support minimization of number of created errors and early detection of errors. Furthermore, required safety performance shall be maintained throughout systems‘ entire life cycle, which requires support for safety performance maintenance by the entire maintenance process.

Presented approach provides easy, fast and context specific access to the information needed in field operations. Human load is significantly reduced by strong context sensitivity. Such relieves human effort of the service technicians from using tools into the actual field operations, which reduces the probability of mistakes. Based on the pilot projects, especially “Show in drawing” function reduces time and effort required for finding location under investigation from drawings.

As reported earlier [16], measurement setups may be easily accessed and performed measurement sessions monitored. The setups may be accessed from both real tagged artefacts and drawings. Same applies also for configuration packages, where aborted and failed downloads are automatically reported in the background, without intentional actions by service technicians.

Failure indications may be easily targeted to the product structure, which significantly helps in finding the actual root causes instead of the symptoms. Instead of component identifier, spare parts may be ordered by the target location, which approach is independent of the existing part and thus removes significant number of errors.

Logistics features serve also maintaining the safety. Tracking of components throughout the logistics chain provides excellent safeguard against various delivery failures, mixing of valid spare parts and intentional replacement of valid part into unapproved one. Traceability also helps in monitoring, that service technicians read the required information and perform the required configuration tasks before the assembly. Legal issues are only one side of the entity. Realized quality is another side, which may be improved only based on the facts of the current way of working.

Special effort is not required for continuous monitoring, because notifications are sent when special actions are needed due to exceptions. Notifications include links to the corresponding applications or reports in order to provide readers always up-to-date status, independent of the notification generation time.

Of course the main prerequisite is, that information to be shared is semantically consistent so, that linking may automatically be included. Creating consistent information has been investigated lot and there exists a good knowledge on using existing design tools for creating such information. In addition to the activities behind the referred literature, there is increasing demand and activity on generic development of design information management. In addition to the reliable communication [1], CANopen is also in design information management one of the leading technologies, which the others should follow.

Major future research topic, in the context of presented platform, is required for clever handling of the log files created by the 3rd party tools. Plain compression or size restrictions may not be optimal and more sophisticated preprocessing may be required.

Conclusions

Utilization of CANopen for material and information logistics in addition to the communication provides significant improvement also in maintenance of functional safety performance. Most common inconsistency problems with ordering, configuring and installing the spare parts can be solved. Significant improvement also applies to the management of tool related problems. It is obvious that CANopen shall be used in conjunction with the other standardized technologies, in order to successfully maintain safety performance with corresponding documentation of the entire systems, over their life time.

Main outcome of the developed approach is, that support for maintenance of functional safety performance can be improved by increasing systematics and utilizing the field status information as a feedback for improvement of the quality bottlenecks. Continuous and intentional monitoring is not required, because various post processors may be executed in the background and only the raised exceptions are passed to the corresponding persons. Such removes repetitive tasks and lets persons concentrate on the demanding decision making and problem solving.

Improved efficiency instead of adding work load may be achieved in reporting. Commonly used identification methods apply directly to CANopen, which together with open design information and tool integration interfaces make CANopen one of the most attractive system integration technologies.

References

[1] Hietikko M., Malm T., Saha H., Comparing performance level estimation of safety functions in three distributed structures, Journal of Reliability Engineering and System Safety, issue 134, Elsevier, 2015, pp. 218-229
[2] CANopen Electronic datasheet – Part 1: General definitions and electronic data sheet specification, CiA-306-1, CiA
[3] Saha H., CANopen device configuration editors, CAN-Newsletter 4/2013, CiA, 2013, pp. 30-33
[4] CANopen Electronic datasheet – Part 2: Profile database specification, CiA-306-2, CiA
[5] Saha H., Systematic re-use of information, CAN-Newsletter 2/2014, CiA, 2014, pp. 20-25
[6] Saha H., Model-based design of distributed mechatronic systems, CAN-Newsletter 4/2014, CiA, 2014, pp. 38-45
[7] Saha H., Optional structures in CANopen projects, CAN-Newsletter 1/2014, CiA, 2014, pp. 32-35
[8] Saha H., Improving development efficiency and quality of distributed IEC 61131-3 applications with CANopen system design, Proceedings of the 13th iCC, CiA, 2012
[9] Saha H., Experimental CANopen emergency error code (EEC) management, CAN-Newsletter 1/2013, CiA, 2013, pp. 12-18
[10] Saha H., SI unit and scaling management in CANopen, CAN-Newsletter 3/2013, CiA, 2013, pp. 30-34
[11] XML Formats for IEC 61131-3, Technical Paper, PLCopen Technical Committee 6, Version 2.01 – Official Release, PLCopen, 2009, 80 p.
[12] Helminen M., Salonen J., Saha H., Nykänen O., Koskinen K.T., Ranta P., Pohjolainen S., A new method and format for describing CANopen system topologies, Proceedings of the 13th iCC, CiA, 2012
[13] Saha H., Exception management in CANopen systems, CAN-Newsletter 2/3013, CiA, 2013, pp. 12-17
[14] Saha H., Accelerated transfer of CANopen projects into assembly and service, CAN-Newsletter 4/2012, CiA, 2012, pp. 16-20
[15] Saha H., CANopen in series production, CAN-Newsletter 3/2015, CiA, 2015, pp. 8 -11
[16] Saha H., Vilenius P., Cloud based CANopen system service approach, Proceedings of the 15th iCC, CiA, 2015, pp. 08-1 – 08-8

Dr. Heikki Saha
TK Engineering Oy
Yrittäjänkatu 17
FIN-65380 Vaasa
Tel.: +358-50-588-6894
heikki.saha@tke.fi
www.tke.fi

Pertti Vilenius
Cloudfield Operations Oy Ab
Yrittäjänkatu 17
FIN-65380 Vaasa
Tel.: +358-45-801-7424
pertti.vilenius@cloudfield.fi
www.cloudfield.fi