# A Methodology to Upgrade Legacy Industrial Systems to Meet Safety Regulations

Kleanthis Thramboulidis
Electrical & Computer Engineering
University of Patras
Greece
thrambo@ece.upatras.gr

Doaa Soliman and Georg Frey
Chair of Automation
Saarland University
Saarbrücken, Germany
{doaa.soliman,georg.frey}@aut.uni-saarland.de

*Abstract*— **There is a need to upgrade legacy system in industry to conform with safety norms and regulations defined by recent standards. The great investment for the development of these systems is the main reason for the industry to look for approaches to upgrade legacy systems instead of adopting a redevelopment of the whole system. In this paper, we describe an approach to upgrade legacy industrial applications based on the IEC61131 function block model without the need to redesign the whole application. The approach that integrates the 3+1 SysML-view model with safety engineering is adopted and is tailored to the needs of upgrading legacy applications. Challenges are identified and solutions are proposed towards the definition of the whole development process including the verification of the so generated safety application. A laboratory system is used as a case study in this paper to demonstrate the applicability of the proposed approach.**

***Keywords- 3+1 SysML; Safety applications; PLCopen; verificationand validation; Model-checking***

## I. Introduction

Social demands for safety has accelerated international standard organizations, such as ISO and IEC to release standards on safety. Manufacturing industries due to the increase in automation and the stronger demands on safety, which is imposed by safety standards, face the challenge of upgrading legacy industrial automation systems to conform with the norms and regulations imposed by these standards and certify that systems are safe for the human life and the environment The alternative to throw away the legacy system and develop a new one from scratch to meet the requirements specification, if such a specification exists, is very expensive. In most of the case the primary motivating factor for upgrading legacy industrial systems to be compliant with safety standards lies in the high value of software running on the existing system.

The IEC61131 [7] set of programming languages is widely used in industry and the majority of the legacy industrial automation systems are based on these languages. That is why safety issues of IEC61131 has already been examined by the research community. In [2] where a safety related evaluation of programming language constructs is given, the function block diagrams of IEC61131 that are based on verified libraries are considered suitable for safety-related control applications that should meet safety requirements of different Safety Integrity Levels (SILs) according to IEC 61508 [5]. Function block diagrams that are developed on the basis of verified libraries, such as the safety library of PLCopen [11], are suitable to meet the requirements of the second upper Safety Integrity Level, i.e., SIL 3. As claimed in [3] it should be noted that the use of IEC61131 function block paradigm even in the case of using safe libraries does not guaranty the safety level of the system. Safety analysis should be performed during development and the integration of the safety analysis with the traditional development process of IEC61131 based industrial automation systems is not obvious. Hazards should be identified before and during the development process of the system and safety measures must be defined to reduce the risk imposed by the use of the system. It should be noted that during the last years the required solutions in technologies to ensure safety have been more complicated [1].

In most of the cases the reengineering of the legacy system is not an adopted solution due to several reasons [4]. In this case the only alternative is to develop a safety system that will meet the safety requirements of the legacy system and effectively integrate it with the legacy system. It is obvious that the approach described in [3] may not be used since it addresses the development of a new system. This may be used only in the case we adopt a reengineering of the whole system. Therefore, this paper presents an approach for upgrading a legacy system to be compliant with safety regulations and norms defined by current standards, such as IEC61508 [5] and IEC61511 [6]. The proposed approach, that utilizes SysML, addresses the following activities that have to be performed by the engineer:

1. Definition of safety requirements for the upgraded system.
2. Definition of the requirements of the safety system.
3. Design of the safety system.
4. Verification of the safety application.
5. Integration with the legacy system.
6. Verification of the upgraded system.

We are not aware of any other published work that describes a methodology for upgrading a legacy system to meet safety requirements. However, there are several works that consider the integration of UML [13][14][15] and SysML [8] with safety engineering.

[1]