Follow the Safety Lifecycle for Burner Management Systems!

Michael D. Scott, P.E.
VP – Process Safety
aE Solutions
P.O. Box 26566
Greenville, SC 29616

Some very exciting events are currently under way with respect to the design of the Burner Management Systems (BMS). For those of you who could not attend ISA 2002 held in Chicago on October 21 – 24, 2002, the following is a brief summary of BMS related topics that came to light during the paper and panel sessions conducted during the show.

There is much confusion with respect to the design of BMS's in industry in general. This was evident by the large attendance at the BMS sessions, emails on the ISA Safety Division bulletin board, and conversations I've had with numerous individuals. The confusion stems from the existence of multiple standards, guidelines, and / or recommended practices within different industries that contain both prescriptive requirements (i.e. NFPA) and performance based requirements (i.e. dIEC 61511 / ANSI/S84.01) that could be applied to the design of BMS's. Thus, individuals are struggling with the concept of which standard guideline, and / or recommended practice should be applied. For example, consider a simple packaged boiler installed in a refinery, one has the following choices with respect to design guidance requirements:

A. Apply NFPA 85 – Boiler and Combustion Control Systems Hazards Code

B. Apply API 556 – Instrumentation and Controls for Fired Heaters and Steam Generators

C. Apply ANSI/ISA S84.01 – Application of Safety Instrumented Systems for the Process industries

Which of the above is the governing document? Should one attempt to apply all three sets of requirements or only one? If only one, which one should I use? If you've been struggling with the above concepts you are not alone and industry is beginning to take some preliminary steps towards convergence of BMS design requirements to help clarify the current confusing situation. Convergence as I am currently aware of it, is a three pronged effort by multiple organizations, which is summarized briefly below:

1. **ANSI/ISA S84.01 Committee** - The SP 84 committee has an action item to draft a Technical Report / Guidance document that basically states that the Safety Lifecycle Concepts outlined in ANSI / ISA S84.01 should be followed with respect to BMS's. The purpose of this TR/Guideline is to provide guidance for users and OEM vendors of BMS's to determine which, if any, safety functions of a BMS should be implemented according to the requirements of ANSI/ISA S84.01-1996 and dIEC 61511. The TR/Guideline will show examples of prescriptive functions that may be required by NFPA standards, such as NFPA 85 and NFPA 86, and, by reference to ANSI/ISA S84.01-1996 and dIEC 61511, will indicate how to determine which functions are safety functions, how to allocate risk reduction to protection layers, and how to determine the required SIL (Safety Integrity Level) for the BMS safety functions. Also by reference to ANSI/ISA S84.01-1996, IEC 61508, and dIEC 61511, the TR/Guideline will give some guidance for how the safety functions should be implemented from a performance perspective to give the desired risk reduction.

2. **NFPA 86** – The NFPA 86 PLC sub-committee chairman has expressed in interest in developing linking verbiage to the concepts of ANSI/ISA S84.01-1996, IEC 61508 and / or dIEC 61511.

3. **API 556** – API 556 is in the very beginning stages of an update. As I understand it, part of their current efforts in this round of updates is to incorporate the concepts of ANSI/ISA S84.01-1996, IEC 61508 and / or dIEC 61511 into this recommended practice document.

Thus, the standards / guidelines organizations themselves are beginning to take steps to help clarify some of the confusion that exists regarding the design of BMS's.

BMS Survey

During the ISA 2002 show a brief and very informal BMS Survey was conducted in an attempt to gather a sense of who's doing what with respect to implementation BMS's and the Safety Lifecycle. This survey was in no way shape or form scientific in nature and was conducted by polling audience members of the BMS sessions. Thus, one cannot tell if the person responding was answering questions with respect to a specific plant site or from a corporation perspective. Also, multiple individuals from a single company could have significantly skewed the results. Thus, the survey should be viewed and interpreted loosely as a YES or NO answer to most questions. One should not focus on the specific percentages presented below. The ISA Safety Division BMS sub-committee will develop a formal survey and distribute it via email in the near future in an effort to gather and present better data to it's members.

BMS SIS Survey	
% of personnel assigning SIL:	25%
Methods used to select SIL:	Risk Matrix, LOPA
% BMS's installed before 1996:	50%
% BMS's installed after 1996:	50%
BMS Logic Solver utilized:	General Purpose PLC: 60% Safety PLC: 45% Solid State Device: 30% DCS: 10% Hardwired Relays: 10%
Most common SIL for typical BMS SIF:	SIL 1: 50% SIL 2: 50%
Standard utilized for Safety Lifecycle:	ANSI/ISA S84.01: 100%
Industries represented:	Power: 15% Chemical: 55% Petrochemical: 30% Pharmaceutical: 0% Pulp & Paper: 0%

Conclusion

Thus, it appears that based upon the survey results and direction several standards agencies are heading, one should begin evaluating the use of the Safety Lifecycle concepts to the design of BMS's, if you are not already doing so! This effort will provide you with the means to evaluate your current level of risk, document independent protection layers and determine if your existing BMS provides the required amount of risk reduction.

Future BMS Related Topics

ISA Safety Symposium March 2003 - Several abstracts with BMS slants have been submitted for approval to be presented at the show. These are as follows:

1. What's the Safety Integrity Level of My Existing Burner Management System?

   <u>Abstract</u>

   Many facilities have existing legacy Burner Management Systems that utilize a General Purpose Safety Configured PLC as the logic solver. Most of these systems were installed prior to the development and finalization of ANSI S84.01, IEC 61511 and / or IEC 61508.

   This paper will discuss the issues, decisions, and challenges encountered when attempting to apply the concepts of the Safety Lifecycle per ANSI/ISA S84.01, IEC 61508 and / or IEC 61511 to the design of an existing BMS for a single burner natural gas fired installation. Development of Markov model for a General Purpose Safety Configured PLC, identification of typical BMS Safety Instrumented Functions (SIF) and subsequent Safety Integrity Levels (SIL) determination will be discussed in detail.

Especially when considering SIL 2 level applications, extra validation steps are required to ensure the suitability of the logic solver for that Safety Integrity Level. Because the General Purpose Safety Configured PLC manufacturer has not ensured system suitability for safety applications per IEC 61508 / IEC 61511, extra validation steps required must be performed by the end-user / operating companies. This effort will drastically influence the cost of ownership. A cost benefits justification for re-using or replacing existing General Purpose Safety Configured PLC's will also be discussed in this paper.

2. Hot-Standby PLC vs. fully redundant Safety PLC for Safety Instrumented Function implementing

   <u>Abstract</u>

   For the lower Safety Integrity Levels, SIL 1 and SIL 2, as defined by IEC61508 and ANSI/ISA S84.01, many end-users / operating companies tend to focus on the use of a general purpose PLC instead of a Safety PLC as the logic solver in their Safety Instrumented Functions. In order to improve the reliability of the general purpose PLC, the use of a Hot-Standby PLC is often suggested.

   This paper will describe the advantages and disadvantages of a Hot-Standby general purpose PLC when compared to a general purpose PLC, simplex Safety PLC, and ultimately a fully redundant Safety PLC. The difference in system behavior for a general purpose PLC, a Hot-Standby PLC, and the simplex or fully redundant Safety PLC will be described using Markov models derived for each of the logic solver configurations. Using these models the performance parameters, PFDavg and MTTFS, for the configurations will be calculated.

   An important aspect why end-users / operating companies are more favorable of the general purpose Hot-Standby PLC compared to a fully redundant Safety PLC is the perceived cost of ownership. Especially when considering SIL 2 level applications, extra validation steps need to be made to ensure the suitability of the logic solver for that Safety Integrity Level. The Safety PLC manufacturer has performed these additional validation steps, whereas the general purpose PLC manufacturer has not. This means that the extra validation steps need to be performed by the end-user / operating companies which will drastically influence the cost of ownership. The cost benefits of each of the logic solver configurations will also be discussed in this paper.

3. Burner Management Flame Detection Requirements, Exceptions and Advances

   <u>Abstract</u>

   The use of flame detection in burner management systems has undergone some serious change over the years, both in the standards and codes we utilize in this industry and the technological advancements that have been realized. While some users continue to resist the requirements being imposed upon them, others are embracing the new technological advances that have been made in this area of instrumentation.

   Users upgrading their systems to meet new federally mandated NOX requirements are facing new challenges when trying to utilize their existing flame detection systems.

   Other users are fighting serious "cost of ownership" issues when trying to outfit their multiple burner platforms with the "required" flame detection systems.

   This paper will discuss the requirements and all-important exceptions that are part of the current codes and standards in this field. Advances made in recent years in flame detection and BMS upgrade issues will form the second half of this paper.