



## Why does your BPCS is not reliable as you'd like to be? / Por que o seu DCS não é confiável como você gostaria?

Autor: Elisio Carvalho Silva

Data: 15/07/2015

Safety functions performed by BPCS have to be restricted due to high vulnerability on this control system such as:

- it is possible to place some function in manual by operator;
- Validation, access security and management of change are less restrictive than a safety instrumented system (SIS);
- some companies allow open connection with other data system that can cause serious impact, like viruses;
- the access to the software system is more frequent, hence, the possibility to insert errors in software is increased.

Due to these reasons, the BPCS has to be assumed a dangerous failure rate not better than 10-5 per hour that is equivalent to 0,1 failure rate per year.

To improve the reliability of the BPCS, it is necessary to maintain it in accordance to IEC 61511/ISA 84.01. This decision will make the BPCS more expensive and less flexible to make changes according to daily operational needs.

Then, the better option is using a logic solver exclusively dedicated to protective systems. With this action your unit will become safer, reducing the possibility to occur a major accident.

Os sistemas de controle, DCS por exemplo, não devem fazer as funções de segurança, tal como intertravamentos de segurança, por alguns motivos:

- No DCS é possível colocar alguma função no manual pelo operador;
- Validação, acesso e gestão de mudança são menos restritivas do que num sistema instrumentado de segurança (SIS);
- Algumas empresas permitem conexão aberta com outros sistemas de dados que podem causar sérios impactos, como vírus;
- O acesso ao software é mais frequente, por isso, a possibilidade de inserir erros no software é aumentada.



Devido a estas razões, para os sistemas de controle (DCS) não se deve assumir uma taxa de falha perigosa melhor do que  $10^{-5}$  por hora, que é equivalente a 0,1 taxa de falha perigosa por ano.

Para melhorar a confiabilidade dos sistemas de controle, é necessário mantê-los em conformidade com a norma IEC 61511 / ISA 84.01. Esta decisão fará com que eles se tornem mais caros e menos flexíveis para fazer alterações de acordo com as necessidades operacionais diárias.

Então, a melhor opção é usar um PLC exclusivamente dedicado para os sistemas de segurança (SIS). Com esta ação, a sua planta vai se tornar mais segura, reduzindo a possibilidade de ocorrer um grande acidente.