ABSTRACT

IEC 61511 Clause 11.2.4 states “If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.” Yet, many control system vendors are selling systems that claim to be capable of being both the BPCS and SIS. They base these claims on IEC 61508 compliance which requires analysis of the system hardware and management of the embedded software. However, the decision to combine the BPCS and SIS is much more complex than simply choosing a suitable hardware and software platform. The likelihood of systemic and human errors greatly influences the actual risk of failure. James Reason's Swiss Cheese model has become the dominant paradigm for analyzing human errors and process safety incidents. This paper will relate the Swiss Cheese model to three categories of automation: 1) separate and independent; 2) not separate and independent; and 3) not separate and not independent. It will discuss how each category affects the holes in the Swiss Cheese and the burden that each category places on the user to maintain functional integrity.