How to achieve sound integrity of safety instrumented function (SIF) when dealing with multiple final elements

Kyu Sun Lee, Ka Ryung Yea, Hee Cheon Cho†,
Heung Sik Kwak
United Pacific PLG
(hccho@unp.co.kr†)

Because of economic, spatial and other constraints, the energy facilities today have become more compact and maintain limited proximity among them. If accident occurs, then, the consequence would be more damaging because of that arrangement. The recognized industry standards, IEC 61508 and 61511 require Safety Instrumented Function (SIF) to be equipped with adequate Safety Integrity Level (SIL) in order to prevent and/or mitigate the hazardous events. It also suggests SIF to be quantitatively verified by analyzing Probability of Failure on Demand (PFD) and Hardware Fault Tolerance (HFT). One important aspect of design is to provide good operability and, because of that, final design may end up with significant number of Final Elements (FE). Often times, more FE mean decreased reliability of SIF. Yet, our goal is to satisfy the expected reliability of SIF (in other word, SIL) in a balanced way such that operability would not be sacrificed too much. In this technical discussion, few ideas on how to achieve required SIL are addressed by giving an example to show how safety and/or PFD can be improved with a HFT reserved for another discussion in the future.