Verification andvalidationofsafetyapplicationsbasedonPLCopensafety function blocks Doaa Soliman n, GeorgFrey

1. Introduction

ProgrammingLogicControllers(PLCs)areincreasinglybeing usedtoimplementsafetyfunctionsforsafetycriticalsystems. Oneofthepreferredprogramminglanguagesinthisareais FunctionBlockDiagram(FBD)accordingtoIEC61131-3(John andTiegelkamp,2001). Therearemanyresearchprojectsinthe fieldofverificationandimplementationoffunctionblockslibraries accordingtothisstandard,e.g. V¨ olkerandKr¨amer(2001) or Song, Koo,andSeong(2004). However,firstly,safetyissuesarenot addressedinIEC61131-3.ThethirdpartofIEC61131dealsonly withfiveprogramminglanguagesusedbyPLCswithoutdistin- guishingbetweencontrol/logicsignalsandsafetysignals.For example,aBooleansafetyrelatedsignalisdeclaredasBOOL accordingtoIEC61131-3,butforasafetyfunctionitshouldbe SAFEBOOLaccordingtoPLCopen.Thisistodifferentiatebetween safetyrelatedsignalsandothersignals.Secondly,PLCprogram- mingsoftwarepackagesprovideonlyfunctionblocklibraries dealingingeneralwithcommunication,mathematicaloperations, logic,andsoon.AsastepforbuildingsafetyapplicationsinIEC 61131-3FBDaccordingtoIEC61508(Bell,2005), PLCopen(2006) specifiesasetofsafetyfunctionblocks(SFBs).Moreover,to demonstratetheusabilityofthedefinedSFBsinreallifesafety applications, PLCopen(2008) developedauserguideline.Several manufacturersofIEC61131programmingtoolshavealready implementedlibrariesaccordingtothisspecification.