

ROCKWELL AUTOMATION
& AUTOMATION WORLD



SAFETY
AUTOMATIONFORUM™

Integrating Machine Safety for OEMs and Manufacturers

Craig Dickson
Operations Manager

Safety Comes Naturally ?



Safety System Design Goals and Challenges

Goal:

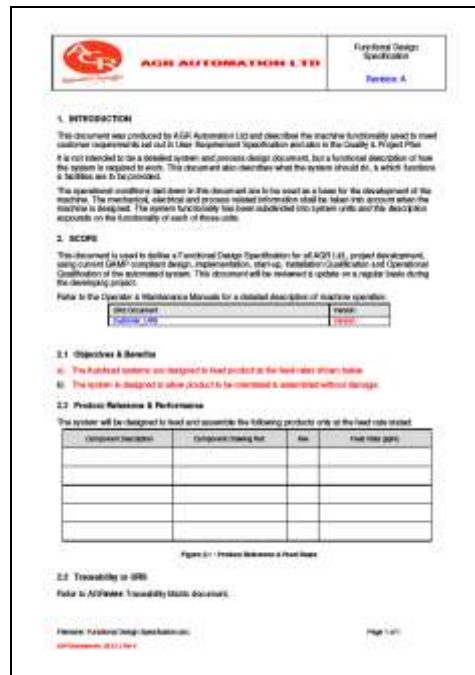
The process of specifying and selection of control systems to deliver automated machinery complying to ISO 13849-1:2006 / IEC 62061

Challenge:

- Deliver a compliant system without compromising the production capability and flexibility of the overall system.
- Deliver a system with capability for expansion and upgrading.
- Deliver a system with global support capability
- Deliver a system with adaptability and scalability

The Process - Steps 1 - 3

1. Completed URS (User Requirements Specification) from the client.
2. FDS (Functional Design Specification) written by AGR and submitted to the client for approval
3. Completion of mechanical concept design, hardware and process specifications, (utilizing GAMP 5 Guidelines)



The Process Cont.- Steps 4 - 7

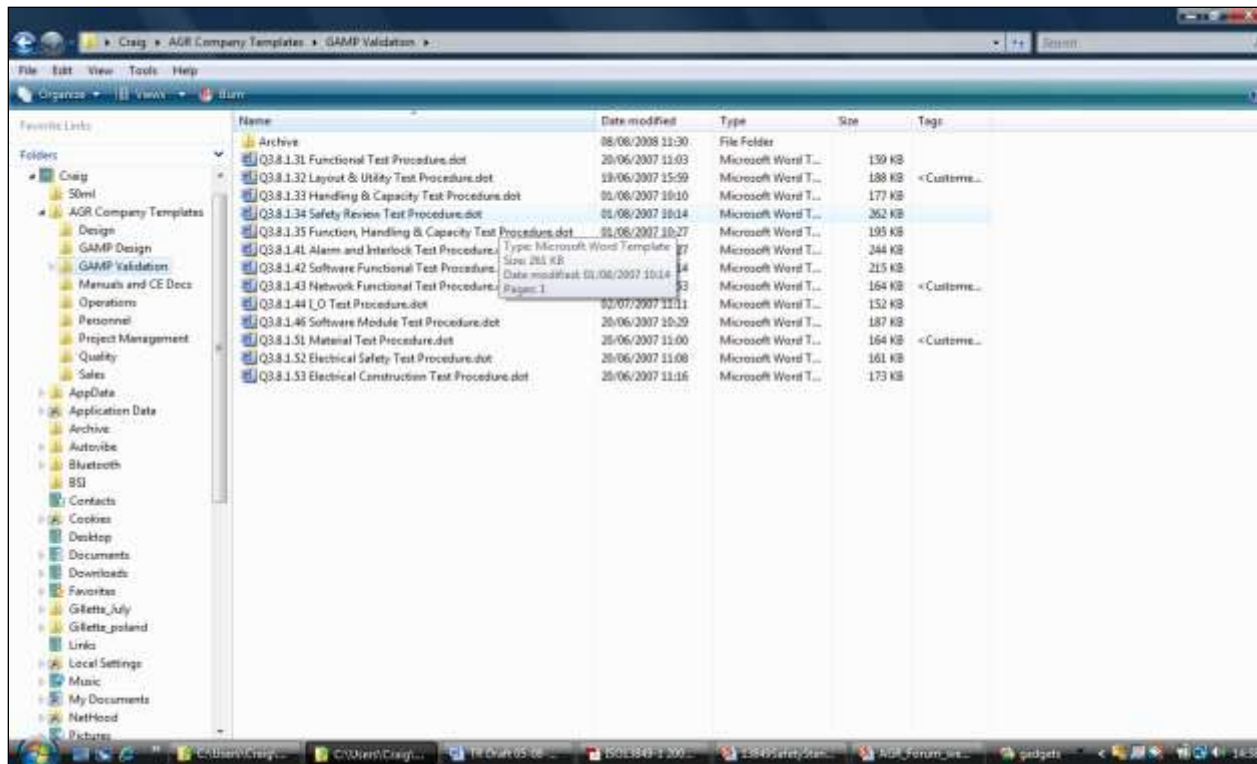
4. Mechanical design concept review meeting and process failure and risk analysis
5. Specification of electrical control equipment, software and safety platform
6. Control hardware and software review meeting and development of FMEA (failure mode and effects analysis)

ASIS AUTOMATION LTD		Safety & Risk Assessment	
Project, Discipline		Revision A	
3.1 Standards Applied			
Number	Year	Title	Effective
001-001-1	1991	General Safety	000403EC
001-001-2	1991	General Safety	000403EC
001-001-3	1991	Safety of machinery with reference to project design (EN 1050)	000403EC
001-001-4	1991	Design of steel work	000403EC
001-001-5	1991	Safety of machinery - emergency stop equipment, electro-mechanical and electrical change	000403EC
001-001-6	1992	Safety	000403EC
001-001-7	1991	Safety of machinery with reference to project design (EN 1050)	000403EC
001-001-8	1991	General Safety	000403EC
001-001-9	1991	General Safety	000403EC
001-001-10	1991	General Safety	000403EC
001-001-11	1991	General Safety	000403EC
001-001-12	1991	General Safety	000403EC
001-001-13	1991	General Safety	000403EC
001-001-14	1991	General Safety	000403EC
001-001-15	1991	General Safety	000403EC
001-001-16	1991	General Safety	000403EC
001-001-17	1991	General Safety	000403EC
001-001-18	1991	General Safety	000403EC
001-001-19	1991	General Safety	000403EC
001-001-20	1991	General Safety	000403EC
001-001-21	1991	General Safety	000403EC
001-001-22	1991	General Safety	000403EC
001-001-23	1991	General Safety	000403EC
001-001-24	1991	General Safety	000403EC
001-001-25	1991	General Safety	000403EC
001-001-26	1991	General Safety	000403EC
001-001-27	1991	General Safety	000403EC
001-001-28	1991	General Safety	000403EC
001-001-29	1991	General Safety	000403EC
001-001-30	1991	General Safety	000403EC
001-001-31	1991	General Safety	000403EC
001-001-32	1991	General Safety	000403EC
001-001-33	1991	General Safety	000403EC
001-001-34	1991	General Safety	000403EC
001-001-35	1991	General Safety	000403EC
001-001-36	1991	General Safety	000403EC
001-001-37	1991	General Safety	000403EC
001-001-38	1991	General Safety	000403EC
001-001-39	1991	General Safety	000403EC
001-001-40	1991	General Safety	000403EC
001-001-41	1991	General Safety	000403EC
001-001-42	1991	General Safety	000403EC
001-001-43	1991	General Safety	000403EC
001-001-44	1991	General Safety	000403EC
001-001-45	1991	General Safety	000403EC
001-001-46	1991	General Safety	000403EC
001-001-47	1991	General Safety	000403EC
001-001-48	1991	General Safety	000403EC
001-001-49	1991	General Safety	000403EC
001-001-50	1991	General Safety	000403EC
001-001-51	1991	General Safety	000403EC
001-001-52	1991	General Safety	000403EC
001-001-53	1991	General Safety	000403EC
001-001-54	1991	General Safety	000403EC
001-001-55	1991	General Safety	000403EC
001-001-56	1991	General Safety	000403EC
001-001-57	1991	General Safety	000403EC
001-001-58	1991	General Safety	000403EC
001-001-59	1991	General Safety	000403EC
001-001-60	1991	General Safety	000403EC
001-001-61	1991	General Safety	000403EC
001-001-62	1991	General Safety	000403EC
001-001-63	1991	General Safety	000403EC
001-001-64	1991	General Safety	000403EC
001-001-65	1991	General Safety	000403EC
001-001-66	1991	General Safety	000403EC
001-001-67	1991	General Safety	000403EC
001-001-68	1991	General Safety	000403EC
001-001-69	1991	General Safety	000403EC
001-001-70	1991	General Safety	000403EC
001-001-71	1991	General Safety	000403EC
001-001-72	1991	General Safety	000403EC
001-001-73	1991	General Safety	000403EC
001-001-74	1991	General Safety	000403EC
001-001-75	1991	General Safety	000403EC
001-001-76	1991	General Safety	000403EC
001-001-77	1991	General Safety	000403EC
001-001-78	1991	General Safety	000403EC
001-001-79	1991	General Safety	000403EC
001-001-80	1991	General Safety	000403EC
001-001-81	1991	General Safety	000403EC
001-001-82	1991	General Safety	000403EC
001-001-83	1991	General Safety	000403EC
001-001-84	1991	General Safety	000403EC
001-001-85	1991	General Safety	000403EC
001-001-86	1991	General Safety	000403EC
001-001-87	1991	General Safety	000403EC
001-001-88	1991	General Safety	000403EC
001-001-89	1991	General Safety	000403EC
001-001-90	1991	General Safety	000403EC
001-001-91	1991	General Safety	000403EC
001-001-92	1991	General Safety	000403EC
001-001-93	1991	General Safety	000403EC
001-001-94	1991	General Safety	000403EC
001-001-95	1991	General Safety	000403EC
001-001-96	1991	General Safety	000403EC
001-001-97	1991	General Safety	000403EC
001-001-98	1991	General Safety	000403EC
001-001-99	1991	General Safety	000403EC
001-001-100	1991	General Safety	000403EC

ASIS AUTOMATION LTD		Safety & Risk Assessment	
Project, Discipline		Revision A	
3.1 Risk Assessment Matrix			
Risk Assessment			Risk Value
Definition	Description		
Event	Something which the prevention is not done		
Failure	The situation that can be recognized as a failure (usually) when a combination of the failure of the related risk probably occurs		
Control point	Any person or person who could be affected by the hazard		
Control measure	Control measure taken to minimize the hazard or to prevent the hazard in accordance to applicable laws		
Qualification of Occurrence (LO)			
Event frequency	Event rate (per annum) occurrence	0.001	
High severity	High severity consequences	1	
Failure	Failure consequences	1.0	
Control	Control consequences	0.1	
Control measure	Control measure consequences	0.01	
Control	Control consequences	0.001	
Frequency of Exposure (FE)			
Annually		0.01	
Monthly		0.1	
Weekly		0.5	
Daily		1.0	
Hourly		24	
Continuously		8760	
Degree of Possibility (DP)			
Extremely Rare		0.01	
Unlikely (1 in 100)		0.01	
Minor (1 in 1000)		0.001	
Major (1 in 10000)		0.0001	
Critical (1 in 100000)		0.00001	
Number of Persons Exposed (NP)			
1		1	
2 to 5		2.5	
6 to 10		5	
11 to 20		10	
21 to 50		25	
51 to 100		50	
101 to 200		100	
201 to 500		250	
501 to 1000		500	
1001 to 2000		1000	
2001 to 5000		2500	
5001 to 10000		5000	
10001 to 20000		10000	
20001 to 50000		25000	
50001 to 100000		50000	
100001 to 200000		100000	
200001 to 500000		250000	
500001 to 1000000		500000	
1000001 to 2000000		1000000	
2000001 to 5000000		2500000	
5000001 to 10000000		5000000	
10000001 to 20000000		10000000	
20000001 to 50000000		25000000	
50000001 to 100000000		50000000	
100000001 to 200000000		100000000	
200000001 to 500000000		250000000	
500000001 to 1000000000		500000000	
1000000001 to 2000000000		1000000000	
2000000001 to 5000000000		2500000000	
5000000001 to 10000000000		5000000000	
10000000001 to 20000000000		10000000000	
20000000001 to 50000000000		25000000000	
50000000001 to 100000000000		50000000000	
100000000001 to 200000000000		100000000000	
200000000001 to 500000000000		250000000000	
500000000001 to 1000000000000		500000000000	
1000000000001 to 2000000000000		1000000000000	
2000000000001 to 5000000000000		2500000000000	
5000000000001 to 10000000000000		5000000000000	
10000000000001 to 20000000000000		10000000000000	
20000000000001 to 50000000000000		25000000000000	
50000000000001 to 100000000000000		50000000000000	
100000000000001 to 200000000000000		100000000000000	
200000000000001 to 500000000000000		250000000000000	
500000000000001 to 1000000000000000		500000000000000	
1000000000000001 to 2000000000000000		1000000000000000	
2000000000000001 to 5000000000000000		2500000000000000	
5000000000000001 to 10000000000000000		5000000000000000	
10000000000000001 to 20000000000000000		10000000000000000	
20000000000000001 to 50000000000000000		25000000000000000	
50000000000000001 to 100000000000000000		50000000000000000	
100000000000000001 to 200000000000000000		100000000000000000	
200000000000000001 to 500000000000000000		250000000000000000	
500000000000000001 to 1000000000000000000		500000000000000000	
1000000000000000001 to 2000000000000000000		1000000000000000000	
2000000000000000001 to 5000000000000000000		2500000000000000000	
5000000000000000001 to 10000000000000000000		5000000000000000000	
10000000000000000001 to 20000000000000000000		10000000000000000000	
20000000000000000001 to 50000000000000000000		25000000000000000000	
50000000000000000001 to 100000000000000000000		50000000000000000000	
100000000000000000001 to 200000000000000000000		100000000000000000000	
200000000000000000001 to 500000000000000000000		250000000000000000000	
500000000000000000001 to 1000000000000000000000		500000000000000000000	
1000000000000000000001 to 2000000000000000000000		1000000000000000000000	
2000000000000000000001 to 5000000000000000000000		2500000000000000000000	
5000000000000000000001 to 10000000000000000000000		5000000000000000000000	
10000000000000000000001 to 20000000000000000000000		10000000000000000000000	
20000000000000000000001 to 50000000000000000000000		25000000000000000000000	
50000000000000000000001 to 100000000000000000000000		50000000000000000000000	
100000000000000000000001 to 200000000000000000000000		100000000000000000000000	
200000000000000000000001 to 500000000000000000000000		250000000000000000000000	
500000000000000000000001 to 1000000000000000000000000		500000000000000000000000	
1000000000000000000000001 to 2000000000000000000000000		1000000000000000000000000	
2000000000000000000000001 to 5000000000000000000000000		2500000000000000000000000	
5000000000000000000000001 to 10000000000000000000000000		5000000000000000000000000	
10000000000000000000000001 to 20000000000000000000000000		10000000000000000000000000	
20000000000000000000000001 to 50000000000000000000000000		25000000000000000000000000	

The Process Cont.- Steps 7 - 9

7. Application of a Safety Risk Assessment and FMEA in determining safety category (Category or PL)
8. Completion of programming of process software modules in PLC and safety PLC
9. Testing and validation of process and safety systems



Influencing factors in Determination of Hardware and Software Selection

1. Category or SIL level requirement
2. System size/ footprint
3. System complexity
4. Process complexity
5. Zoning requirements
6. Smart or dumb safety monitoring
7. Cost

System Complexity

- Achieving CAT 3 on small simple systems can be cost effective and relatively easily achieved without the use of a safety PLC
- Achieving CAT 3 on a complex system is more difficult but can be made simpler by utilizing a safety PLC. This option offers the functionality to achieve the CAT3 level without a loss of performance from the Automation System.
- Utilizing the safety PLC also delivers a scalable solution easily and quickly modified when system upgrades are applied.

Complex Automation Employing Safety PLC

Complex Zoned Automated Assembly System



HMI Displaying Zoning



Master PLC with Safety PLC fitted



Distributed Safety I/O

SmartPod - Multi-Disciplined

AGR Automation

- Multi-Disciplined Manufacturing
- Assembly
- Quality
- Profiling
- Gluing
- Utilising the Rockwell Control Platform

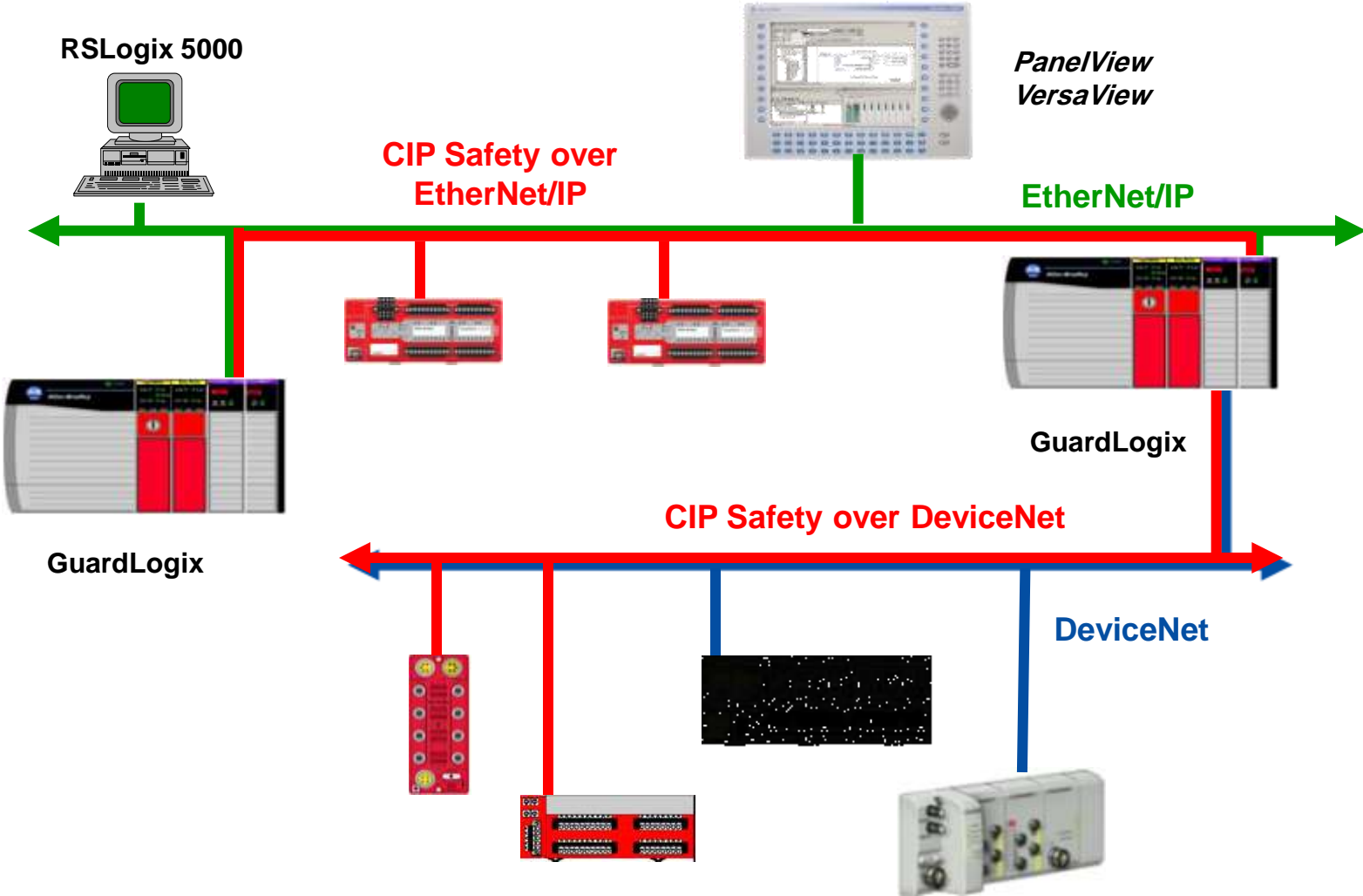
Rockwell Automation

- Multi-Disciplined Control
- Sequential Control
- Motion Control
- Drives Control
- Process Control
- AND Safety Control on the same platform

Machine Safety and Machine Development

- **Safety LifeCycle**
 - Safety is an integral part of the machine design process
- **Functional Safety**
 - The concept of functional safety is changing the behavior of users and designers of automation systems
 - Functional safety standards are no longer national, but international i.e. IEC 62061
- **Automation**
 - Today's standards now allow safety systems to adopt state of the art technology
- **Integration**
 - The better safety is integrated into the control system, the more in-control a machine is, the safer it is.
- **Quality and compliance**
 - Increased data access and logging through an information enabled platform allow an easier route to confirm quality and compliance of product

GuardLogix Architecture



SmartPod - Information Enabled

- Standard and safety messaging on the same network
- Transparent and seamless access to standard and safety information throughout the complete network
- Allows for increased diagnostics and hence improved OEE as the ability to identify problems are greatly increased
- Easily accessible information allows for condition monitoring, historical trending, etc, to be carried out
- The trend in safety is moving from reactive to predictive, and an integrated information enabled machine allows for additional permissive signals from air/oil pressure, etc, to be used in a safety routine

One Platform now does it all

- Standard control and safety control in **one** controller
- Standard controllers and safety controllers in a **common** chassis
- Standard control and safety control on **common** networks



SmartPod - Flexible Modular Platform

- Modular design allows flexibility, future proofing, commonality, etc
- Spares are standard off the shelf and globally available

AGR Automation

- Modular design of SmartPod allows unrivalled flexibility and saleability for the end user

Rockwell Automation

- Expandable utilizing DeviceNet or Ethernet connectivity



IA Accelerated - Safety

- Faceplates to speed HMI screen development and commonality
 - Safety I/O faceplates
 - Safety Instruction faceplates

The image displays three HMI faceplates for safety modules, each titled 'Safety Node Name' with a close button (X).

The top-left faceplate shows a 'Probable Cause' section with the message: "The configuration is invalid." It includes a bell icon, a hand icon, and three columns: IN (0-7), IN (8-15), and OUT (0-7).

The middle-left faceplate shows a 'Recommended Action' section with the message: "Configure the module correctly." It includes a bell icon, a hand icon, and three columns: IN (0-7), IN (8-15), and OUT (0-7). At the bottom, there are buttons for 'Circuit Reset' (green) and 'Fault Reset' (red).

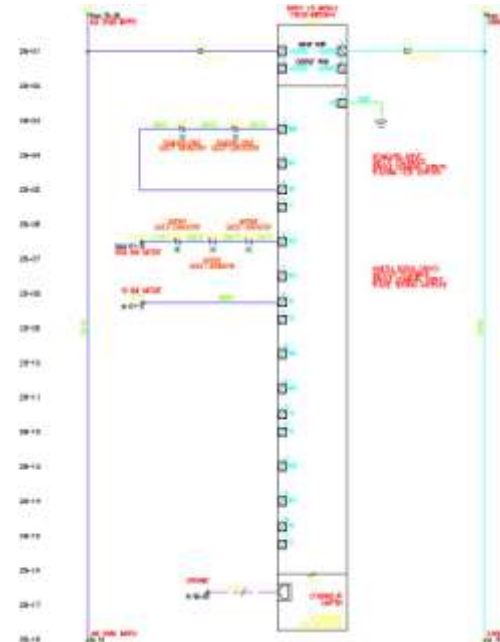
The right faceplate shows a 'Help - Manual Control' section with a legend: SI = State indicator, DI = Demand indicator, CI = Cycle indicator. Below the legend is a table of input status:

Input	State	Demand	Cycle	Device Description
0	Red	Grey	Red	Input 0
1	Red	Grey	Red	Input 1
2	Grey	Grey	Grey	Input 2
3	Orange	Orange	Grey	Input 3
4	Red	Orange	Red	Input 4
5	Red	Orange	Red	Input 5
6	Grey	Grey	Grey	Input 6
7	Orange	Grey	Grey	Input 7

At the bottom of the right faceplate, there are buttons for 'Circuit Reset' (green) and 'Fault Reset' (red).

IA Safety Accelerator - System Design Guidelines/Tools

- A suite of safety components that assist in safety Logic, I/O configuration, field device wiring (CAD drawings), HMI Diagnostic Screens.
- A device selection guide based on safety requirements.
- FactoryTalk View Faceplates for GuardLogix Controller and Safety I/O Blocks including companion Logix Add-On Instructions.



GuardLogix - Summary

- GuardLogix - Safety Integrated Controller
 - Single controller view of standard and safety
 - GuardLogix based on standard Logix technology
- Common Programming / Design / Configuration Tool
 - RSLogix 5000+ safety extensions
 - Standard control via RLL, FBD, SFC, STL and safety control via RLL
- Leverages standard ControlLogix hardware
 - Racks, power supplies, communications
- Certified safety instructions
 - Simplify user application creation
 - Basic library available at release
- Security environment attached to safety

GuardLogix - Safety PLC

- Reduces engineering efforts
 - Single engineering software RSLogix 5000
 - Less networks and communication between systems
 - Data exchange between standard and safety part using tags
- Reduces maintenance efforts
 - Single network for safety and standard
 - Less training requirements
- Reduces inventory
 - Shares components with ControlLogix
 - Single Network
- Increases diagnostics capability
- Increases flexibility without compromising security

Summary

- By carrying out the required process steps to ensure the system delivered the required Safety PROTECTION Level to protect Operators. Machinery and Process.
- The selection of the Hardware and Software Platform met the requirements of flexibility and expandability of the Smartpod Automation Platform.

Delivered

- Future proof flexibility and re-configurability of the Automation system.
- Cost advantages of manufacture, development and re-validation.
- Improved Safety Performance through the life cycle of the automation System

<http://hseworld.wordpress.com>