REVEAL YOUR **BEST**


Dan Mulholland
Steve Lindsay
24th September 2019

DIGITIZATION OF THE LEGACY

EMEA HUG

Honeywell
Honeywell & Trinity Systems Alliance

• 2018
  – Honeywell and Trinity collaborate and develop a proof of concept that uses iDefine to generate Safety Builder Functional Logic Diagrams

• 2019
  – Honeywell and Trinity enter alliance agreement to design an interface that automates application generation from native xls C&E in iDefine to Safety Manager SC and SIM-SM
  – Presenting joint capabilities at Americas and EMEA User Groups
software tools enabling transformation of automation data into meaningful, useful and actionable information.

... enabling users to

- Regain ownership of legacy systems
- Understand functionality clearly
- Deliver lifecycle engineering efficiencies
- Improve compliance & reduce risk

by MAKING DIGITAL
Keys to Successful Execution
One single source of the truth

Critical risks to manage

- Clarity
- Project Complexities
- Accommodate Changes

Key capabilities to succeed

- Automate Definition & Test
- Improve Communication of Design, Efficiency, Standardization
- Automate Change Impact Analysis And Implementation
The Challenge
Build on good bedrock

- Resolving End User challenges
- Drive accuracy, efficiency & consistency in engineering
- Understanding & Compliance in Maintenance and Modification
- Removing Risk from Critical Activities

Define
Design & Build
Support & Improve (Service Delivery)

Baselining
Define

Efficiency, Accuracy

Evergreen and Future Proof
RECOVERING LEGACY KNOWLEDGE
Making Future Proof
Deviation from Design

- FAT changes
- Build up the plant after design
- Interfaces to other systems causes issues

- P&ID
- C&E
- User Requirements Specification
- Safety Requirements Spec
- Instrument Index
Inputs

Core Functionality
(Unknown)

Outputs
7.4.2.12 Where a pre-existing software element is reused to implement all or part of a safety function, the element shall meet both requirements a) and b) below for systematic safety integrity:

a) meet the requirements of one of the following compliance routes:
   – Route 1S: compliant development. Compliance with the requirements of this standard for the avoidance and control of systematic faults in software;
   – Route 2S: proven in use. Provide evidence that the element is proven in use. See 7.4.10 of IEC 61508-2;
   – Route 3S: assessment of non-compliant development. Compliance with 7.4.2.13.

NOTE 1 Route 1S, 2S and 3S are the element compliance routes of 7.4.2.2 c) of IEC 61508-2 with particular reference to software elements. They are reproduced here for convenience only, and to minimize references back to IEC 61508-2.

NOTE 2 See 3.2.8 of IEC 61508-4. The pre-existing software could be a commercially available product, or it could have been developed by some organisation for a previous product or system. Pre-existing software may or may not have been developed in accordance with the requirements of this standard.

NOTE 3 Requirements on pre-existing elements apply to a run-time library or an interpreter.

b) provide a safety manual (see Annex D of IEC 61508-2 and Annex D of this standard) that gives a sufficiently precise and complete description of the element to make possible an assessment of the integrity of a specific safety function that depends wholly or partly on the pre-existing software element.

7.4.2.2

- The operating systems are likely not the same
- Software does not “wear out”

7.4.2.12

- If 1S is applied then it must be demonstrated that the original software was developed in line with the Functional Safety process of IEC 61508 current edition.
- It would also have to be demonstrated for any modifications implemented
- For any gap then the fall-back position is to follow route 3S.
- Evidence is unlikely to be available.
Costs Associated with Missing IP

Missing 5% of available clear data increases operating costs by 25%

10% data disparity leads to 100% higher operational cost

Most companies operate at between 50% and 80% accuracy

80% related to 900% overspend of associated operational costs

30% of Production Losses were attributed to poor information management

Source: Institute of Configuration Management
Where the IP resides

- 42%, Employee's Brain
- 26%, Paper Documentation
- 20%, Electronic Documentation
- 12%, Electronic Knowledge
Preserving IP through Digital Threads

1. Source logic is automatically converted

2. FB logic is automatically converted to Cause and Effect diagrams

3. Gap analysis

4. Understand and test design before FAT

5. Logic is generated and updated automatically into Safety Manager

6. Documentation is generated automatically

- Review gaps in design
- Review modifications
- Fix systematic errors
- Add new requirements
Preserving IP through Digital Threads

1. Source logic is automatically imported

2. Pattern recognition substitutes obsolete IO typicals with latest IO typicals

3. Upgrade functionality, add diagnostics, comms.

4. Review and Validate functionality

5. Logic is generated and updated automatically into Safety Manager

- Review gaps in design
- Review modifications
- Fix systematic errors
- Add new requirements

6. Documentation is generated automatically

© 2019 by Honeywell International Inc. All rights reserved.
Process Safety Analytics- Functionality Re-Applied

PSS provides an ability use digitized IP to monitor ‘real time’ the SIF performance and produce ‘in use’ reliability data

- Device information
- Cloud Analytics
- Capture proven-in-use data for SIF elements
- Compare SIF types across units and sites
- Track SIF overrides, bypasses across units and sites
- Roll-up reports via email or to your device. Drill-down links
- Cloud Data Consolidation
- Expected SIF Behavior from Cause/Effects
- DCS/SIS Process Data
  - Sequence of Events, Event Log

© 2019 by Honeywell International Inc. All rights reserved.
DIGITIZATION OF DESIGN
Making Future Proof
Traditional delivery based

Accuracy

Time

Commissioning

FAT/Acceptance

Traditional - “Details of the project are not known until the project is completed.”
Threading these Together
A right first time process eliminating cost and schedule risk

1. Design naturally.
2. Emulate and understand / test your design.
3. Documentation is generated automatically,
4. Logic is generated and updated

- No surprises at FAT
- No late changes
- No delayed start-up
Rapid Controls Prototyping

- Simulation / Acceptance
- Commissioning

% Knowledge of System

Accuracy

With a Digitization to a Model

Traditional Process

Traditional

FAT/Acceptance

Automated Process

Time
Takeaway

- Recover existing functional definition
- Understand and train
- Apply new standards
- Digitize

- Assure modification compliance
- Rapid requirements definition and communication
- Accurate & repeatable development
- Digital Traceability
Location in Demo room