Table of Contents

I. Introduction

II. FPGA-based I&C Platforms and its Development Lifecycle

III. Logic Translation Process

IV. Tool Qualification Process

V. Summary

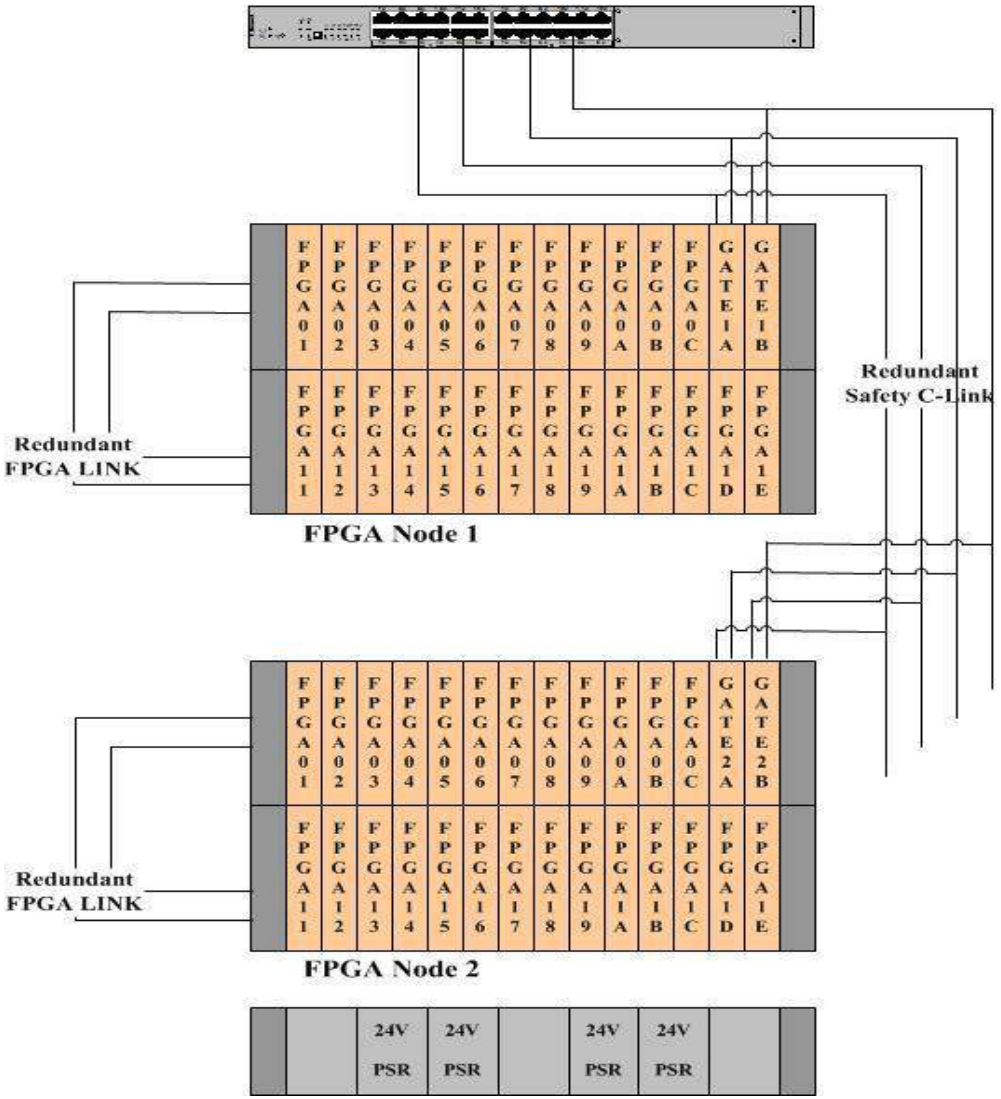
Introduction

- The loop logics used in a digital control system for process controls are usually implemented through CAD drawings or loop schematics.
- To execute loop logic algorithms, the CAD drawings are first translated into logic equations. The logic equations are then compiled into executable binary files that are finally loaded into the controller memory.
- The process of translating CAD drawings into logic equations is laborious and errors prone, especially for a system with a great number of inputs and outputs.
- It is therefore desired to automate the translation process, and achieve error-free implementation and conversion of loop control algorithms, especially for critical loop controls as applied in the nuclear industry, where safety and reliability are always the primary concern.
- For this reason, logic translation process needs to be automatic. The automation tool – One-Step for FPGA Applications has been developed.

Introduction

- However, the developed tool has to contain no errors that may mask errors in the system and software being developed, before the tools are used.
- The automation tool qualification has to be put in place.
- IEEE Std 7-4.3.2-2003 guidance is used during the tool development.
- The tool not only automates the logics translation, but also enhances reliability and therefore errors-free in logics implementation for FPGA applications is achievable.

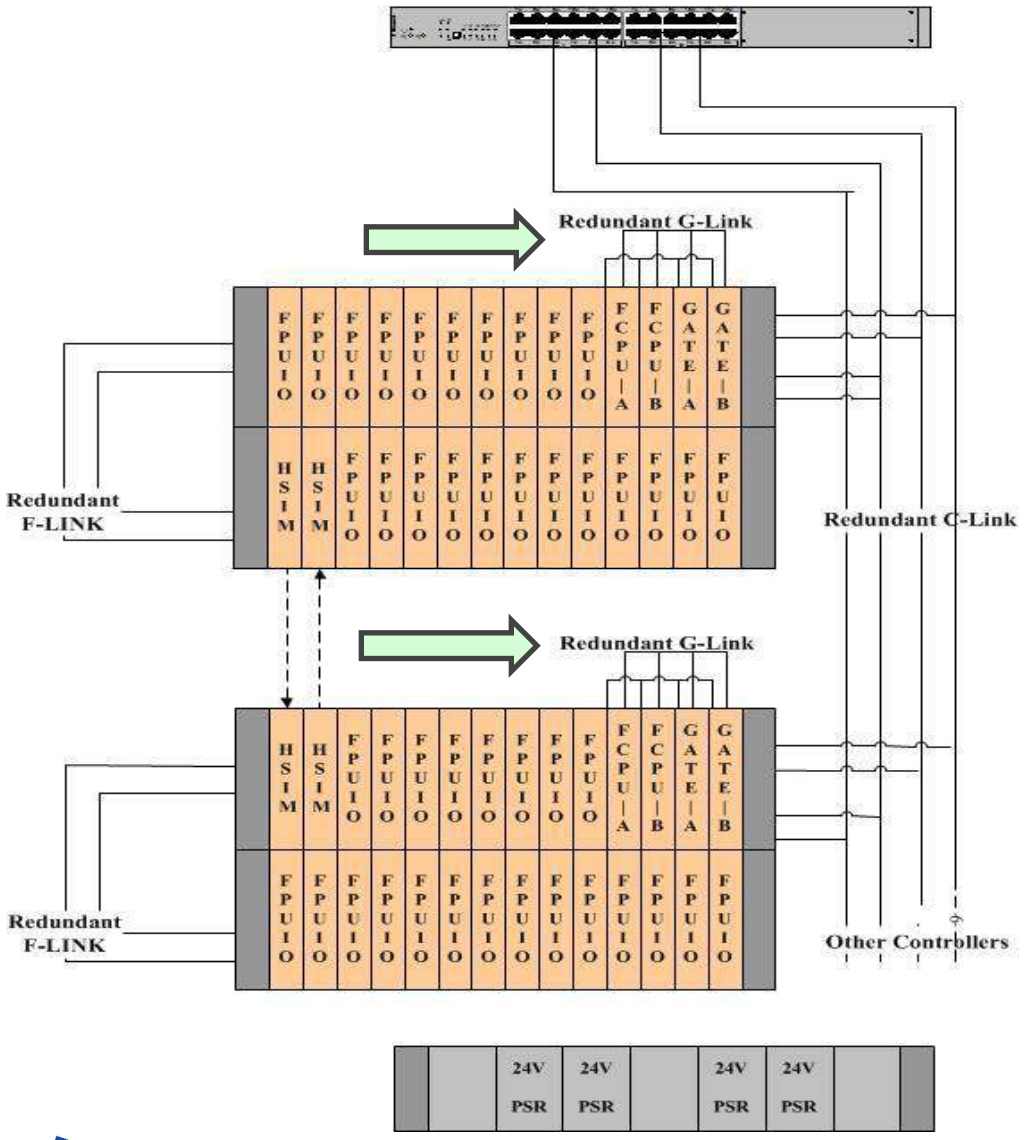
HFC-6000 FPGA System Configuration - I



This diagram illustrates the typical configuration of HFC-6000 FPGA control system with **Distributed Loop Control Scheme** -

- Two (2) or more FPU Control Modules and redundant Gateway Controller communicate with:
  - Safety C-Link to other Nodes
  - F-Link within the FPGA Node
- Each HFC-6000 FPGA Node is capable of connecting up to 26 FPU Control Modules in two (2) racks. All FPUs are connected via 12.5MB F-Link.
- Accessories (i.e. Power Supply, Hubs,…)

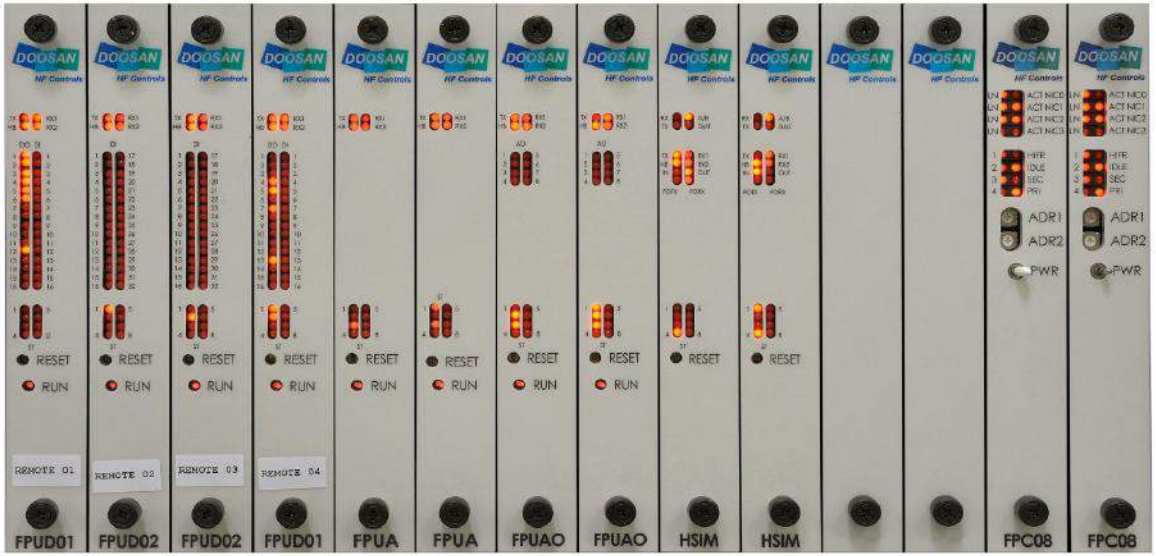
HFC-6000 FPGA System Configuration - II



This diagram illustrates the typical configuration of HFC-6000 FPGA control system with **Centralized CPU (i.e. FCPU) scheme** -

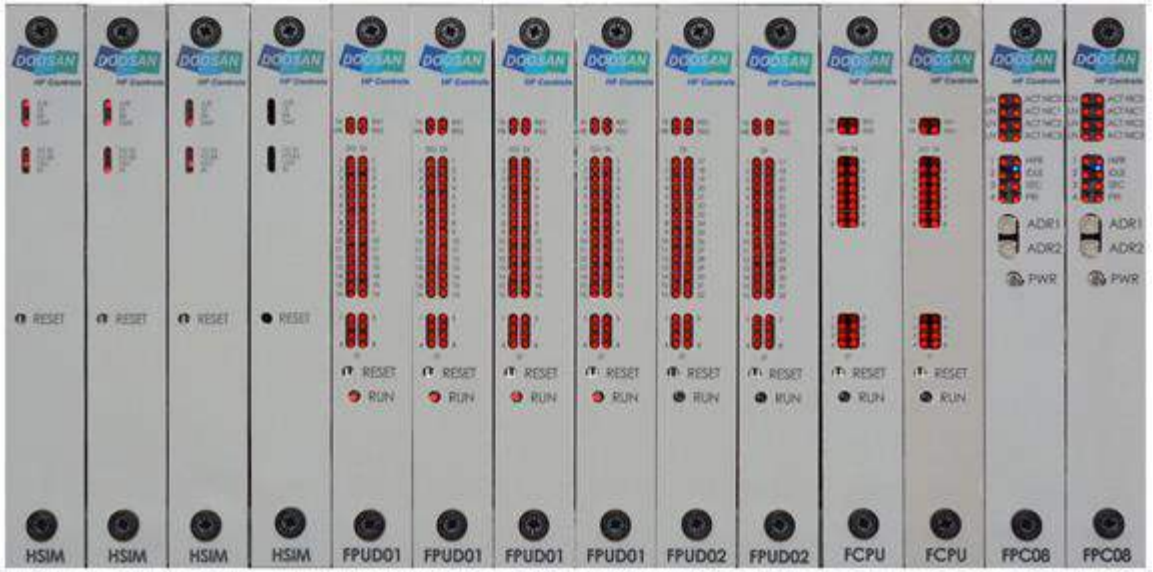
- Redundant FCPU and its FPU I/O Modules with redundant Gateway Controller with:
  - Safety C-Link to other controllers
  - G-Link to Gateway Controller
  - F-Link to its FPU I/O Modules
- Each redundant FCPU is capable of connecting up to 24 FPU I/O Modules in two (2) racks via 12.5MB F-Link.
- Accessories (i.e. Power Supply, Hubs,…)

Rack Configuration with FPU and FCPU



Distributed Logic Control

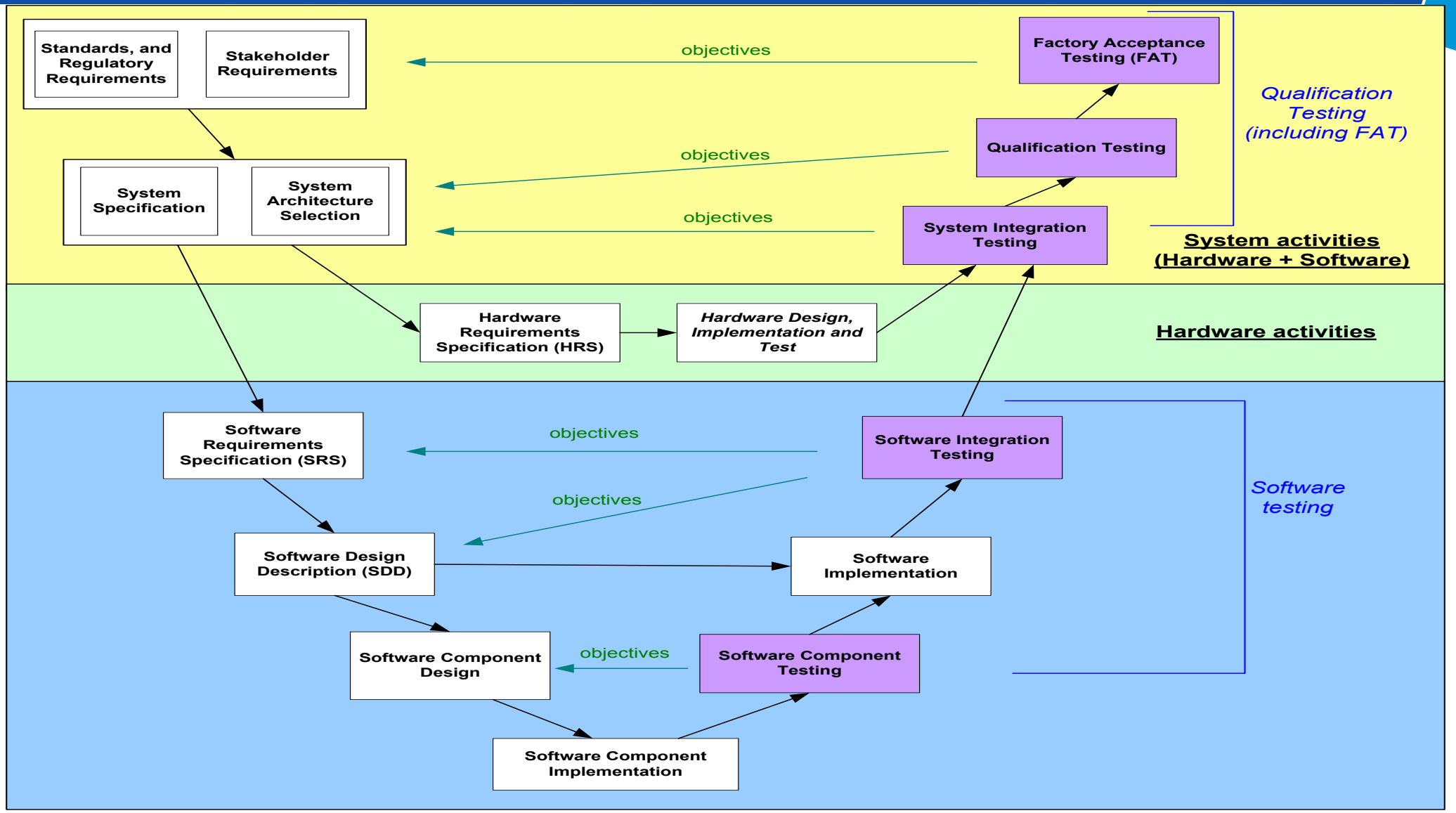
Centralized Logic Control



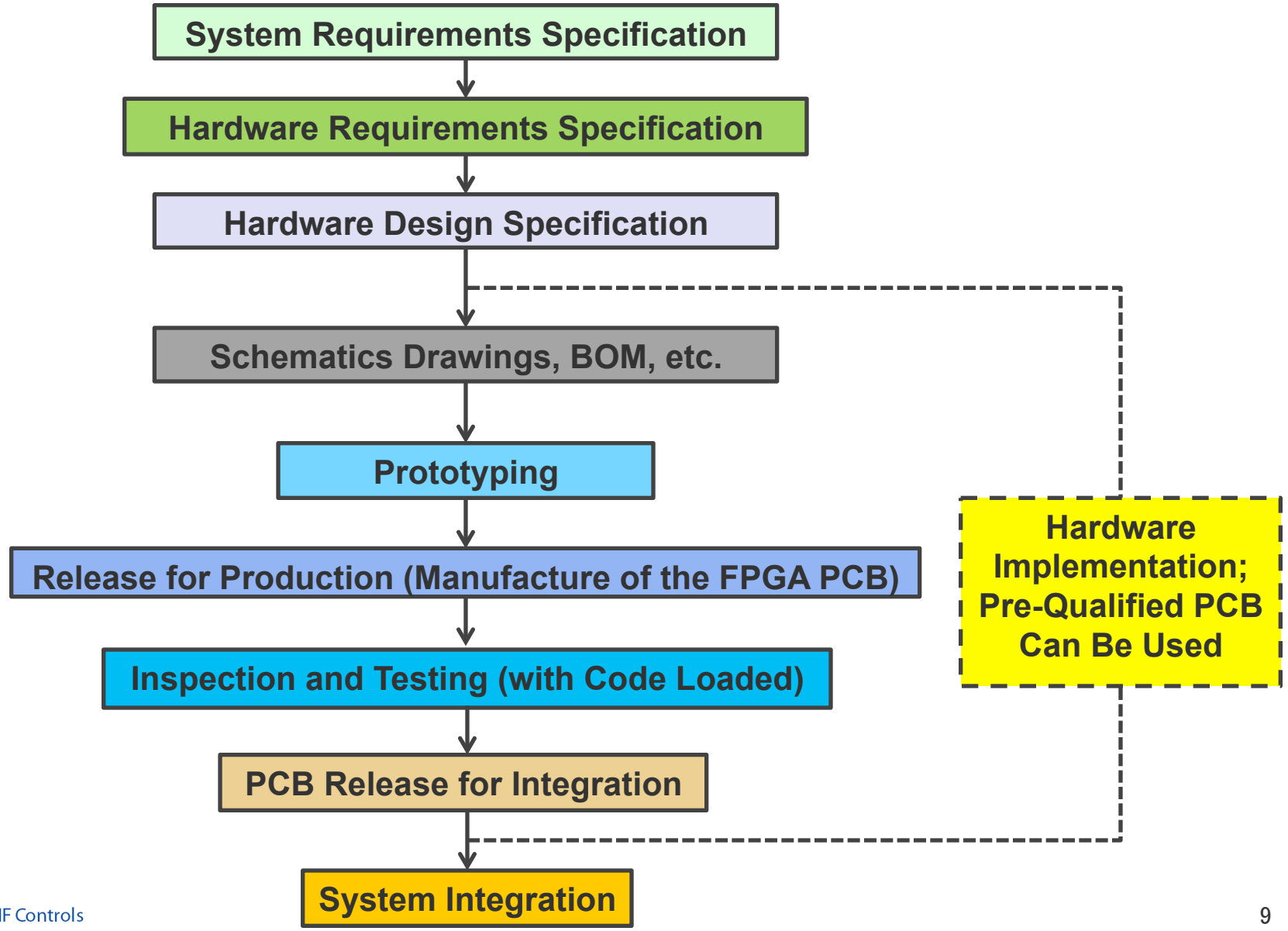
FPGA-based Application Development Lifecycle

1. Development process of FPGA-based application is similar to that of software for microprocessor-based systems.
2. The control system application development starts with system requirements specification.
3. The system requirements are then allocated to the FPGA specific application requirements.
4. FPGA architecture and design specification are then constructed.
5. With the completion of the design, the FPGA implementation is followed.
6. FPGA-based module level testing is planned and executed.
7. FPGA-based modules are integrated with system for system integration testing and acceptance testing.

FPGA-based Application Development Lifecycle and V&V (SW Perspective)



FPGA-based Hardware Development (Lifecycle Process)



FPGA-based Hardware Implementation (EQ Process)

For EQ and EMC qualification of the FPGA-based Control Systems, the TR-107330 requirements are applicable because the FPGA-based systems are the same as the PLCs in terms of digital devices.

1.Environmental Test - conditions presumed to be possible.

2.Seismic Test - ensures that the system continues to operate correctly during the seismic conditions which are provided in EPRI TR-107330.

3.Electromagnetic Interference ensures that the system operate correctly under the temperature and humidity /Radio-Frequency Interference (EMI/RFI) Test - ensures that the system is not susceptible to and does not radiate more than the specified EMI/RFI levels.

4.Surge Withstand Capability Test - ensures that the system withstands the specified surge limits.

5.Electrical Fast Transient / Burst (EFT/B) Test - ensures that the system withstands the specified EFT/B limits.

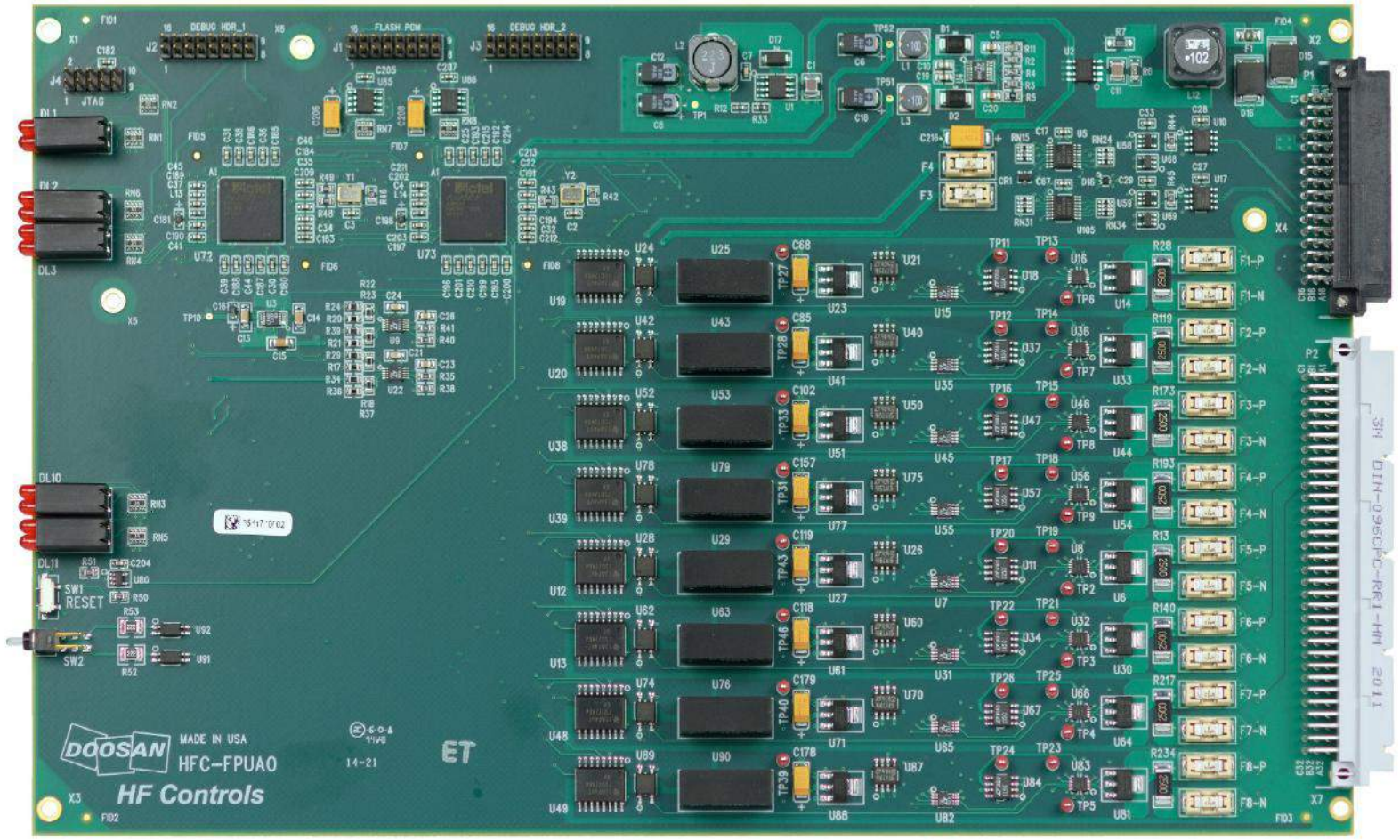
6.Electrostatic Discharge (ESD) Test - ensures that the system continues operation when exposed to the specified ESD levels.

FGPA-based I/O Boards – Digital Input / Output

HFC-FPUD01 Digital Input and Output Module

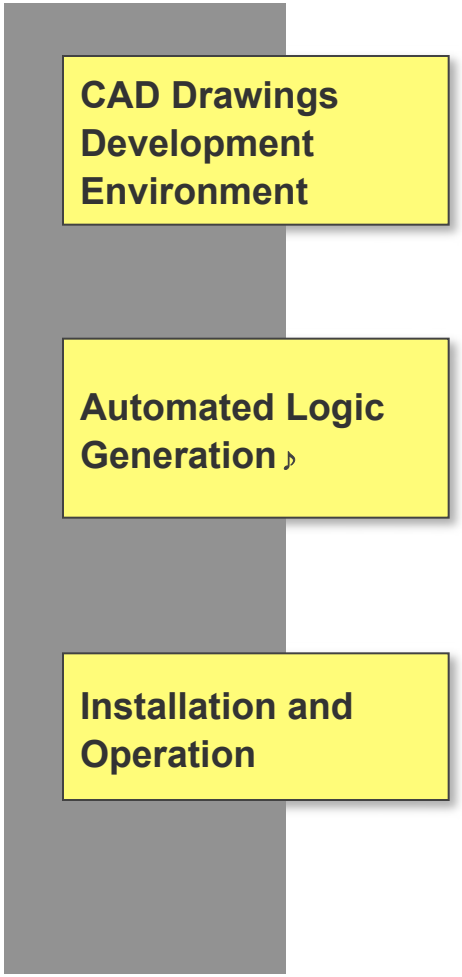
- FPGA based intelligent module diagnostics and self checking capabilities
- Power on reset circuitry with onboard watchdog timer
- Redundant power feeds with onboard diode auctioneering
- Redundant communications capability
- Onboard status LED indications and fuse protection
- 1 millisecond SOE resolution option
- Optional Sequence of Events Recording (SOE)

FGPA-based I/O Boards – Analog Input / Output



Shown is HFC-FPUAO Analog Output Module

HFC Automated Logics Generator *ONESTEP®*



HFC *ONESTEP®* Automated Logic Generator for NPP I&C provides a single documentation source for engineering logics drawings, application programs, and operator interface graphics.

Developed as the nuclear class 1E qualified auto-documentation tool to meet the requirements of NPP I&C Configuration Management and Versions Control

Automated and secured project engineering process minimizes project cost of Engineering, V & V process, production, and on-site installation

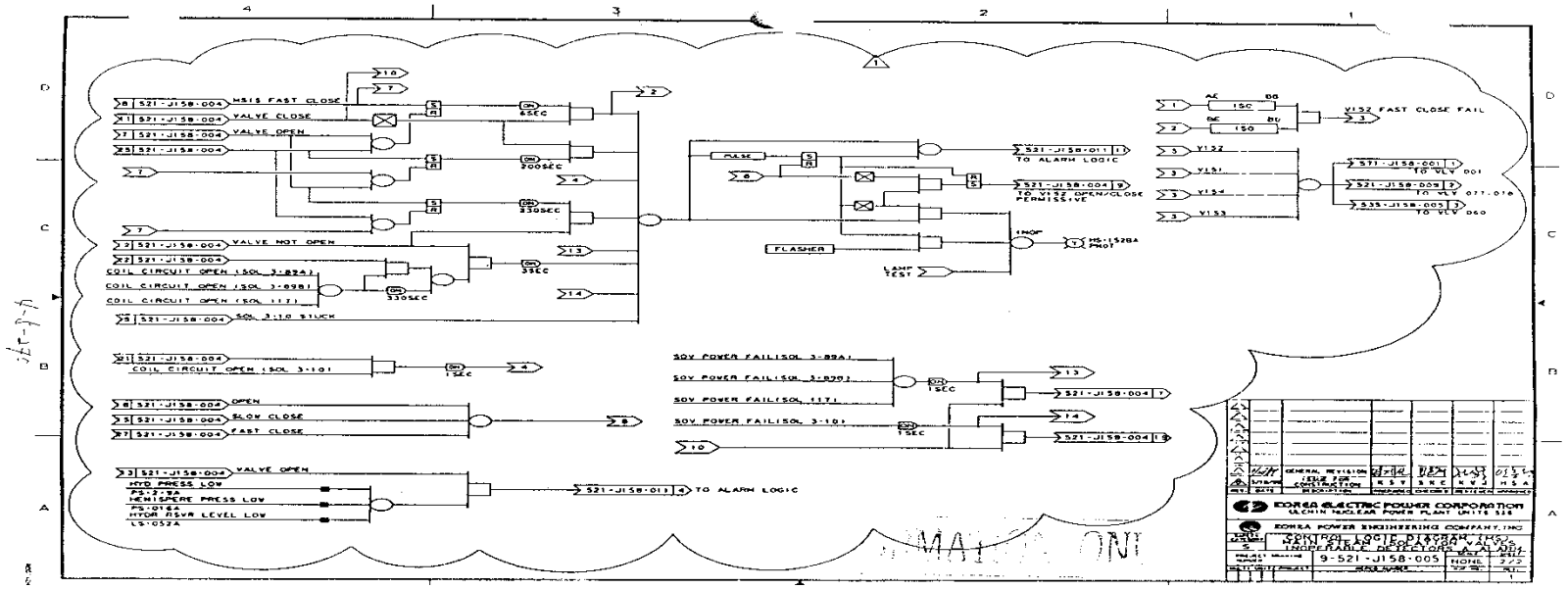
The only efficient and reliable way

- **To create customary "Functional Block" for application logic programming;**
- **To create symbol from typical control logic drawing**
- **To create control logic drawings from multiple symbols.**

"The drawings the engineer designed generated the graphics the operators monitored in plant operation."

The Requirement of Automated PGM Tool -

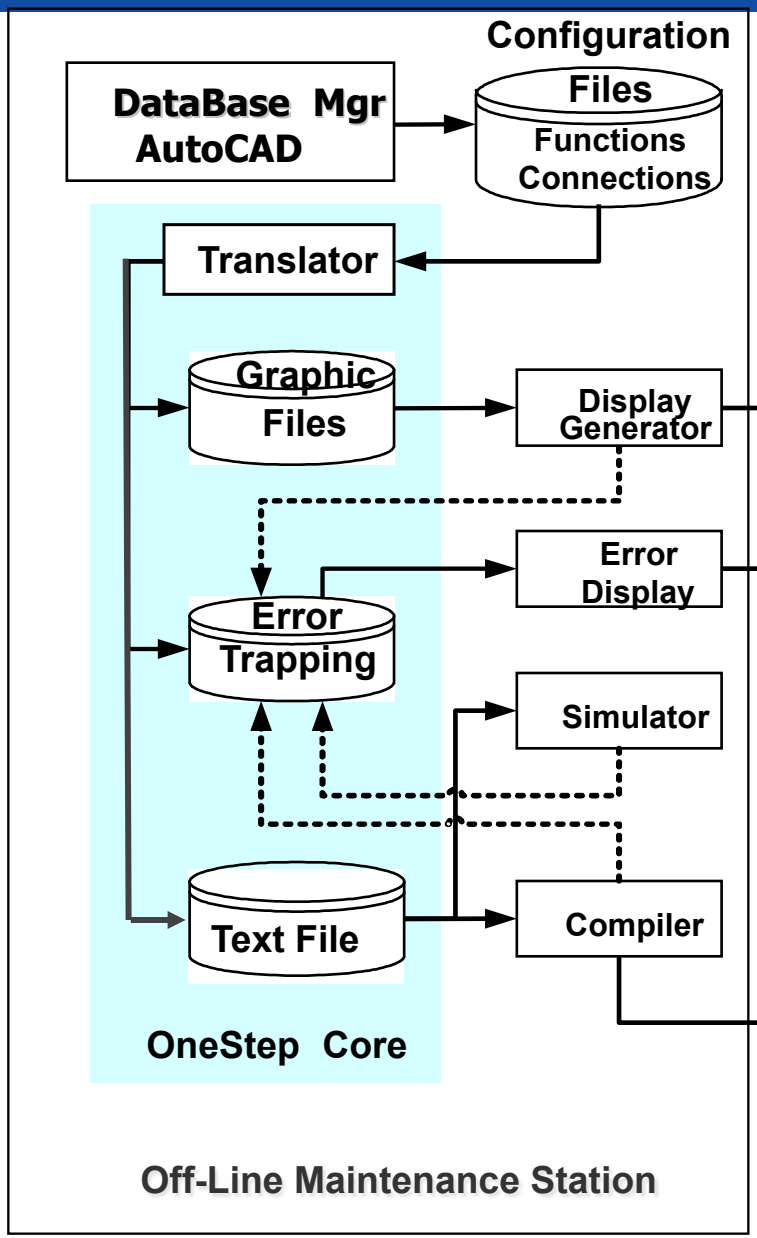
Most of Existing NPP I&C systems were built from integrated analog control circuitry to control device individually. The control and logic diagram represents the control process.



Automated Logics Generator for NPP I&C

FOR:

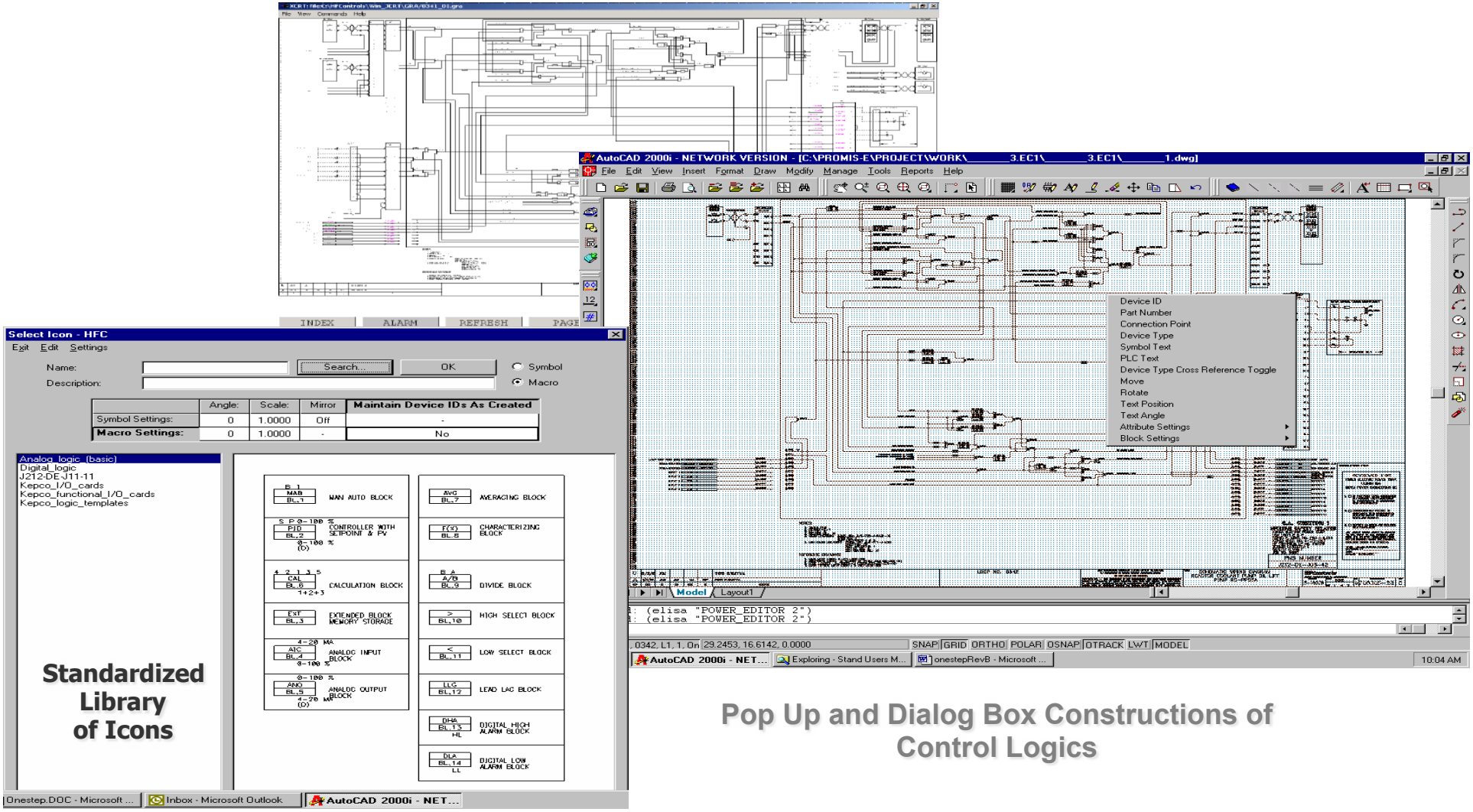
- New Plant I&C System
- Plant I&C System Upgrade
- Retrofit Plant I&C System



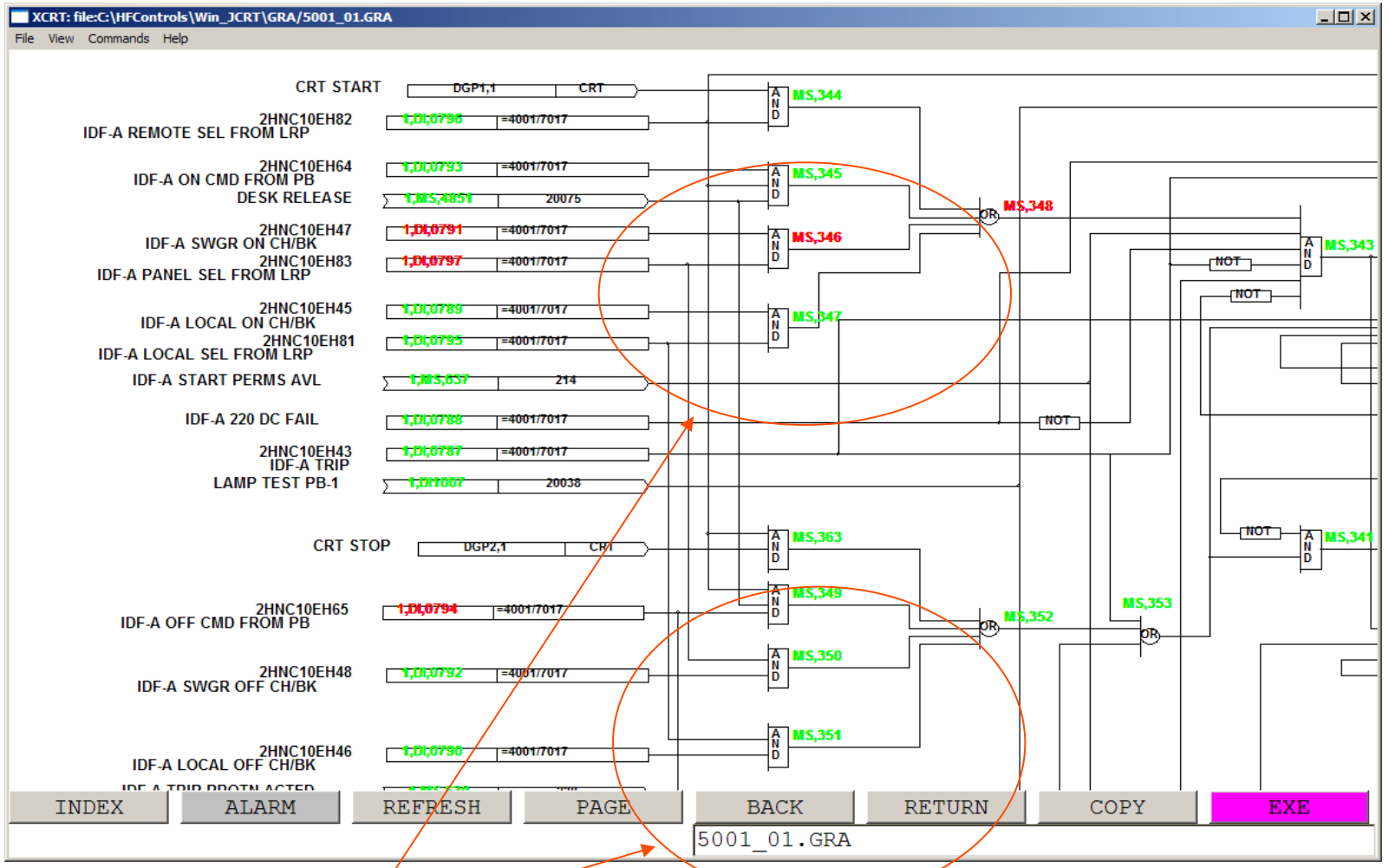
OneStep Software Architecture

DOOSAN HF Controls

Sample Drawings – OneStep™

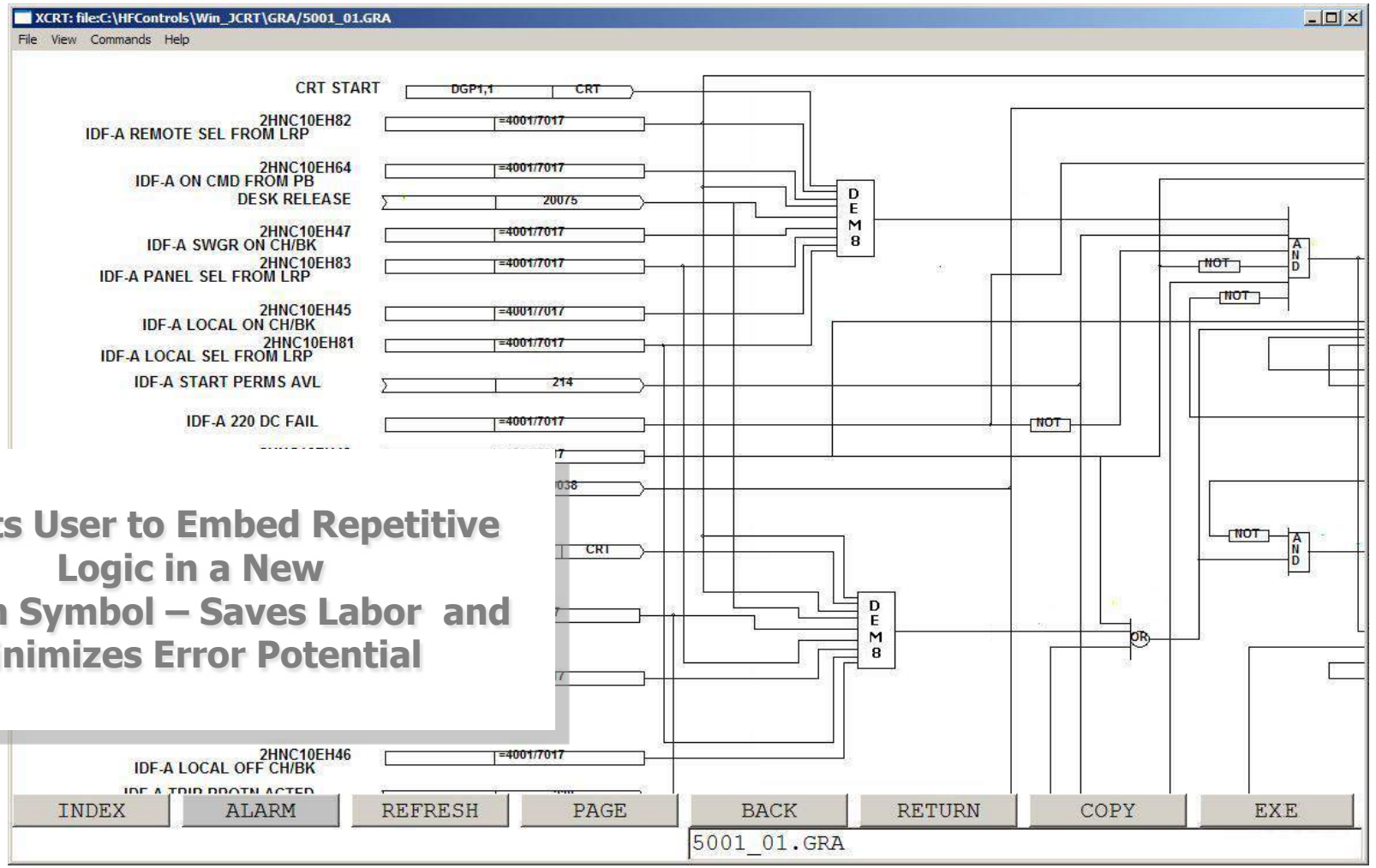


Diagnostic Dynamic Displays

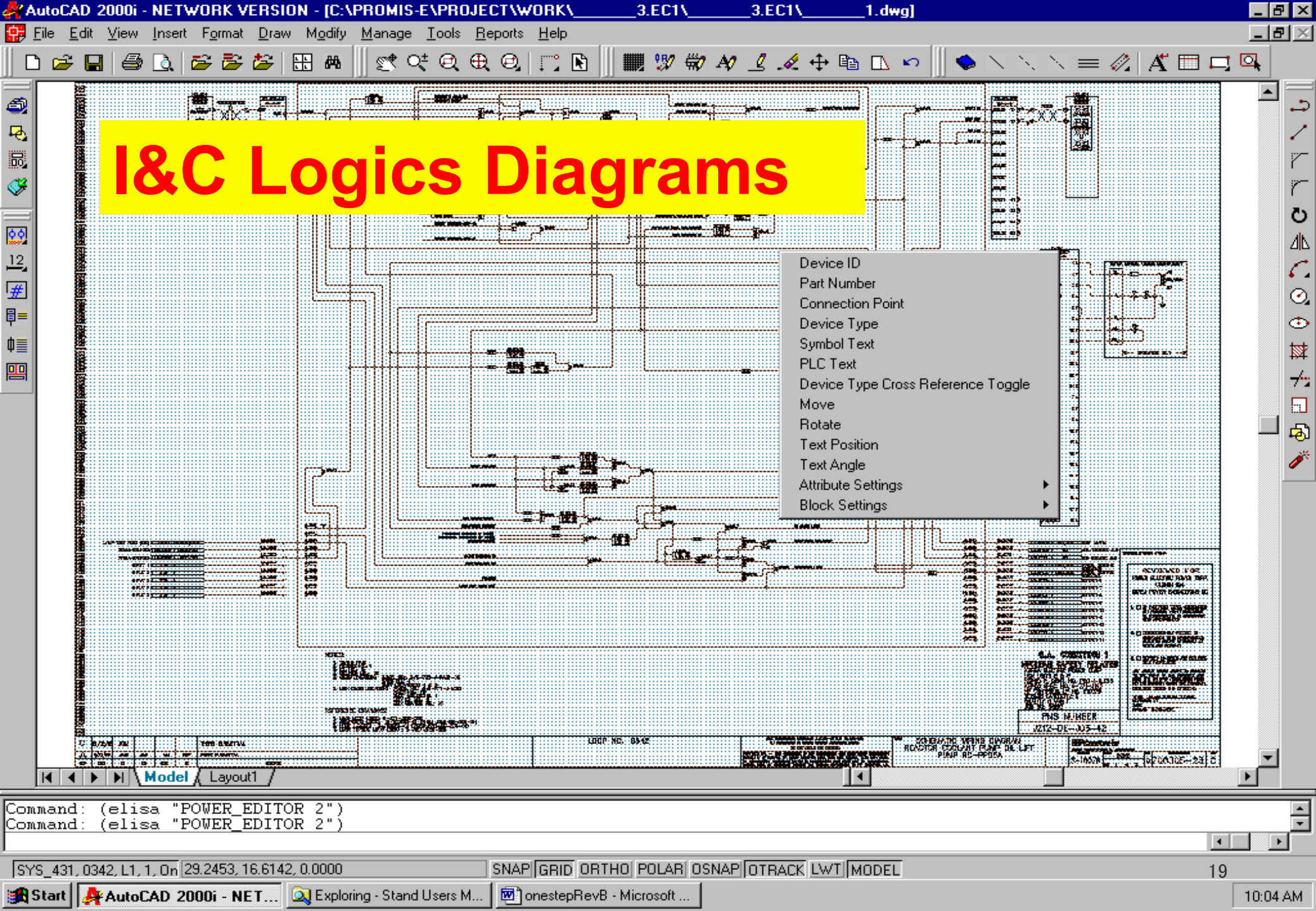


Note: Recurring Logic

Creation of New Functional Blocks



Permits User to Embed Repetitive Logic in a New Custom Symbol – Saves Labor and Minimizes Error Potential


AutoCAD 2000i - NETWORK VERSION - [C:\PROMIS-E\PROJECT\WORK_____3.EC1_____3.EC1_____1.dwg]
File Edit View Insert Format Draw Modify Manage Tools Reports Help
I&C Logics Diagrams
Device ID
Part Number
Connection Point
Device Type
Symbol Text
PLC Text
Device Type Cross Reference Toggle
Move
Rotate
Text Position
Text Angle
Attribute Settings
Block Settings
Model
Layout1
Command: (elisa "POWER_EDITOR 2")
Command: (elisa "POWER_EDITOR 2")
SYS_431, 0342, L1, 1, On
29.2453, 16.6142, 0.0000
SNAP GRID ORTHO POLAR OSNAP OTRACK LWT MODEL
19
Start
AutoCAD 2000i - NET...
Exploring - Stand Users M...
onestepRevB - Microsoft ...
10:04 AM

Eqedt

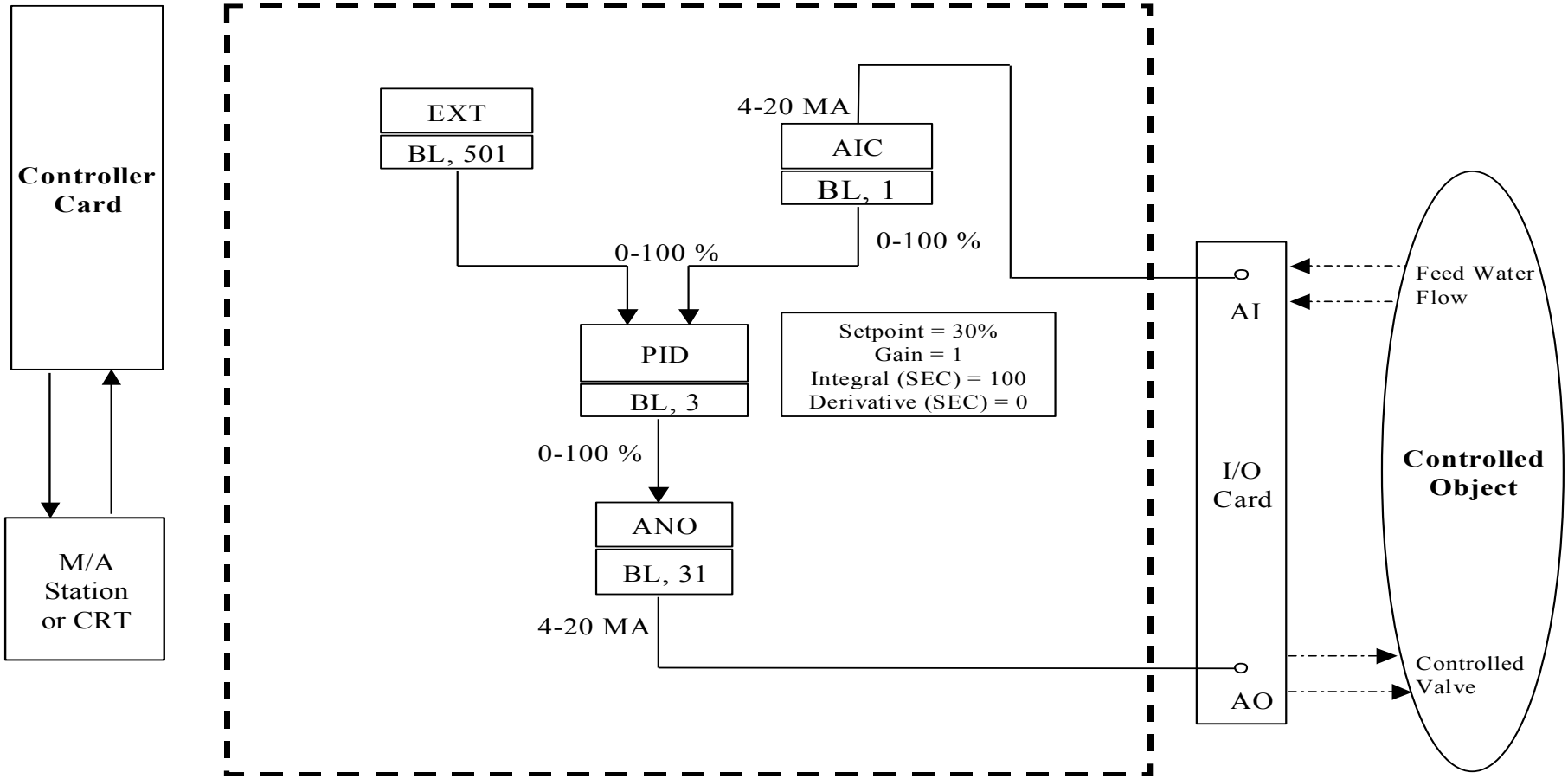
File Edit View Mode Compile Remote Ladder Loop Help

```
FILE NAME: REM02\LOGEQU.02
COMP DATE: 8/8/2003
COMP TIME: 17:30
S.W.VER: 513
CRC VALUE: 47711
FILE SIZE: 9788
AIC(BL, 5, 100)
ANO(BL, 2, 100)
DLA(BL, 6, 100)
CO,99=VA,12
;MAB(BL, 501, 100)
;BL,1 =R1,BL,1
MS,110=/DI,29 & DI,29
FL,17=DI,1 AND /DI,1
DO,3=FL,1
INC CO,100
BL,1=VA,101.5
TIME CO,14
DIAL,1 =CO,14 GT VA,30
            TI,31    P=          10 SEC
            TI,32    P=          10 SEC
            TI,33    P=          15 SEC
            TI,35    P=          10 SEC
            TI,36    P=          10 SEC
            TI,37    P=          15 SEC
            TI,39    P=          10 SEC
```

Qualified Software Tool to Convert Logic into Equations (Analytical Format) and Eventually Binary Files to Be Downloaded into Controllers!

demo REM: 02

An Example for Feed water Control Logics



A Simple Analog Loop Schematics

Control Logics Equations – Analytical Form

To execute the above algorithm, the logic schematics shown in the previous figure is translated into the following logic equations:

BL, 501 = VA, 30, IF (BL, 501 EQ VA, 0.0)(1)

MAGRP(BL, 3, BL, 1, BL, 501, BL, 3, BL, 3) (2)

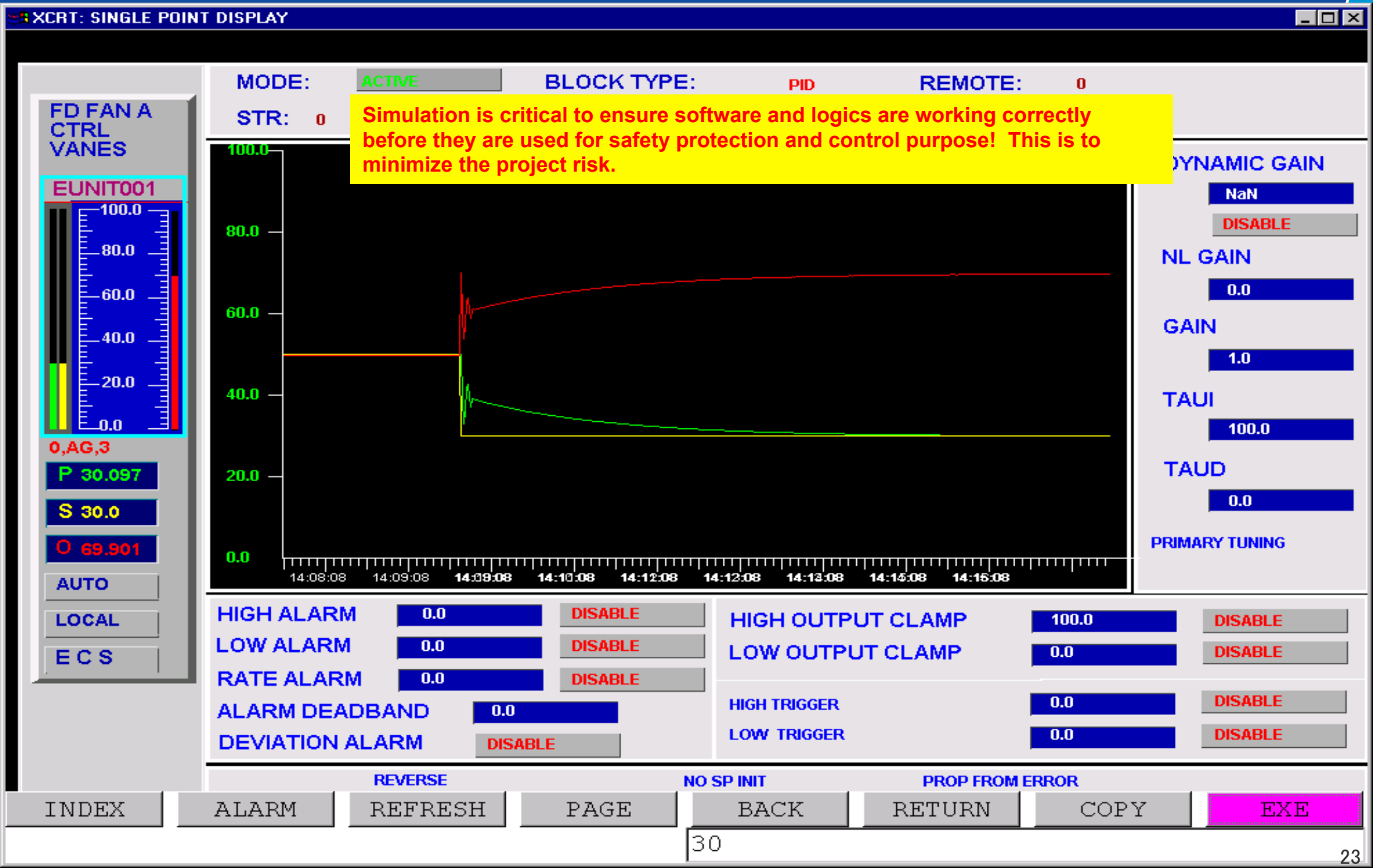
AIC(BL, 1, 100) (3)

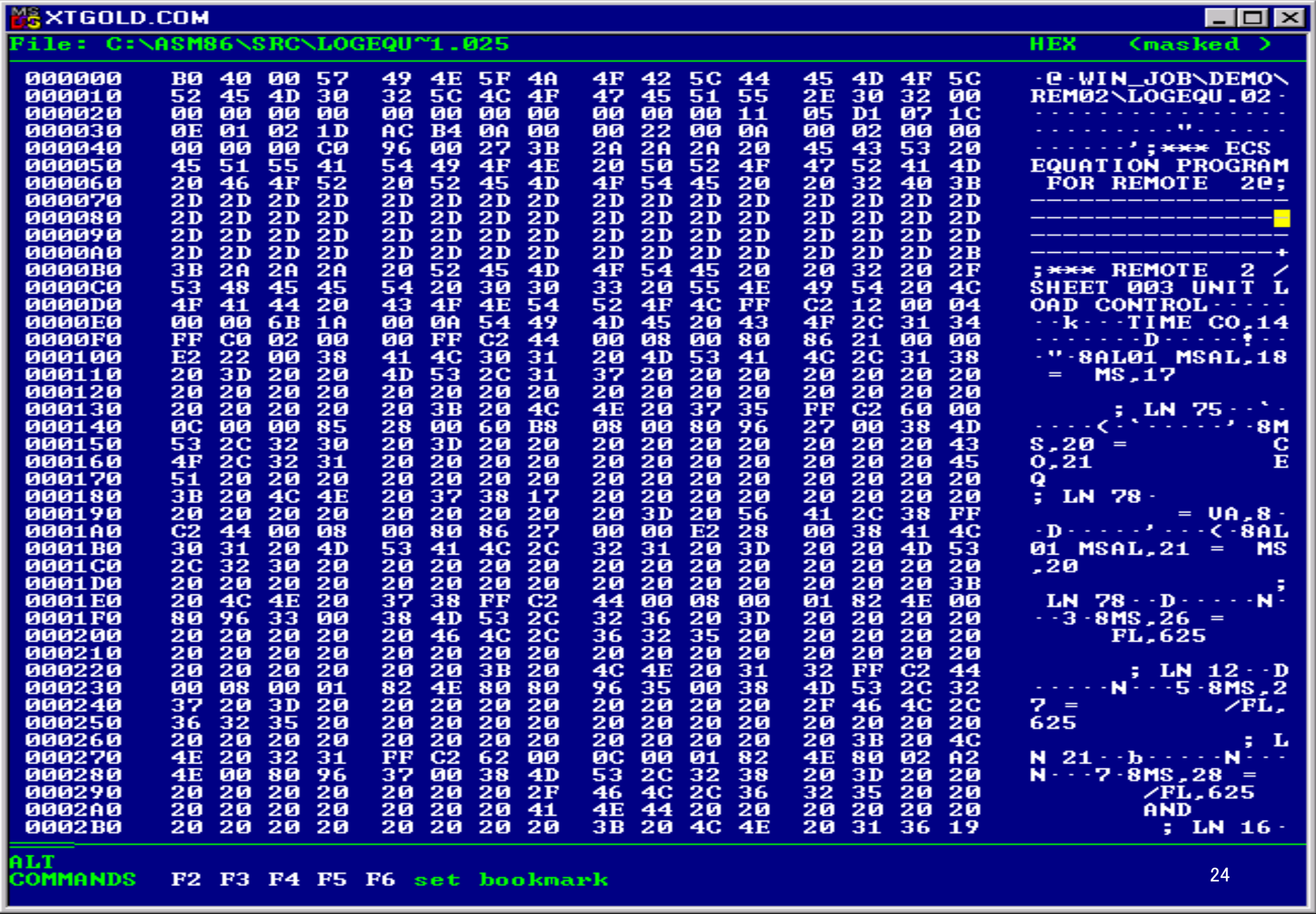
PID(BL, 3, 100) (4)

ANO(BL, 31, 100) (5)

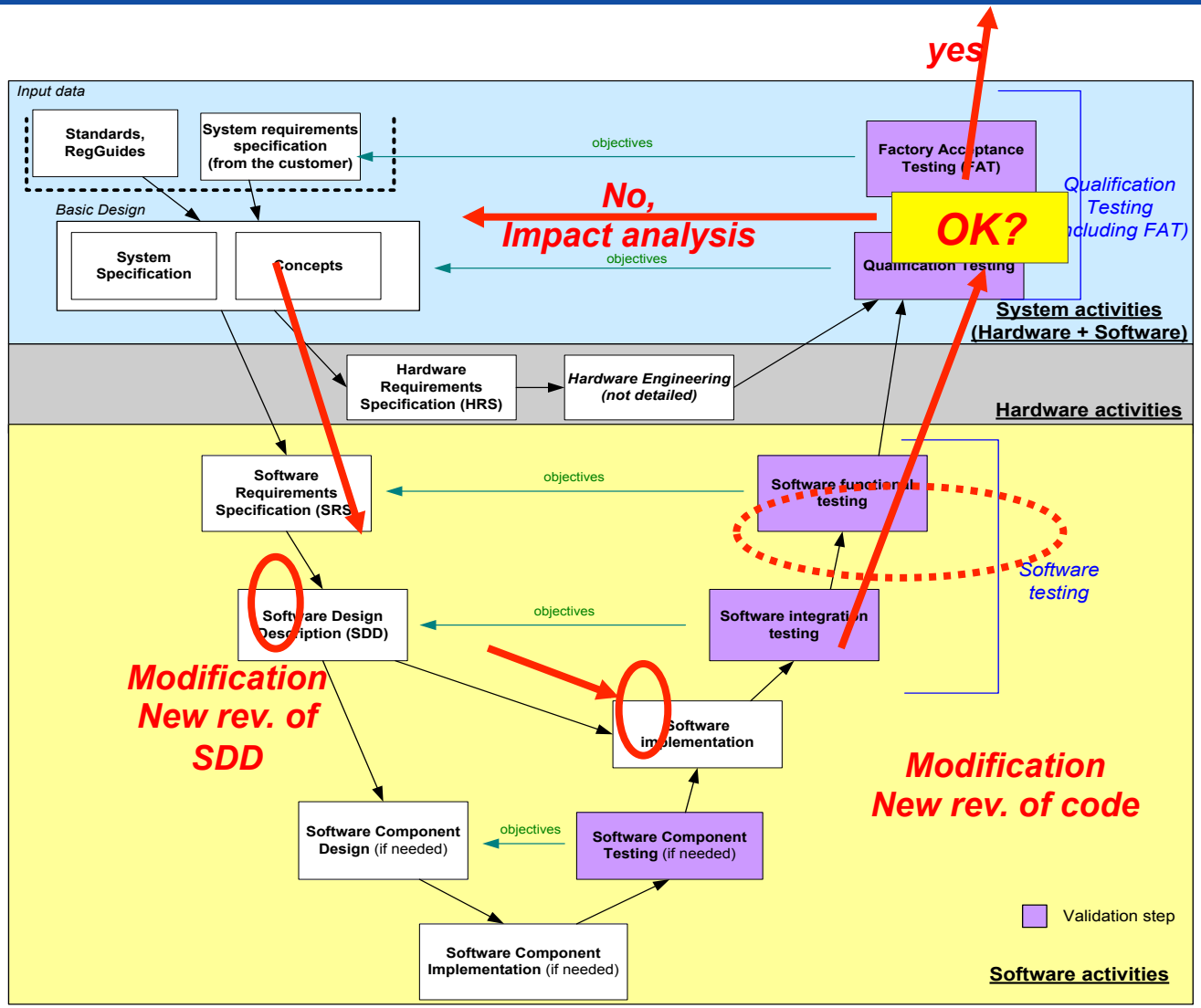
These equations are then compiled into a binary file that is programmed into the onboard EPROM of the controller to be executed.

Simulation to Ensure Logics Correctness




XTGOLD.COM
File: C:\ASM86\SRC\LOGEQU~1.025
HEX (masked)
000000 B0 40 00 57 49 4E 5F 4A 4F 42 5C 44 45 4D 4F 5C
000010 52 45 4D 30 32 5C 4C 4F 47 45 51 55 2E 30 32 00
000020 00 00 00 00 00 00 00 00 00 00 00 11 05 D1 07 1C
000030 0E 01 02 1D AC B4 0A 00 00 22 00 0A 00 02 00 00
000040 00 00 00 C0 96 00 27 3B 2A 2A 2A 20 45 43 53 20
000050 45 51 55 41 54 49 4F 4E 20 50 52 4F 47 52 41 4D
000060 20 46 4F 52 20 52 45 4D 4F 54 45 20 20 32 40 3B
000070 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
000080 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
000090 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
0000A0 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2B
0000B0 3B 2A 2A 2A 20 52 45 4D 4F 54 45 20 20 32 20 2F
0000C0 53 48 45 45 54 20 30 30 33 20 55 4E 49 54 20 4C
0000D0 4F 41 44 20 43 4F 4E 54 52 4F 4C FF C2 12 00 04
0000E0 00 00 6B 1A 00 0A 54 49 4D 45 20 43 4F 2C 31 34
0000F0 FF C0 02 00 00 FF C2 44 00 08 00 80 86 21 00 00
000100 E2 22 00 38 41 4C 30 31 20 4D 53 41 4C 2C 31 38
000110 20 3D 20 20 4D 53 2C 31 37 20 20 20 20 20 20 20
000120 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000130 20 20 20 20 20 3B 20 4C 4E 20 37 35 FF C2 60 00
000140 0C 00 00 85 28 00 60 B8 08 00 80 96 27 00 38 4D
000150 53 2C 32 30 20 3D 20 20 20 20 20 20 20 20 20 43
000160 4F 2C 32 31 20 20 20 20 20 20 20 20 20 20 20 45
000170 51 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000180 3B 20 4C 4E 20 37 38 17 20 20 20 20 20 20 20 20
000190 20 20 20 20 20 20 20 20 20 3D 20 56 41 2C 38 FF
0001A0 C2 44 00 08 00 80 86 27 00 00 E2 28 00 38 41 4C
0001B0 30 31 20 4D 53 41 4C 2C 32 31 20 3D 20 20 4D 53
0001C0 2C 32 30 20 20 20 20 20 20 20 20 20 20 20 20 20
0001D0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3B
0001E0 20 4C 4E 20 37 38 FF C2 44 00 08 00 01 82 4E 00
0001F0 80 96 33 00 38 4D 53 2C 32 36 20 3D 20 20 20 20
000200 20 20 20 20 20 46 4C 2C 36 32 35 20 20 20 20 20
000210 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000220 20 20 20 20 20 20 3B 20 4C 4E 20 31 32 FF C2 44
000230 00 08 00 01 82 4E 80 80 96 35 00 38 4D 53 2C 32
000240 37 20 3D 20 20 20 20 20 20 20 20 20 2F 46 4C 2C
000250 36 32 35 20 20 20 20 20 20 20 20 20 20 20 20 20
000260 20 20 20 20 20 20 20 20 20 20 20 20 20 3B 20 4C
000270 4E 20 32 31 FF C2 62 00 0C 00 01 82 4E 80 02 A2
000280 4E 00 80 96 37 00 38 4D 53 2C 32 38 20 3D 20 20
000290 20 20 20 20 20 20 20 20 2F 46 4C 2C 36 32 35 20
0002A0 20 20 20 20 20 20 20 20 41 4E 44 20 20 20 20 20
0002B0 20 20 20 20 20 20 20 20 3B 20 4C 4E 20 31 36 19
ALT
COMMANDS F2 F3 F4 F5 F6 set bookmark

Configuration Management and Testing



There can be several rounds of testing

Do not lose the control of the configuration during testing!

Development and V&V Tool Qualification Guidance

Software Tool Regulatory Qualification Guidance

- The guidance specified in IEEE Std 7-4.3.2 shall be used to evaluate and qualify tools before they are used. The guidance requires that software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management.

- One or both of the following methods shall be used to confirm the software tools are suitable for use:
  - ✓ A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.
  - ✓ The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.
  - ✓ Finally, tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

- Based on the guidance, the qualification of software Development and V&V tools consists of the following steps including tool requirements specification development, tool detailed design and implementation, tool V&V program, tool revision control and the use of the tool in nuclear safety I&C applications.

Tool Requirements Specification, Design Description and Implementation

- The tool Requirements Specification defines the functions, capabilities, and limitations of the tool.
- The tool Design Description shows how the tool will be structured to satisfy the requirements identified in the tool requirements specification.
  - ✓ It is a translation of requirements into a description of tool structure, tool module components, interfaces, and data necessary for the implementation of the tool.
  - ✓ In essence, the tool design description becomes a detailed blueprint for the implementation activity.
- In a complete tool design description, each requirement must be traceable to one or more design entities.
- During the tool implementation, if there are third party tools or modules involved, then these tools or modules shall be treated as commercial tools that are subjected to a dedication process defined in EPRI TR 106439-1996 to reach high confidence in their uses.

Engineering Tool Qualification – Tool V&V Program

A V&V program for use in FPGA applications should be developed. This program is consistent with the guidance provided by the IEEE Std 7-4.3.2-2003 and the V&V methodologies specified in the IEEE Std 1012-2004. Specific steps are described as follows:

- Review and Verification of Tool Requirements Specification and Design Implementation
- Tool Code Review and Walkthrough
- Tool Code Coverage Testing (complete for all needed logics gates and MACROs)
- Tool Functional Coverage Testing (all logics functions)
- Tool Functional and Timing Simulation Testing (on all required logics and selected examples)
- Tool Use in the FPGA Circuitry System Testing (on selected typical applications as well as loops logics that have been used in operating NPPs)

Summary and Discussions

1. FPGA-based development process is basically similar to that of software for microprocessor-based systems. In order to reach high confidence in the FPGA-based systems, Verification and Validation that is consistent with the IEEE Std 1012 should be performed along with EQ.
2. Logic translation process needs to be automatic. The automation tool – One-Step for FPGA Applications has been developed.
3. The tool not only automates the logics translation, but also enhances reliability and therefore errors-free in logics implementation for FPGA applications is achievable.
4. The tool has to be qualified to ensure that the tool would not mask any errors during the logic translation process.

The End

Thank you!

QUESTIONS?