HF Controls

Development and Qualification of One-Step Logic Conversion Automation for FPGA Applications

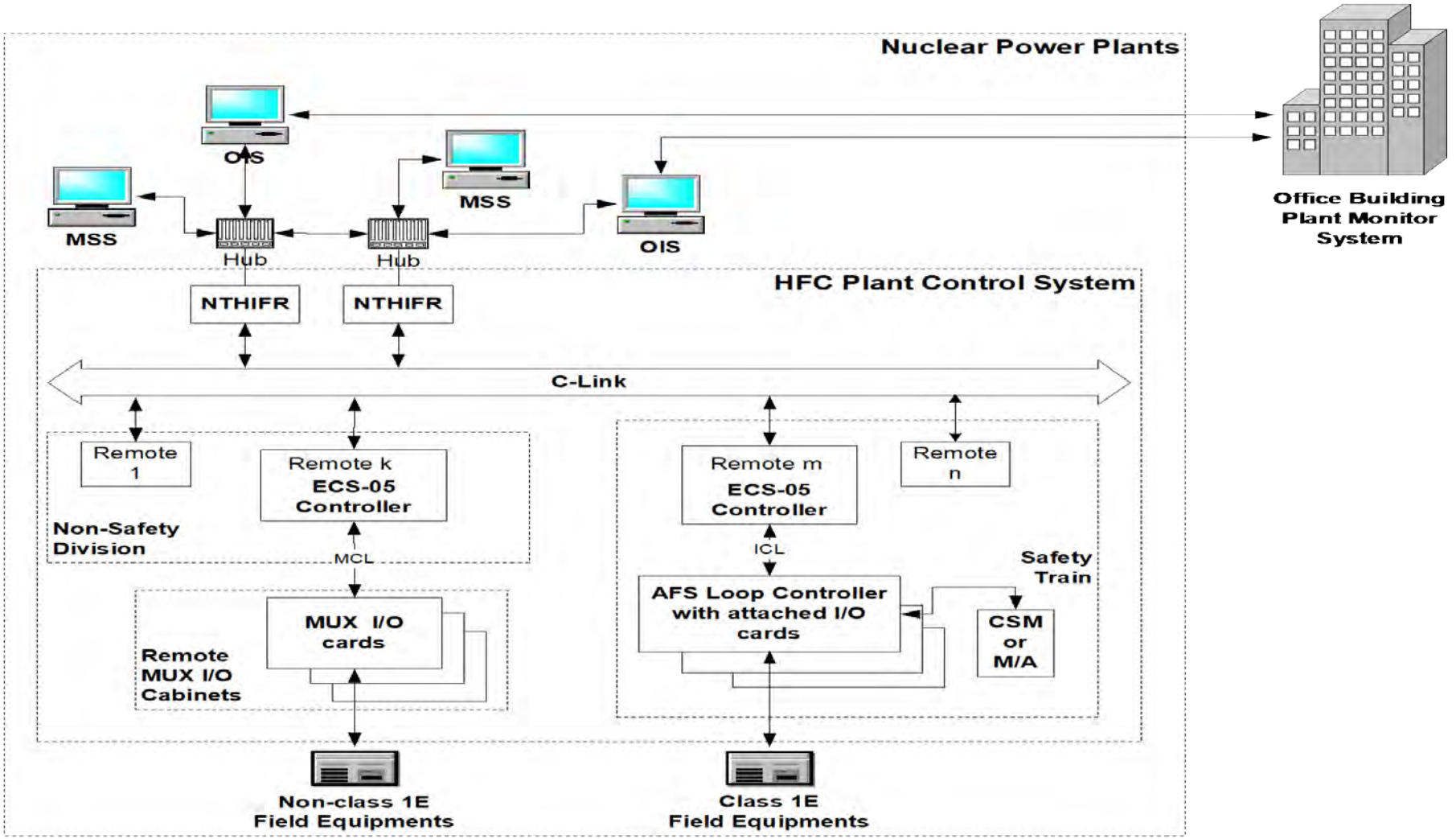
Allen HSU and Steve YANG

12th International Workshop on Application of
Field Programmable Gate Arrays in Nuclear Power Plants
October 14-16, 2019 in Budapest, Hungary

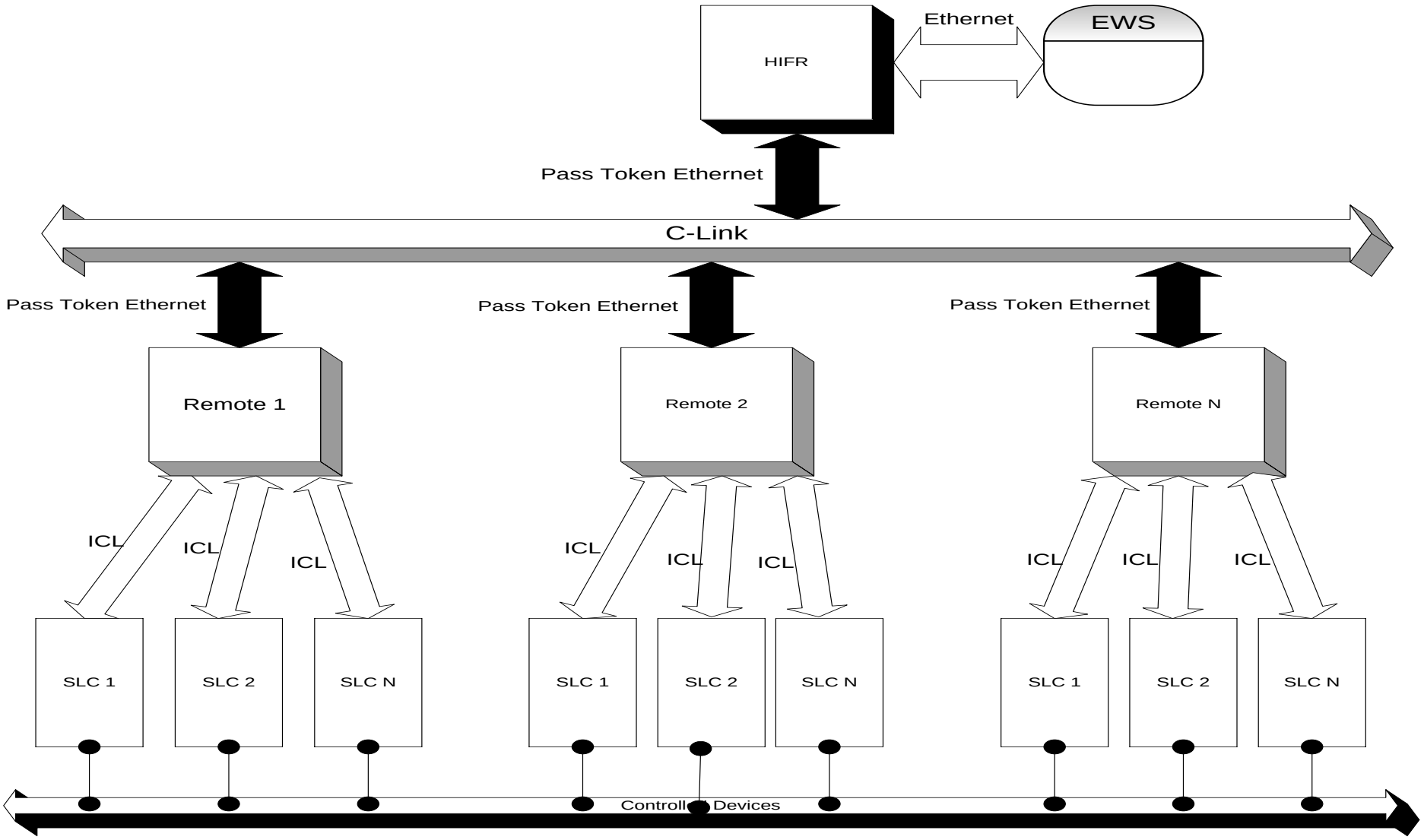
Innovation Leadership Service

Table of Contents

One-Step Used In A PCS Application



Basic PCS Communication Architecture



Requirements for One-Step Tool

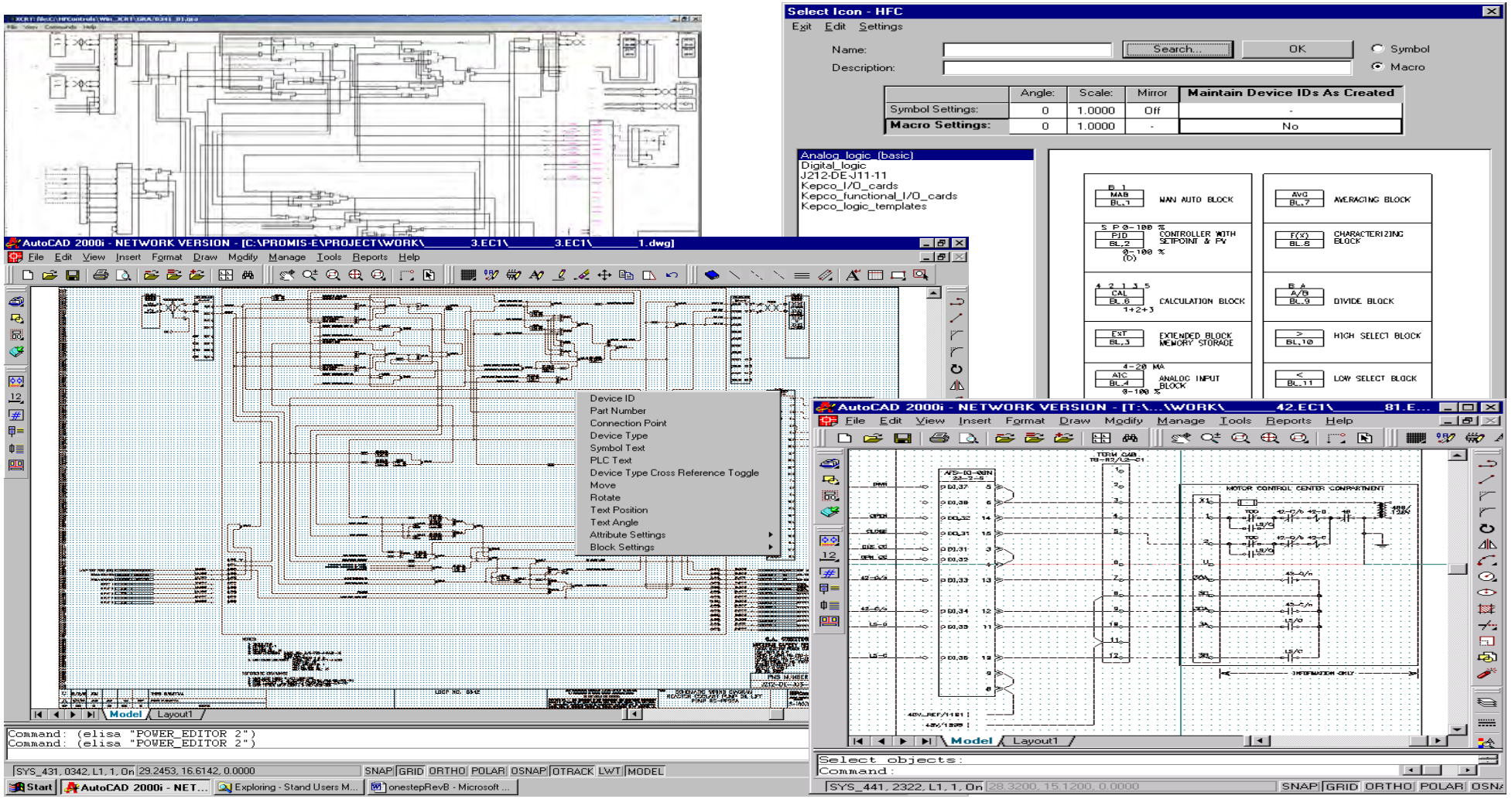
➢Plant Specific Requirements

- ✓ The tool shall automate the process of converting application logics into binary files to be downloaded into controllers,
- ✓ The application logic can be dynamically displayed for diagnostic indications, and
- ✓ The tool shall be used for safety applications.

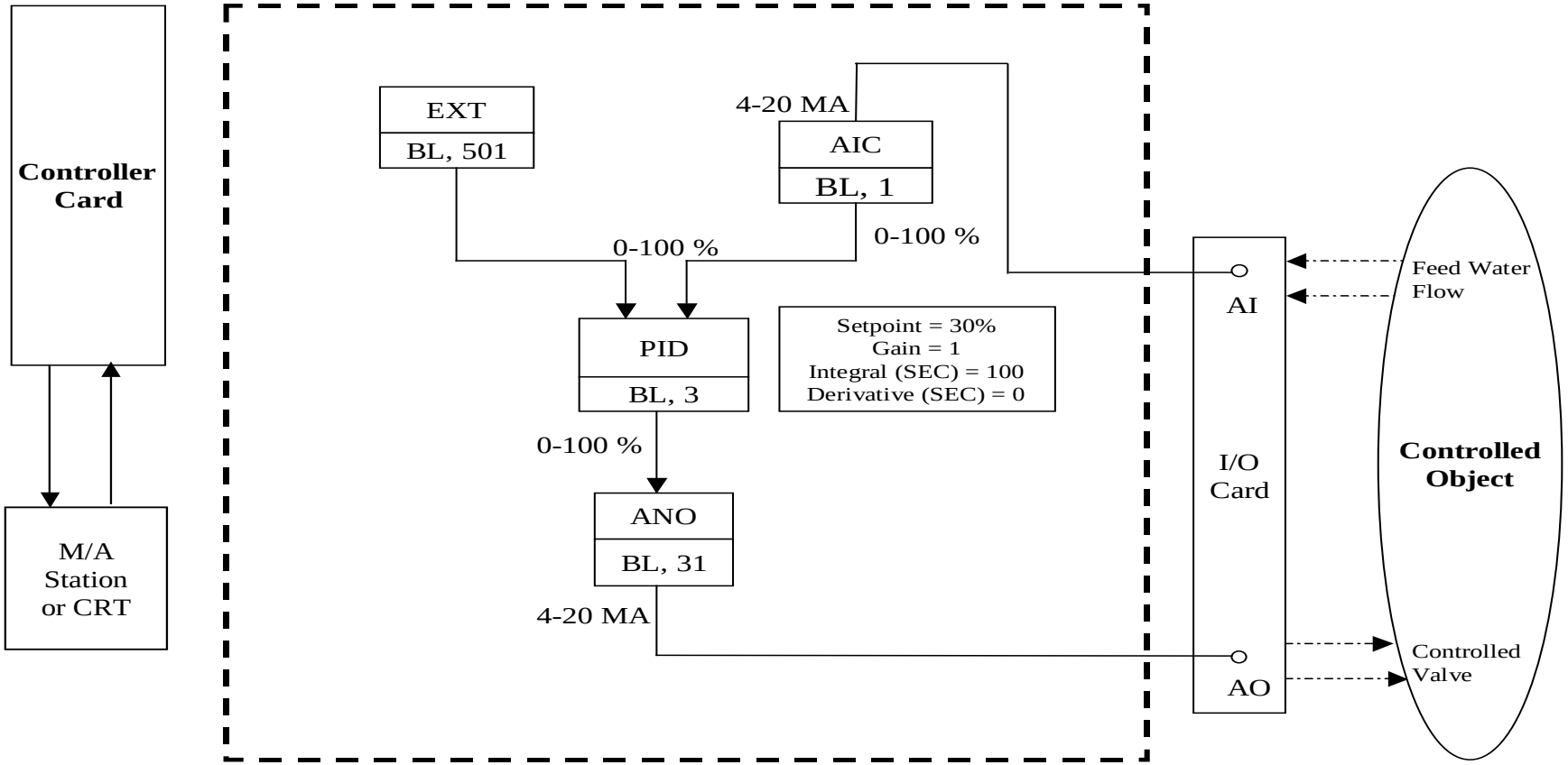
➢Industry Guidance – IEEE Std 1012-1998

- ✓ The tools that insert or translate code (e.g., optimizing compilers and auto-code generators) shall be assigned the same integrity level as the integrity level assigned to the software element that the tool affects.
- ✓ If the tool cannot be verified and validated, then the output of the tool shall be subject to the same level of V&V as the software element.

Example Drawings



Feed-Water Flow Example Illustration



A Simple Analog Loop Schematics

Feed-Water Flow Example Illustration – Logic Equations

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)

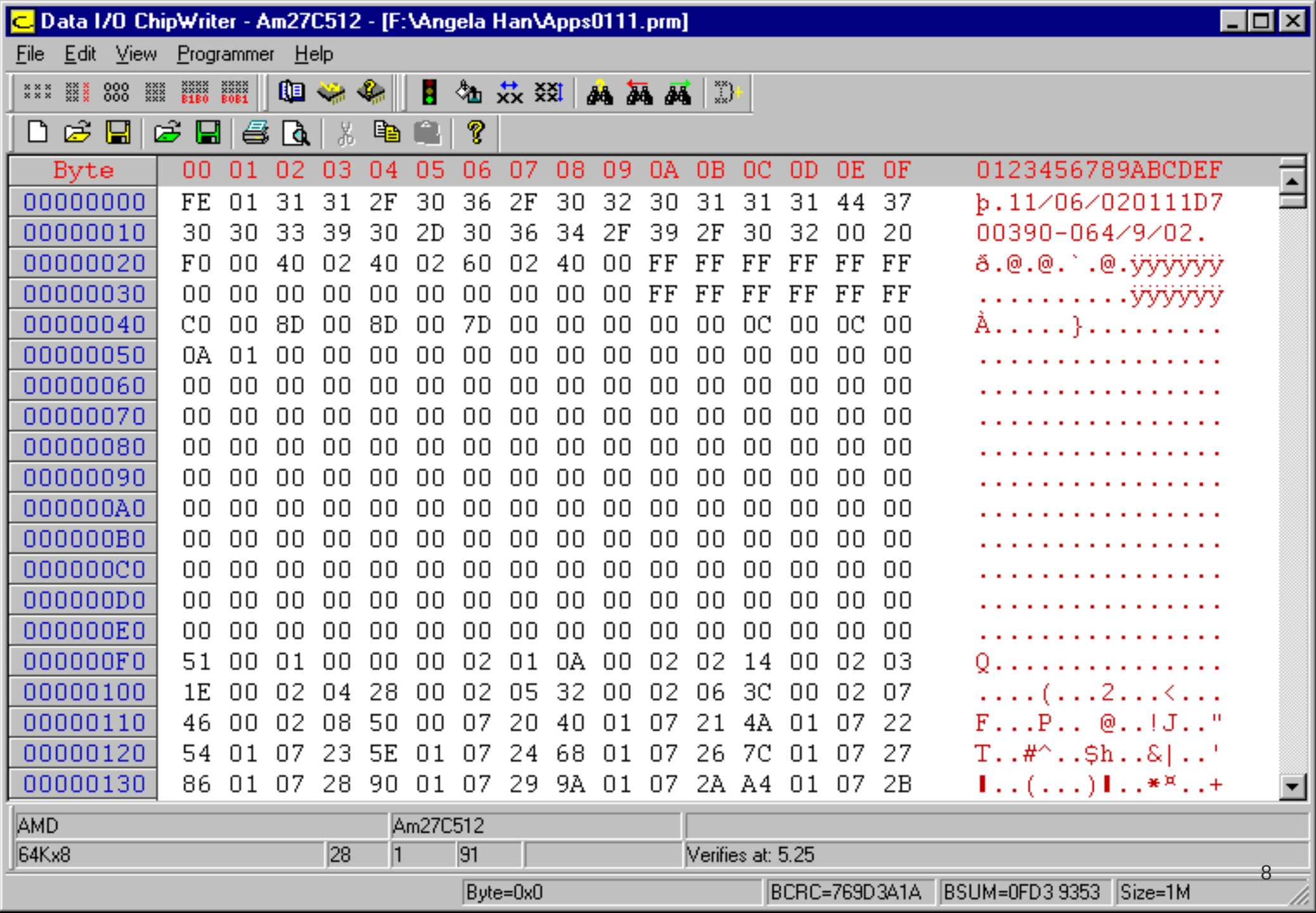
MAGRP(BL, 3, BL, 1, BL, 501, BL, 3, BL, 3) (2)

AIC(BL, 1, 100) (3)

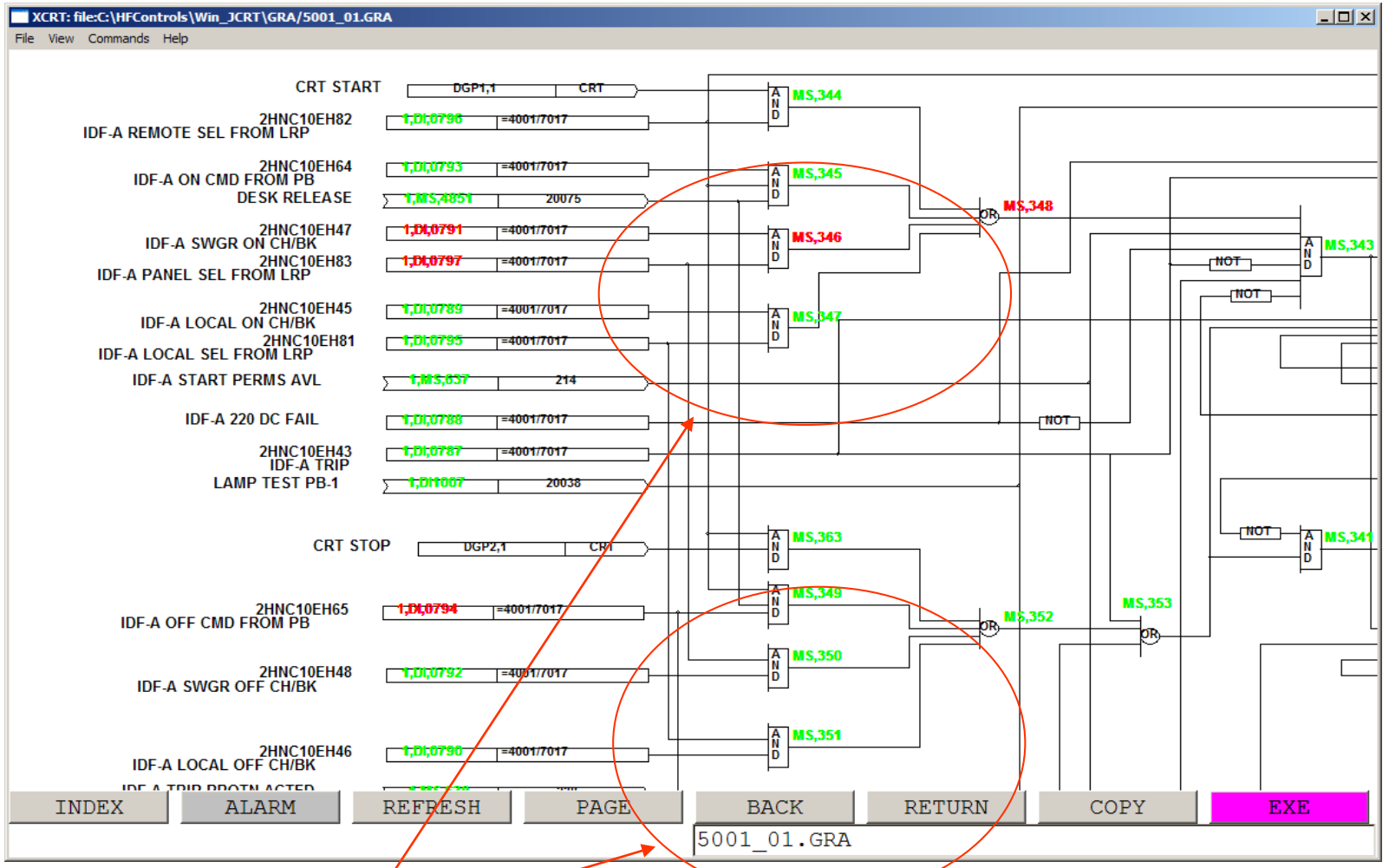
PID(BL, 3, 100) (4)

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.


Data I/O ChipWriter - Am27C512 - [F:\Angela Han\Apps0111.prm]
File Edit View Programmer Help
Byte 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00000000 FE 01 31 31 2F 30 36 2F 30 32 30 31 31 31 44 37 þ.11/06/020111D7
00000010 30 30 33 39 30 2D 30 36 34 2F 39 2F 30 32 00 20 00390-064/9/02.
00000020 F0 00 40 02 40 02 60 02 40 00 FF FF FF FF FF FF ð.@.@.`.@.ÿÿÿÿÿÿ
00000030 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF ....ÿÿÿÿÿÿ
00000040 C0 00 8D 00 8D 00 7D 00 00 00 00 00 0C 00 0C 00 À.....}.....
00000050 0A 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000F0 51 00 01 00 00 00 02 01 0A 00 02 02 14 00 02 03 Q...............
00000100 1E 00 02 04 28 00 02 05 32 00 02 06 3C 00 02 07 ....(...2...<...
00000110 46 00 02 08 50 00 07 20 40 01 07 21 4A 01 07 22 F...P.. @..!J.."
00000120 54 01 07 23 5E 01 07 24 68 01 07 26 7C 01 07 27 T..#^..$h..&|..'
00000130 86 01 07 28 90 01 07 29 9A 01 07 2A A4 01 07 2B ‡..(...)š..*¤..+
AMD
Am27C512
64Kx8
28
1
91
Verifies at: 5.25
Byte=0x0
BCRC=769D3A1A
BSUM=0FD3 9353
Size=1M

Diagnostic Dynamic Displays



Note: Recurring Logic

Development of One-Step for FPGA

➢ Tool Requirements Specification

This is one of the important documents to specify the tool requirements including

- ✓ **its editable functions on Auto CAD and its Promis*E add-ons,**
- ✓ **One-Step assembler to convert the output files of application logic to FPGA Verilog,**
- ✓ **generate the necessary codes/tables for required RQ and I/O tables, and**
- ✓ **One-Step Linker to link the Verilog codes with pre-developed FPGA based utilities to generate flash to FPGA boards.**

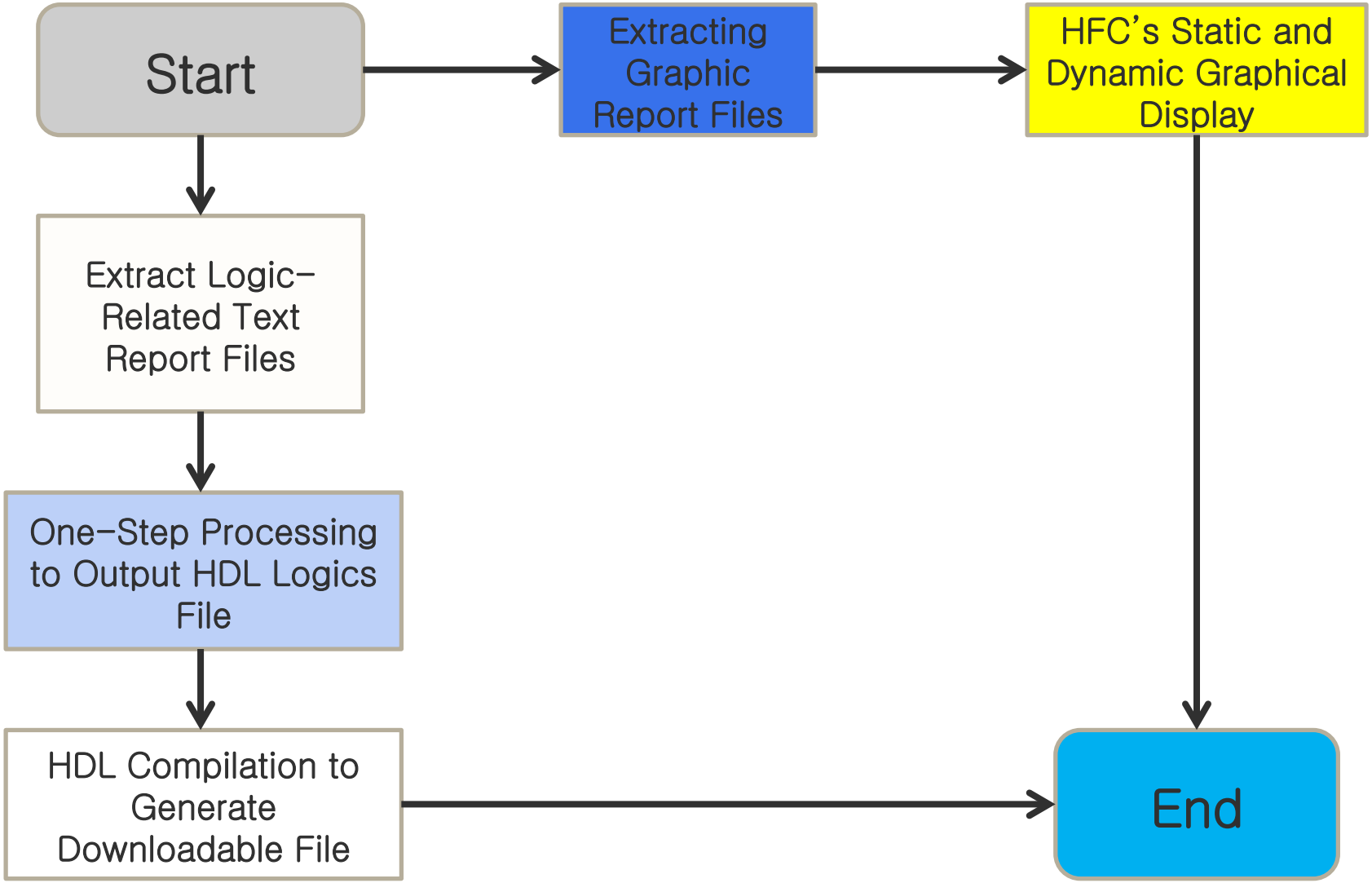
Development of One-Step for FPGA

➢ Tool Detailed Design Description and Implementation

- ✓ The tool Detailed 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.
- ✓ There are two distinctive design and implementation stages:
  - First of all, the generation of the FPGA Verilog file from CAD drawing output files, and
  - Secondly, the realization of downloadable code (which is equivalent to the microprocessor based hex file). This includes FPGA manufacturers' tools integration process via HFC automation scripts.

One of the key elements for this stage is the assurance of the manufacturers' FPGA and its third party tools, which are included in HFC One-Step for FPGA tool development and V&V process.

Development Process Flow of One-Step for FPGA



V&V of One-Step for FPGA

Tool V&V Program

As the development of One-Step for microprocessor program, HFC implemented a V&V program for the One-Step tool for FPGA. This program is consistent with 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 such as LDS and DPS)**
- ✓ **Tool Use in the FPGA Circuitry System Testing (on selected applications such as LDS and DPS, as well as loops logics that have been used in operating NPPs)**

XCRT: SINGLE POINT DISPLAY

FD FAN A CTRL VANES

EUNIT001

0,AG,3

P 30.097

S 30.0

O 69.901

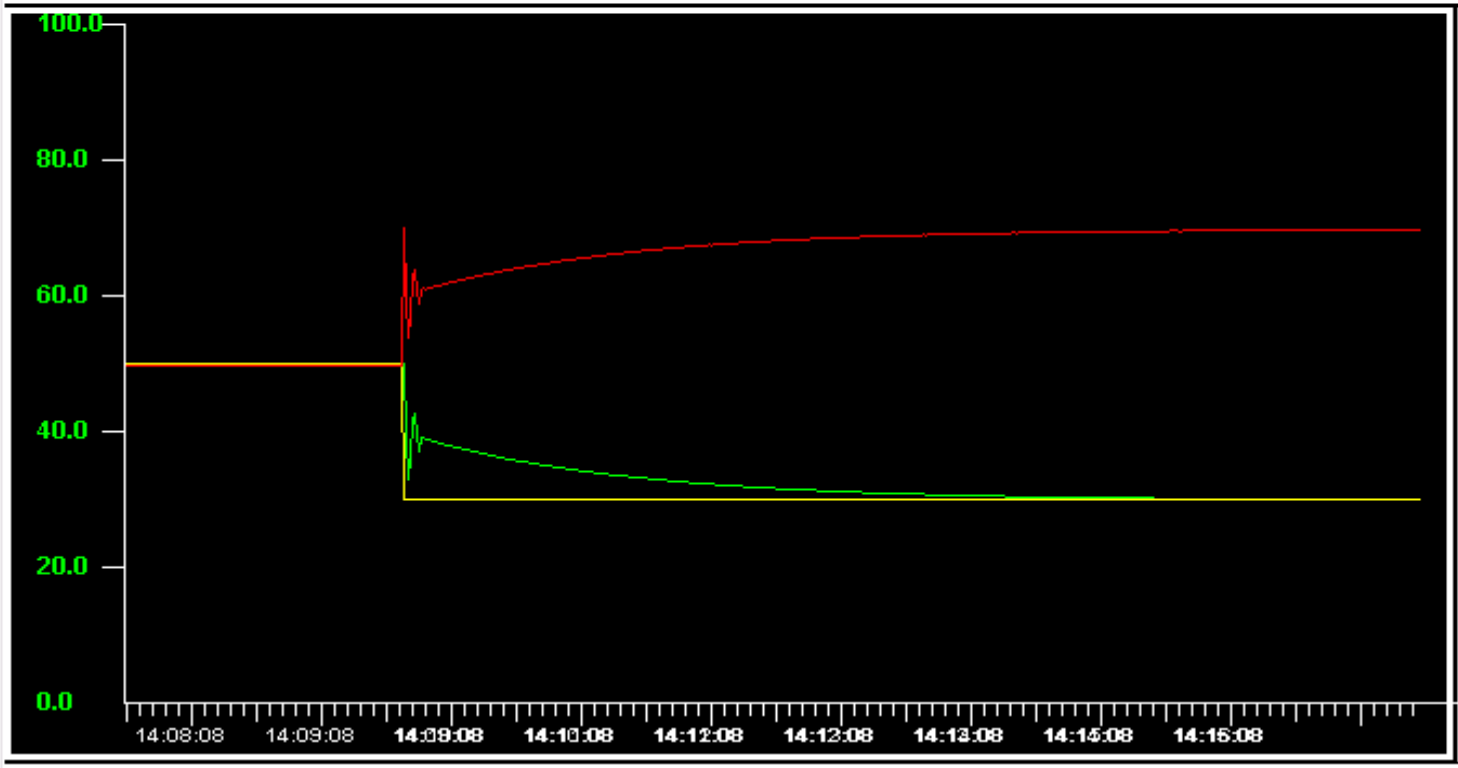
AUTO

LOCAL

E C S

MODE: ACTIVE BLOCK TYPE: PID REMOTE: 0

STR: 0 FREQ: 0 PHASE: 0 BLOCK: 3



DYNAMIC GAIN

NaN

DISABLE

NL GAIN

0.0

GAIN

1.0

TAUI

100.0

TAUD

0.0

PRIMARY TUNING

HIGH ALARM 0.0 DISABLE

LOW ALARM 0.0 DISABLE

RATE ALARM 0.0 DISABLE

ALARM DEADBAND 0.0

DEVIATION ALARM DISABLE

HIGH OUTPUT CLAMP 100.0 DISABLE

LOW OUTPUT CLAMP 0.0 DISABLE

HIGH TRIGGER 0.0 DISABLE

LOW TRIGGER 0.0 DISABLE

REVERSE NO SP INIT PROP FROM ERROR

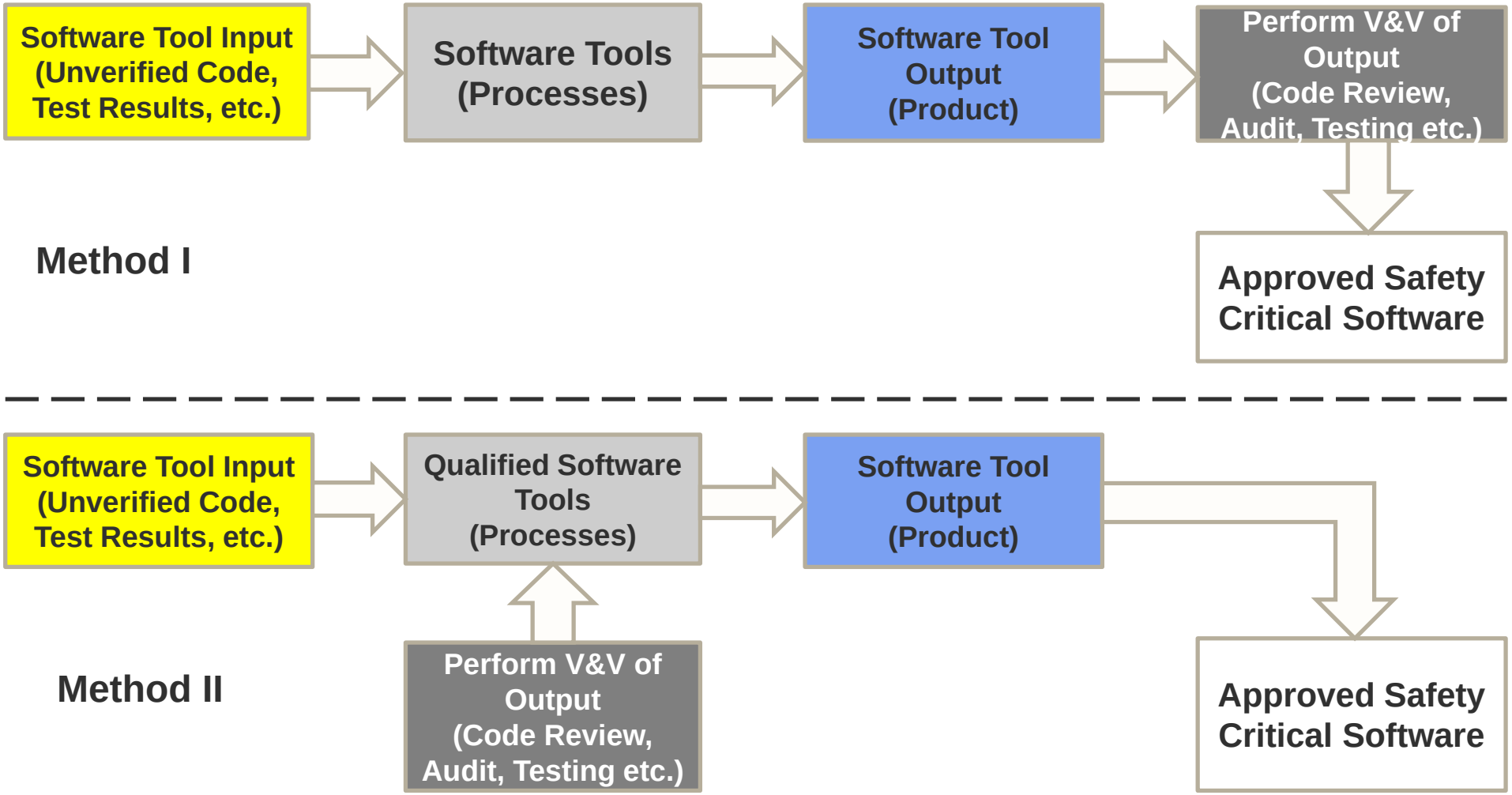
INDEX ALARM REFRESH PAGE BACK RETURN COPY EXE

30

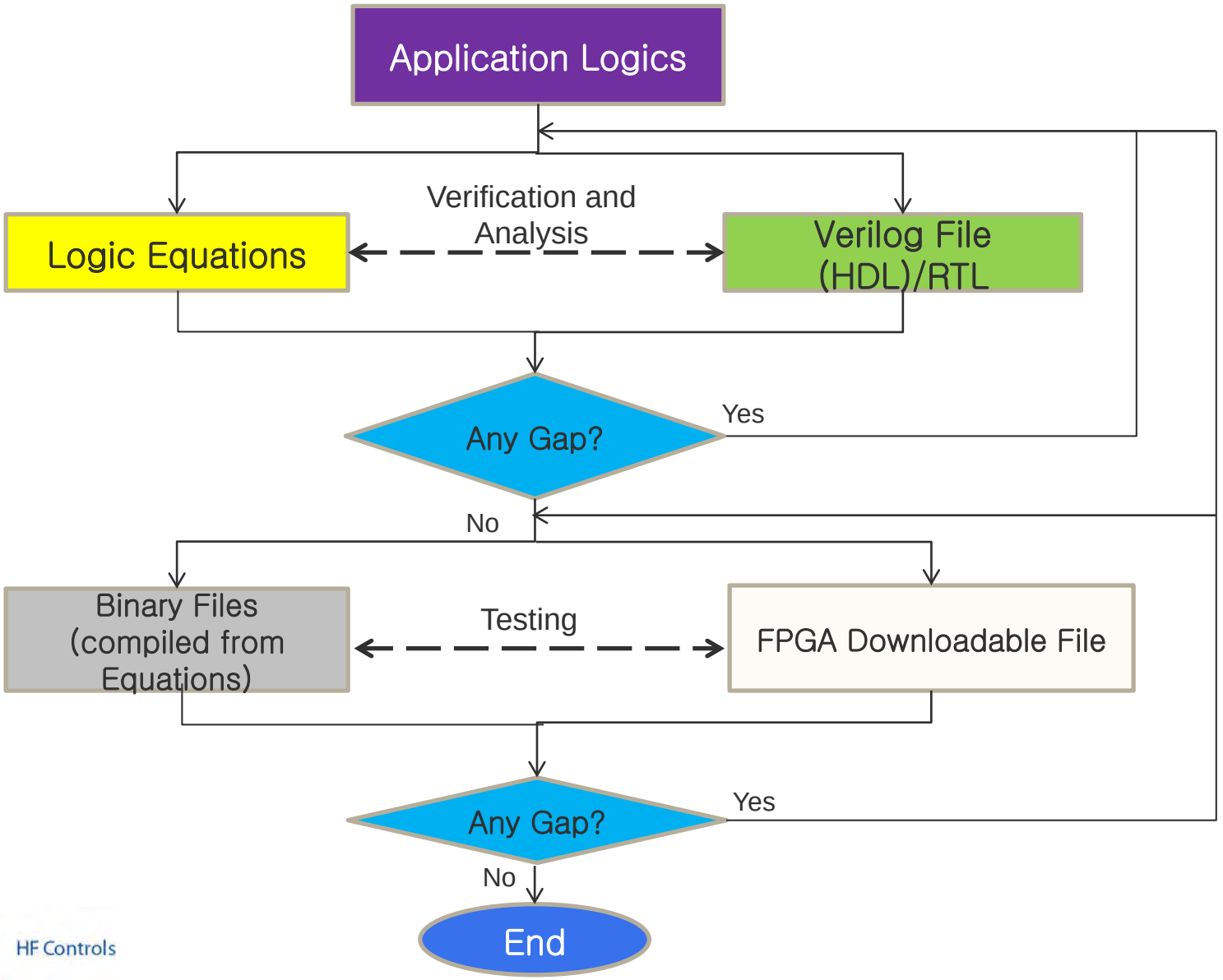
One-Step Tool Regulatory Guidance / Industry Standards

- **Software Tool Regulatory Qualification Guidance**
  - ✓ **In addition to IEEE Std 1012, HFC uses the guidance specified in IEEE Std 7-4.3.2-2003 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: 1) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required. And 2) 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 HFC FPGA One-Step tool consists of the 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.**

Acceptable Approaches for Approval of Tools



Proven One-Step (Microprocessor) as Further Assurance Reference for FPGA Applications



Summaries and Conclusion

1. One-Step Automates the Logic Translation Process for FPGA Applications
2. One-Step Automates the Archiving of Large Volume of Logic Schematics
3. Qualification of One-Step uses Guidance provided in IEEE Std 1012, IEEE Std 7-4.3.2 and IAEA NP-T-3.17
4. The assurance of One-Step for FPGA applications to generate correct results is based on disciplined specification and lifecycle process, and experience from proven microprocessor history.
5. Manual Labor and Errors Are Eliminated; and Safety and Reliability Are Secured.

The End

Thank You!