Use of SMART Devices in Safety Related Computers

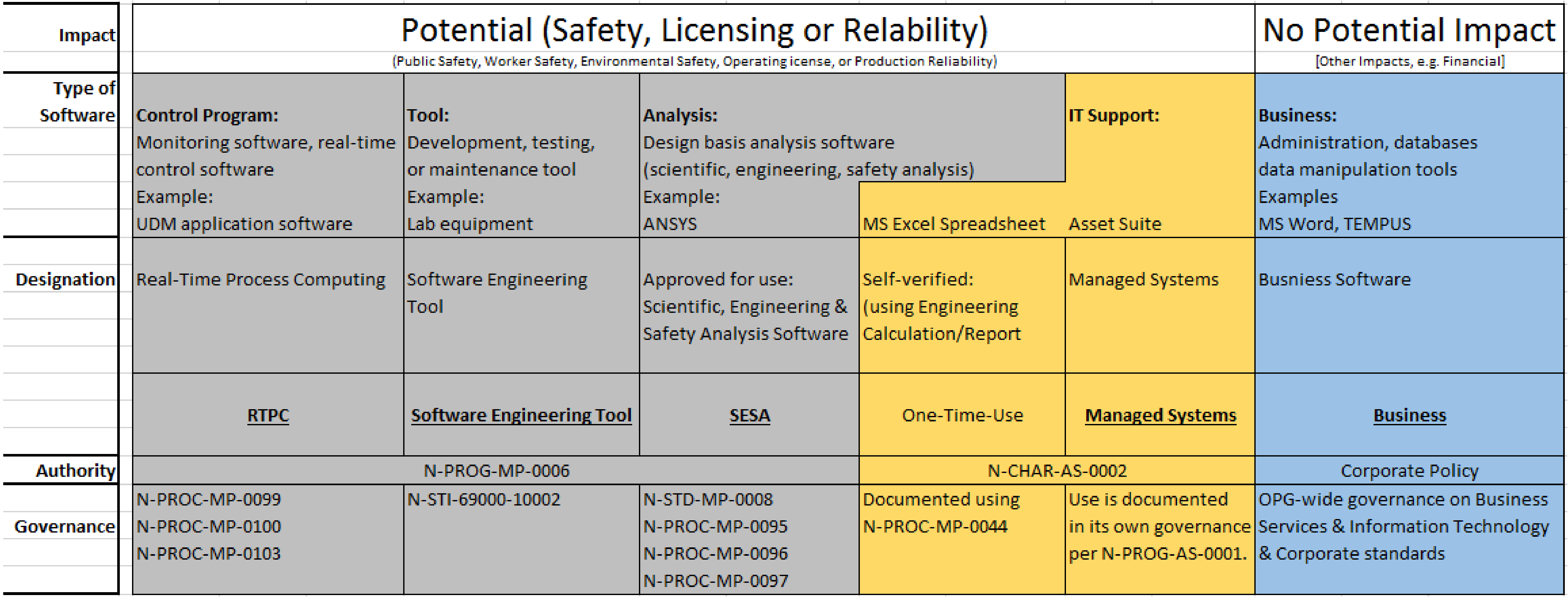
Energiforsk Conference | October 22 2019

Kevin McKay

Safety Related Computers

Ontario Power Generation

Classification



Impact	Potential (Safety, Licensing or Relability)					No Potential Impact
	(Public Safety, Worker Safety, Environmental Safety, Operating icense, or Production Reliability)					[Other Impacts, e.g. Financial]
Type of Software	**Control Program:** Monitoring software, real-time control software Example: UDM application software	**Tool:** Development, testing, or maintenance tool Example: Lab equipment	**Analysis:** Design basis analysis software (scientific, engineering, safety analysis) Example: ANSYS	MS Excel Spreadsheet	**IT Support:** Asset Suite	**Business:** Administration, databases data manipulation tools Examples MS Word, TEMPUS
Designation	Real-Time Process Computing	Software Engineering Tool	Approved for use: Scientific, Engineering & Safety Analysis Software	Self-verified: (using Engineering Calculation/Report	Managed Systems	Busniess Software
	RTPC	**Software Engineering Tool**	**SESA**	One-Time-Use	**Managed Systems**	**Business**
Authority	N-PROG-MP-0006			N-CHAR-AS-0002		Corporate Policy
Governance	N-PROC-MP-0099 N-PROC-MP-0100 N-PROC-MP-0103	N-STI-69000-10002	N-STD-MP-0008 N-PROC-MP-0095 N-PROC-MP-0096 N-PROC-MP-0097	Documented using N-PROC-MP-0044	Use is documented in its own governance per N-PROG-AS-0001.	OPG-wide governance on Business Services & Information Technology & Corporate standards

Categorization

- Graded Approach
  - Classification: RTPC, SESA, Managed Systems, Business IT
  - RTPC Category I, II, III, and IV

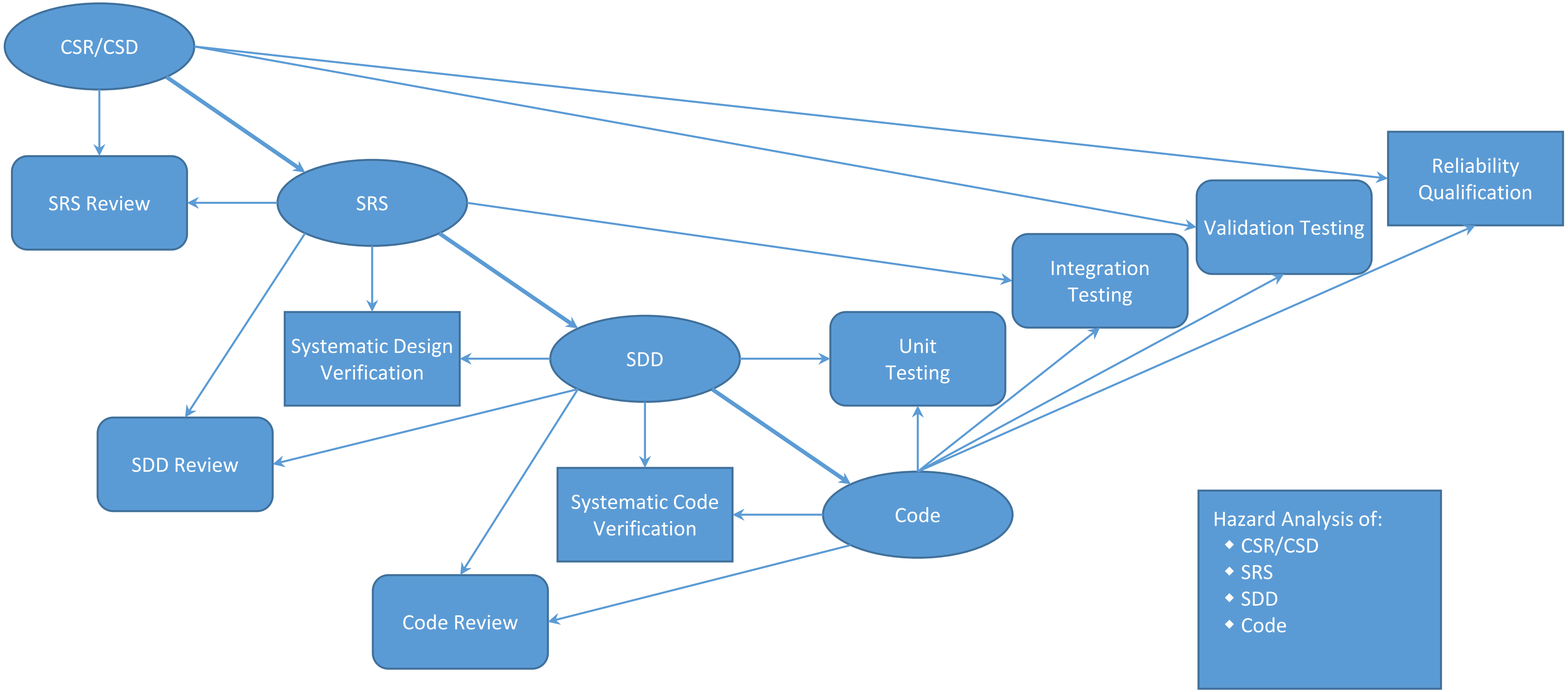
- Pre-Developed Software
  - CSA N290.14 Software Qualification

- Custom Developed Software
  - Centre of Excellence Standards
    - CE-1001-STD
    - CE-1002-STD
    - CE-1003-STD

Software Qualification

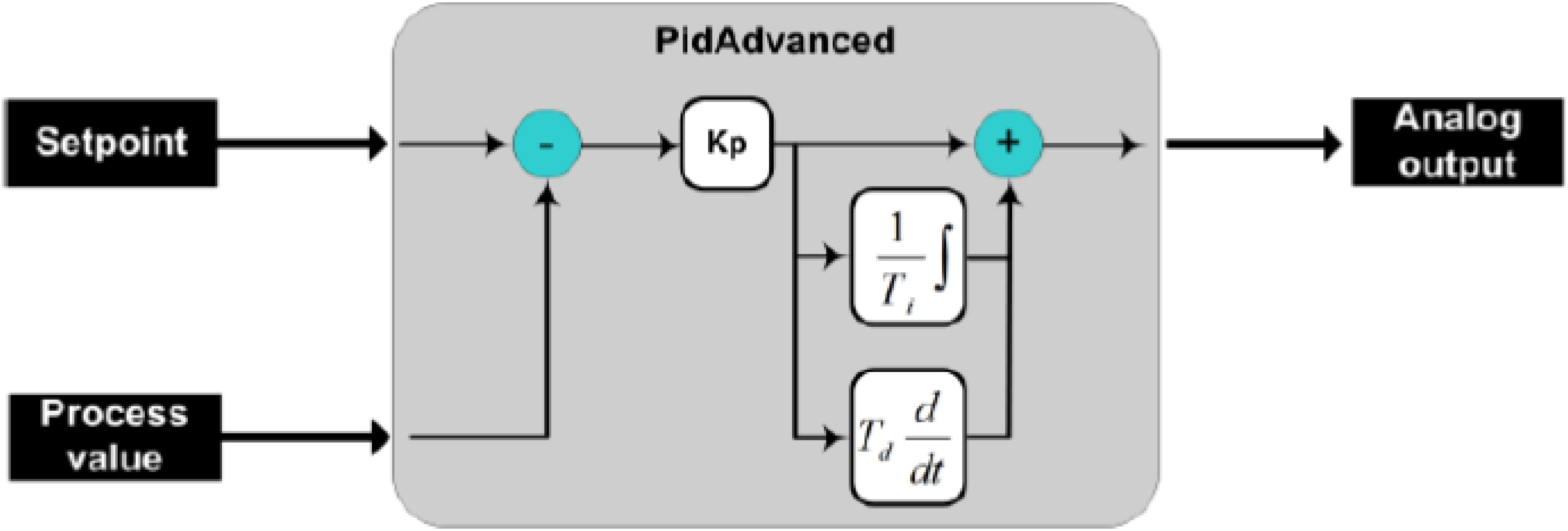
- Pre-developed Software (N290.14-15)
  - Recognized Program Method
    - SIL, ISO, IEC, etc
  - Mature Product Method
    - Unit Years of Operation
  - Proof through Testing
    - Low complexity software
    - Minimum successful test executions or hours
  - Preponderance of Evidence
    - Partial compliance with applicable industry standards
    - Complementary testing
    - Proven in-use arguments

Software Development (CUSTOM)

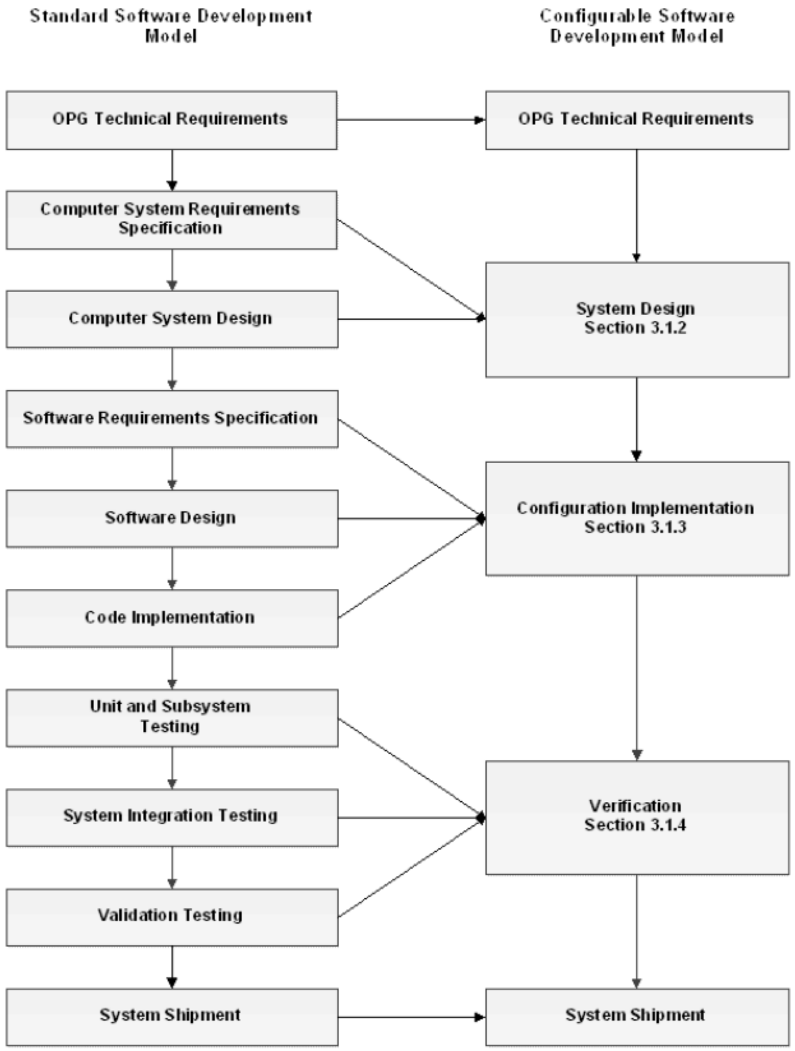


CSR – Computer System Requirements
CSD – Computer System Design
SRS – Software Requirements Specification
SDD – Software Design Description

What about Configurable Logic?



Configurable Logic Development



Standard Software Development Model

Configurable Software Development Model

OPG Technical Requirements

Computer System Requirements Specification

Computer System Design

Software Requirements Specification

Software Design

Code Implementation

Unit and Subsystem Testing

System Integration Testing

Validation Testing

System Shipment

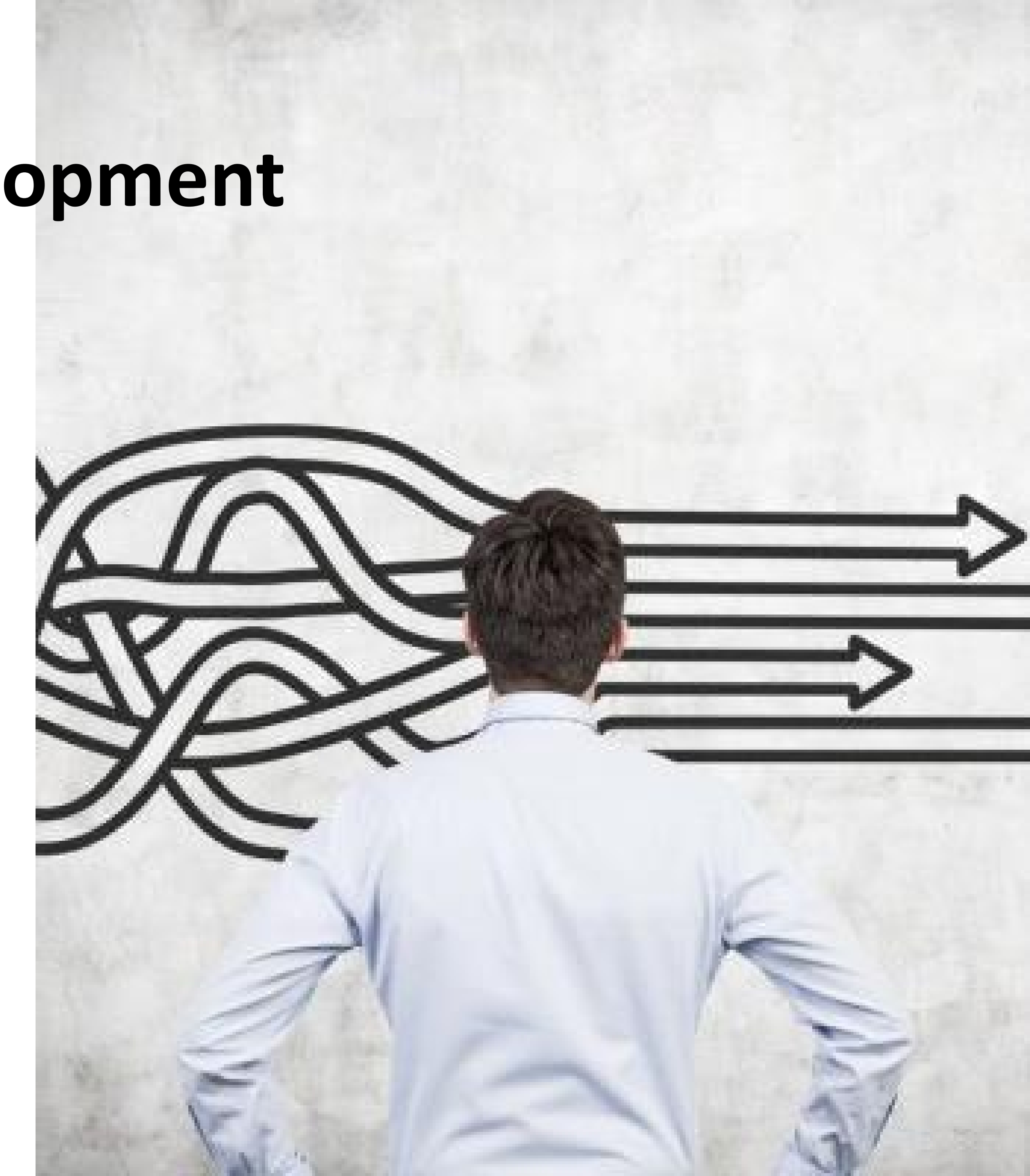
OPG Technical Requirements

System Design Section 3.1.2

Configuration Implementation Section 3.1.3

Verification Section 3.1.4

System Shipment



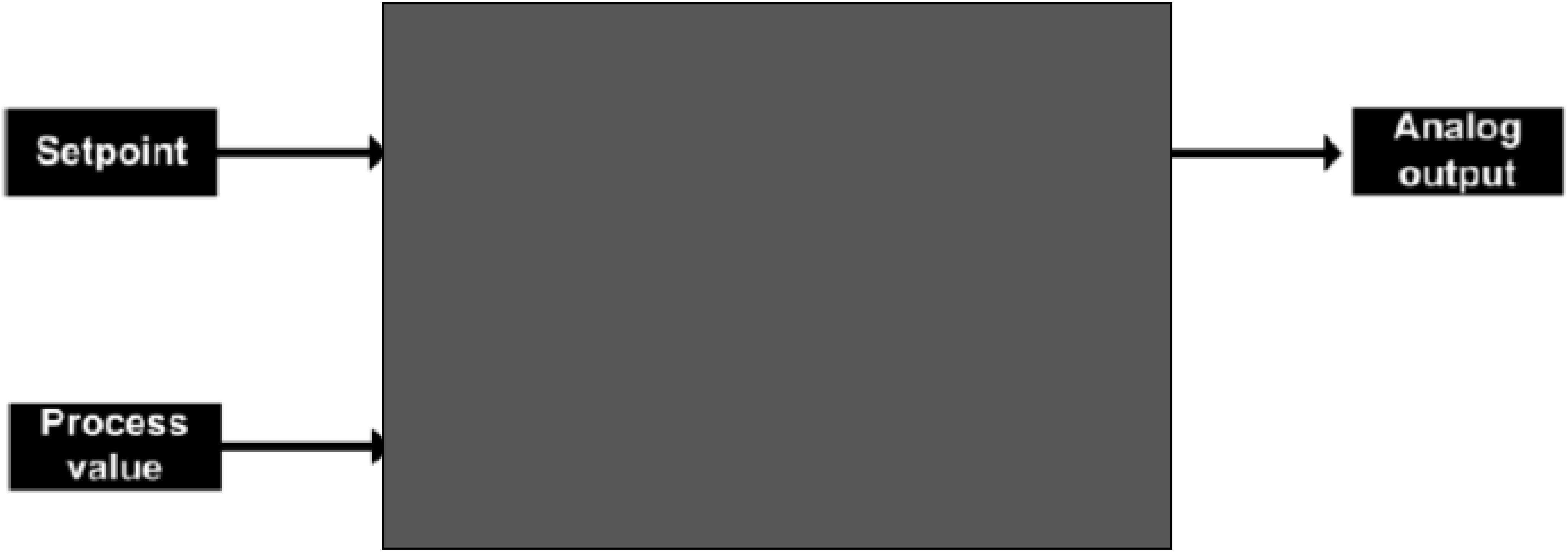
Smart Devices

- What is a Smart Device?
  - Configurable but not programmable
  - Limited and Pre-developed Functionality
  - Low Complexity

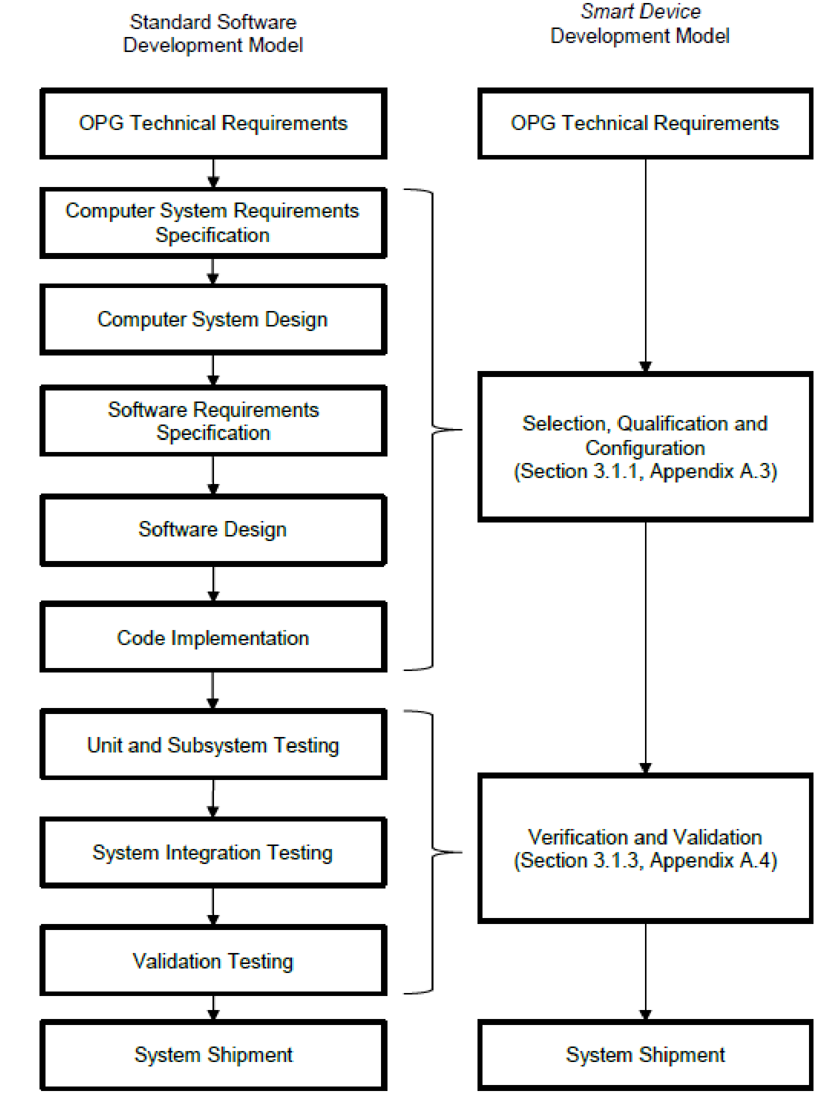
- Example Devices:
  - Uninterruptible Power Supplies
  - Transmitters, Network Switches
  - Relays

- Example Configuration:
  - Set points, I/O ranges, PID parameters
  - Menu settings, i.e. Event Logging setting, Trend settings, User Interface, etc.
  - Enabling features, functionality, i.e. Write Protection, Passwords, etc.

Smart Device



Smart Device Development



Standard Software Development Model

OPG Technical Requirements

Computer System Requirements Specification

Computer System Design

Software Requirements Specification

Software Design

Code Implementation

Unit and Subsystem Testing

System Integration Testing

Validation Testing

System Shipment

Smart Device Development Model

OPG Technical Requirements

Selection, Qualification and Configuration (Section 3.1.1, Appendix A.3)

Verification and Validation (Section 3.1.3, Appendix A.4)

System Shipment

Figure 1: Mapping from Standard Development Model to Smart Device Development Model

Thank you!

Questions?

ONTARIO POWER GENERATION