CENG 5434: Microcomputer Systems Design WELCOME 11/2/2022

REMIND ME TO RECORD

This week we discuss a number of items.

Contents

1. **Go over Quiz**

   REDO Quiz problems you missed if less than 75 score – with good details. References from my lectures or our website. Mail it to me.

   1b_Accuracy, Precision & Resolution __ Electronic Measurements (1).pdf
   1c_Analog-to-Digital Converters _ EE Times.pdf

Serious Quiz Review – Going over Web Data

Your final project presentation December 7, 2022

Dec. 5-10 Regular Session Finals week

2. **Let's Go over the rules**

No 8051 chips. Expect wireless connections for your project.

Project Reports – brief presentation 5min with slides and Written Report

2_1 GoodRequirements_Summary.pdf

2_2 SUMMARY OF DOCUMENTATIONforFinalReport_5434.pdf

HW8 – Your first project report – Follow the instructions

LECTURE 3 Power (I expect a calculation if battery-powered product)

3_1 Video Dips in Power Supply:

Dips in the Supply Voltage can Confuse a Microprocessor
4,502 views •Jan 12, 2017 6:00
https://www.youtube.com/watch?v=cI6daT3kOuk

3_2 Paper How to Calculate Power Needs:

https://www.edn.com/efficient-powering-of-a-robot-swarm/

LECTURE 4 Product design, manufacturing, Patent and Certification

4a_SEISCO_NEC_Calculations_Slides.pdf

4b_HarmanPatents_List_4CH_1CH.pdf

4c_HarmanSeitzFluid_heating_control_system6246831.pdf

4d_Patent No. 10,024,571_1Chamber.pdf

5_2 Federal and Certifying Agencies NEC, UL, etc.

A Guide to United States Electrical and Electronic Equipment Compliance Requirements

https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8118r1.pdf

LECTURE 5_2 UL Standard 449 Electric Heating Appliances

LECTURE Computer Standards for Critical Applications

UL 1998 (Software), 4_2 UL 60730 (Automatic Controls),

UL 1998 (Software)

Underwriters Laboratories Inc.

Standard for Safety

Software in Programmable Components

Let's explore a few sections.

1 Scope Page 12
1.1 These requirements apply to non-networked embedded microprocessor software whose failure is capable of resulting in a risk of fire, electric shock, or injury to persons.

2.55 TEST PLAN – A document describing the scope, approach, resources, and schedule of intended test activities. It defines test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning.

2.56 TEST PROCEDURES – Detailed instructions for the set-up, execution, and evaluation of results for a given test case.

2.57 TOOL – Any equipment (e.g., logic analyzers, oscilloscopes, multimeters, digital and analog computers), devices, or software programs [e.g., simulators, computer-aided software/systems engineering (CASE) tools, compilers, type checkers, static analyzers, automated testing scripts, debuggers, linkers, loaders, assemblers, code generators, code librarians, editors, and software analyzers] used to automate or partially automate software development activities, including design, implementation, and testing.

2.58 TOOL QUALIFICATION – The acceptance of analysis, testing, and resulting evidence for which confidence is obtained regarding the correctness of a tool's outputs.

3.1 A risk analysis shall be conducted to determine:
a) The set of risks; and
b) That the software addresses the identified risks.
3.2 The risk analysis shall be based on the safety requirements for the programmable component.
3.3 An analysis shall be conducted to identify the critical, non-critical, and supervisory sections of the software.
3.4 An analysis shall be conducted **to identify states or transitions that are capable of resulting in a risk.**

4_1_1 Example: Control States of Heater See my Document

6 Software Design Page 12 RA = Risks Addressed

2.44 RISKS ADDRESSED (RA) STATE – A state that is characterized by all reasonably foreseeable risks associated with the intended use of the product being addressed such that there is no longer a likelihood of the risk.

6.1 A fault in the software shall not initiate an event that results in a risk.

6.2 The software shall maintain an RA state upon detection of a condition that is capable of resulting in a risk as identified in Section 3, Risk Analysis.
6.3 Detection of a failure in the software during the intended operation of the product shall be handled in a manner that is in accordance with the product safety requirements.

6.4 The software shall employ means to identify and respond to states that are capable of resulting in a risk. Examples of such means include initialization, fail-safe and fault-tolerant concepts, run-time checks, and built-in tests.

6.5 In allocating resources to tasks, consideration shall be given to the scheduling frequency of the task, the criticality of the task, and the resources utilized by the task, as well as the impact that each of these factors has on the ability to address the identified risks.

6.6 Means shall be employed for the prevention, detection, and resolution of non-terminating and non-deterministic states and error states such as division by zero and under/overflow that are capable of affecting the intended operation of the software.

6.7 All variables shall be set to initial values before being used by any instruction.

8 Measures To Address Microelectronic Hardware Failure Modes Page
8.1 Means shall be employed to address all microelectronic hardware failure modes identified by Section 3, Risk Analysis. Appendix A contains examples of acceptable measures for microelectronic hardware.

8.2 Physical failures of the following microelectronic hardware shall be considered:
a) CPU registers, instruction decoding and execution, program counter, addressing and data paths;
b) Interrupt handling and execution;
c) Clock;
d) Non-volatile and volatile memory and memory addressing;
e) Internal data path and data addressing;

f) External communication and data, addressing, and timing;
g) Input/output devices such as analog I/O, D/A and A/D converters, and analog multiplexers;
h) Monitoring devices and comparitors; and
i) Application-Specific Integrated Circuits (ASICs), Gate Array Logics (GALs), Programmable Logic Arrays (PLAs), and Programmable Gate Arrays (PGAs) hardware.

8.3 Analysis of possible combinations of microelectronic hardware failures, software faults, and other events that are capable of resulting in a risk. This includes, for example, microelectronic hardware failures that cause software faults that are capable of resulting in a risk.

12.2 Software plan Page 23
12.2.1 A software plan shall be documented, which describes the software development activities.
12.2.2 The software plan shall include a description of the software design methodology, development rationale, any metrics to be collected, applicable standards and the engineering methods/techniques employed, and an itemized list of all documents produced throughout the software process.

12.4 Configuration management plan Page 23

12.4.1 A configuration management plan, which applies to off-the-shelf software, software tools, and the manufacturer-provided software, shall be documented.

12.4.2 The configuration management plan shall describe:

a) How changes to the software and hardware are managed;

b) The initiation, transmittal, review, disposition, implementation and tracking of discrepancy reports and change requests; and

c) The methods and activities employed to formally control receipt, storage and backup, handling, and release of software and all documentation identified in this section.

APPENDIX A – EXAMPLES OF MEASURES TO ADDRESS MICROELECTRONIC HARDWARE FAILURE MODES Page 27

A2.1 The following table provides examples of acceptable measures for covering various failure modes for select components.

Table A2.1
Coverage for microelectronic hardware failure modes

Component[a]	Fault/error	SW class[b] 1	SW class[b] 2	Examples of acceptable measures[c, d, e]	Description
1. **CPU**					
1.1	stuck-at	rq		functional test; or	A5.5
Registers					
				periodic self test using either:	A5.6
				-static memory test	A7.2.9
				-word protection with single-bit redundancy	A7.3.2
	DC fault		rq	comparison of redundant CPU's by either:	
				-reciprocal comparison	A7.1.19
				-independent HW comparator; or	A7.1.6
				internal error detection; or	A7.1.10
				redundant memory with comparison; or	A7.2.8
				periodic self tests using either:	
				-walkpat memory test	A7.2.10
				-abraham test	A7.2.1
				-transparent galpat test; or	A7.2.3
				word protection with multi-bit redundancy; or	A7.3.1
				static memory test and word protection with	A7.2.9
				single-bit redundancy	A7.3.2

RECORD OFF

RECORD ON

LECTURE MICROCOMPUTER SAFETY STANDARDS 60730

IEC 60730 Safety Standard for Household Appliances

Last Updated: Sep 16, 2015

The International Electro-technical Commission (IEC) has developed safety standard IEC 60730 that discusses mechanical, electrical, electronic, environmental endurance, EMC, and abnormal operation for home appliances.

The IEC 60730 standard classifies appliance software into three categories:

- **Class A** - Control functions that are **not intended to be relied upon for the equipment's safety** such as humidity controls, lighting controls, timers, and switches.
- **Class B** - Control functions that are intended to prevent unsafe operation of the controlled equipment such as thermal cut-offs and door locks for laundry machines.
- **Class C** - **Control functions that are intended to prevent special hazards. Examples are automatic burner controls and thermal cut-outs for closed, unvented water heater systems.**

Major home appliance products, such as washing machines, dishwashers, dryers, refrigerators, freezers, and cookers/stoves, tend to fall under the Class B classification. An exception is an appliance that might cause an explosion, such as a gas-fired controlled dryer that falls under Class C.

Cypress has developed safety features, including IEC 60730 Safety Library along with application notes to help manufactures meet the regulation with PSoC devices.

Application Notes:

- AN78175 - PSoC® 3 and PSoC 5LP - IEC 60730 Class B Safety Software Library
- AN79973 - PSoC3 and PSoC5 CapSense CSD - IEC 60730 Class B Safety Software Library
- AN81828 - PSoC® 1 – IEC 60730 Class B Safety Software Library
- AN89056 - PSoC® 4 – IEC 60730 Class B and IEC 61508 SIL Safety Software Library

Certification Reports:

- VDE Certification Report for PSoC 1 CY8C22x45 and CY8C28xxx
- VDE Certification Report for PSoC 3 and PSoC 5
- UL Certification Report for PSoC 4

https://www.cypress.com/documentation/other-resources/iec-60730-safety-standard-household-appliances

IEC 60730

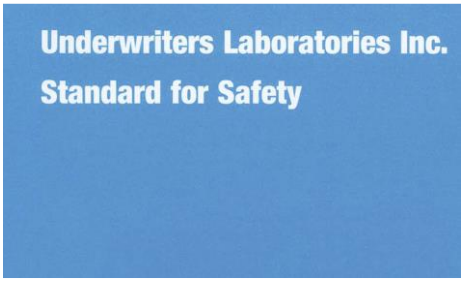
The IEC/UL 60730 standard for safety is an established testing specification for electrical, electronic, mechanical, EMC, and other features of AC appliances. The specification's Annex H spells out the safety aspects most relevant to safe operation of MCU hardware and software used in appliances. Software requirements are further defined in Annex Q of the IEC 60335-1. These safety standards require certification that proves compliance with the standards and shows system robustness. To simplify compliance, OEM's require components that can be certified as IEC 60730 compatible or compliant. Specifically for MCUs, 60730 Annex H - Requirements for Electronic Controls details test and diagnostic methods.

60730 allows manufacturers to take one of three approaches to address safety in MCU-based systems.

1. Dual-channel architecture with two MCUs, each performing related tasks in lock step, one checking the other.
2. Single-channel architecture accompanied by functional testing at the point of manufacture (the option used most frequently today). This method has the drawback of not being able to address problems once the appliance is out of the factory.
3. Single-channel with periodic self-test architecture addressing the problem of in-service operation by having firmware that regularly checks critical functions of the electronic control

Microcontrollers that support the single-channel self-test option likely provide the highest level of consumer protection at the lowest cost. A good idea is to have two accurate oscillators on an MCU — one to operate the appliance and the other to supply an independent time base for when periodic tests are executed.

5_1_1_Automatic Electrical Controls for Household and Similar Use



See My Copy

5_1_2 Functional Safety for ISO 26262, IEC 61508, IEC 60730 and IEC 62304

Robustness, reliability and safety of end-products are becoming ever more important. In some application segments these requirements are formalized and mandatory, while in others this is implemented to differentiate the product and take the step from a good product to an excellent product.

https://www.microchip.com/design-centers/functional-safety?gclid=CjwKCAiAqJn9BRB0EiwAJ1Sztet7bMu0nI0TyQX-ty8AqQ1nKpRaJaf68vc2o5r843Rwv_XOKCaooRoCfaEQAvD_BwE

In addition to the Functional Safety Ready controllers, Microchip offers a wide portfolio of PIC, AVR and SAM microcontrollers and dsPIC33 digital signal controllers that also support IEC 60730 compliant VDE- and UL-certified Class B libraries, offering you a range of options to select a device for your household appliance design.

MICROCONTROLLERS (MCUs) and DIGITAL SIGNAL CONTROLLERS DSCs)	AVR® and PIC® MCUs	PIC24 MCUs and dsPIC®
IEC 60730 Class B Library	Yes	Yes

5_1_3_Example Compliance Sheet for SEISCO Heater

UL/IEC 60730-1 - Automatic Electrical Controls for Household and Similar Use, General Requirements:

5_1_3_UL 60730 CDF Single Chamber Cert.pdf

RECORD OFF

Remember Take Home will be posted Test Next time.

NO class November 23rd.