http://www.bitron.net

2007

S.P.I.N.

Meeting 11th October 2007

SAFETY IN THE AUTOMOTIVE

SAFETY DEALS WITH PROTECTION AGAINST HAZARDS AND RISKS THAT CAN ARISE FROM THE OPERATION OF A SYSTEM

SAFETY IS BECOMING A KEY POINT SINCE EVERY CAR MAKER PUTS GREAT ATTENTION TO THE HEALTH OF PEOPLE

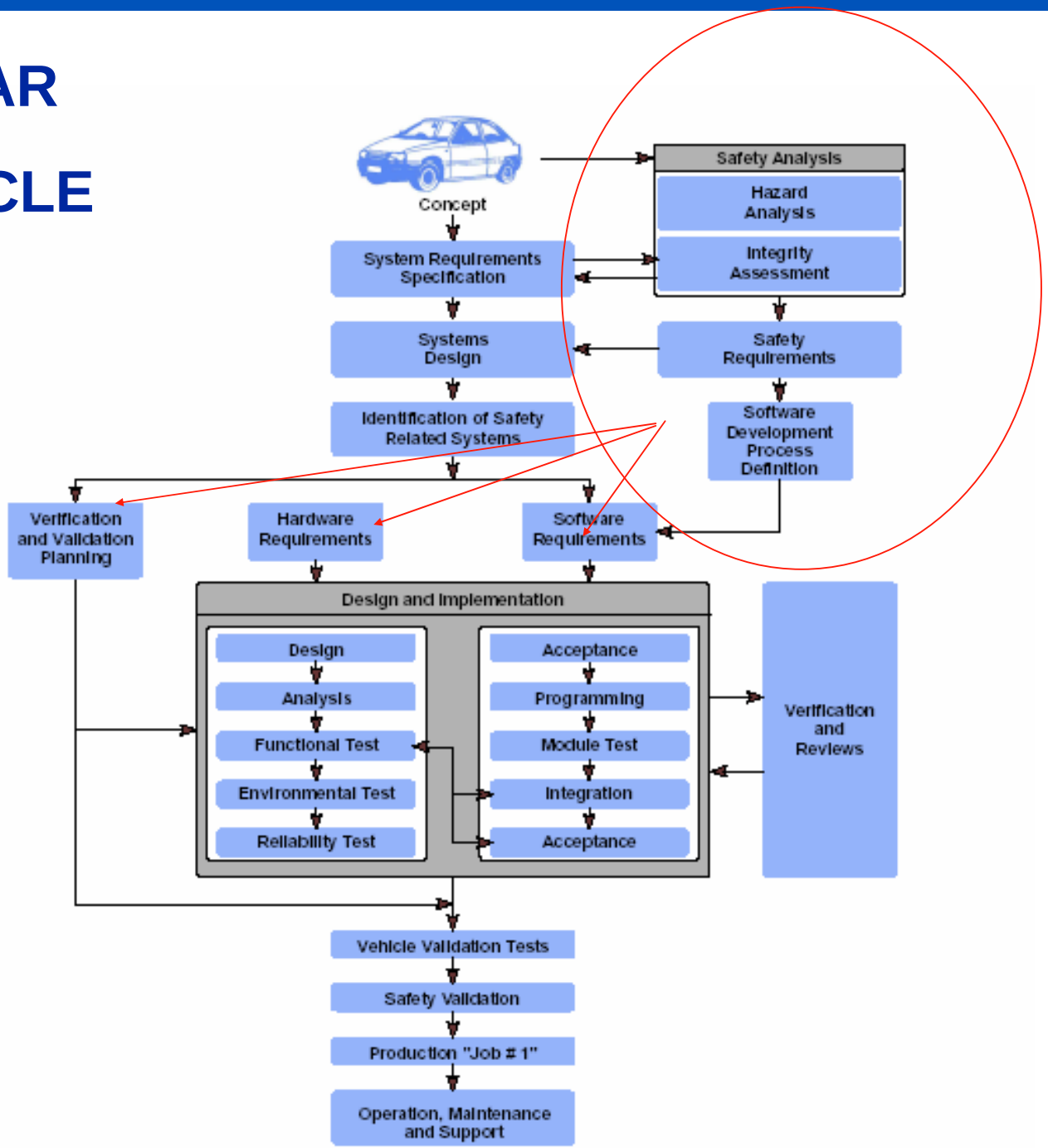
THE GROWTH OF THE COMPLEXITY OF ELECTRONIC SYSTEMS ON BOARD A CAR LEADS TO AN INTRINSIC NEED OF TRUST IN ECU'S

MANUFACTURERS WANT TO AVOID ANY ACCIDENT FOR LEGAL MATTERS AND LOSS OF REPUTATION

SAFETY HAS IMPACTS ON THE WHOLE ARCHITECTURE OF A SYSTEM: HARDWARE AND SOFTWARE, THE REQUIRED SYSTEM'S SAFETY LEVEL IS REACHED WITH THE CONTRIBUTION OF BOTH.

SAFETY IN THE CAR

PROJECT LIFECYCLE



SAFETY IN THE ARCHITECTURE

SAFETY IS NOT ONLY A MATTER OF SOFTWARE, BUT IT IS THE COMBINATION OF THE CONTRIBUTION OF HW & SW

SIMPLE ARCHITECTURE IN BOTH HW & SW IS THE WINNING APPROACH: COMPLEX SYSTEMS ARE HARDLY CONTROLLABLE

CONFINING THE SAFETY RELATED AREAS IN A WELL DEFINED HW SECTION OR SW COMPONENT IS THE MOST EFFECTIVE WAY TO PRODUCE SAFE SYSTEMS.

A SMALL HW AREA CAN BE ANALYSED AND CONTROLLED BETTER AND DEEPER THAN A BIG ONE. THE SAME APPLIES TO THE SW.

SOMETIMES IS BETTER TO ADD A DEDICATED PART OF HW OR A DEDICATED SW ROUTINE TO IMPLEMENT THE SAFETY REQUIREMENTS RATHER THEN INCLUDE SAFETY FEATURES IN A CHEAPER (i.e. POOR) ARCHITECTURE.

SAFETY IN THE ARCHITECTURE cont'd

THE TYPICAL SAFE APPROACH IS TO HAVE FUNCTIONS SEPARATION OR REDUNDANCY DEPENDING UPON THE SAFETY TARGET.

HW CHANNELS CAN BE DUPLICATED AND THE SW CAN MANAGE THESE CHANNELS IN DIFFERENT WAYS, IN ORDER TO MINIMIZE ERROR RISKS.

THE WRAP-AROUND (READ BACK) OF DIGITAL AND ANALOGUE OUTPUTS IS A MEANS TO CONTROL THE OUTPUTS OF A SYSTEM. IF THE COMPARISON BETWEEN SET AND READ VALUES FAILS, A RECOVERY ACTION SHALL TAKE PLACE. THIS LEADS TO THE NEED OF RESERVING SOME FREE INPUTS.

THE USE OF AN EXTERNAL, WINDOW TYPE, WATCHDOG OR INTERNAL, BUT WITH SEPARATED CLOCK.

A MULTIPROCESSOR ARCHITECTURE IN WHICH ONE CONTROLLER MANAGES SAFETY MATTERS, LEAVING TO THE OTHER THE NON SAFETY TASKS.

SAFETY IN THE ARCHITECTURE cont'd

THE POSSIBILITY TO CUTOFF ALL THE DANGEROUS ACTUATIONS BY MEANS OF A HW CUT-OUT LINE, MAYBE CONNECTED TO THE WATCHDOG.

THE POSSIBILITY TO READ THE DGND IN THE A/D CONVERTER CHANNEL SO TO DISCHARGE PARASITIC CAPACITANCE OF THE MUX.

AVOID ANY FLOATING SIGNAL ON THE PCB.

MANY MORE…

SAFETY IN THE PROJECT LIFECYCLE

AN EARLIEST APPROACH IS THE MOST EFFECTIVE ONE

PSA USES THE S.D.F METHOD : SURÉTÉ DE FONCTIONNEMENT

IT STARTS FROM THE ANALYSIS OF FEARED EVENTS AND GIVES THEM A CRITICALITY LEVEL (4 THE MOST DANGEROUS)

IT IS BASED ON FUNCTIONS ANALYSIS: i.e. THE FEARED EVENT IS “THE REAR DOOR SHALL NOT BE OPENED IF THE KID SECURITY IS ACTIVE”

TO THIS LIST THE ECU SUPPLIER SHALL ANSWER WITH HW+SW SOLUTIONS WHOSE TARGET IS TO MINIMIZE THE PROBABILITY THAT THE FEARED EVENT HAPPENS (GOTO F.T.A.)

THIS LIST BECOMES THE LIST OF SAFETY REQUIREMENTS: FROM HERE ONWARD, THE SAFETY ENTERS THE SOFTWARE LIFECYCLE

SAFETY IN THE PROJECT LIFECYCLE cont'd

ANOTHER APPROACH IS THE F.T.A. : FAULT TREE ANALYSIS

IT STARTS FROM THE ANALYSIS OF THE POSSIBLE MALFUNCTION OF A COMPONENT (HW & SW): i.e. "WHAT HAPPENS IF THIS COMPONENT (HW & SW) FAILS IN WHATEVER MODE ?

THIS APPROACH GENERATES A LIST OF COUNTERMEASURES

THIS LIST BECOMES THE LIST OF SAFETY REQUIREMENTS: FROM HERE ONWARD, THE SAFETY ENTERS THE SOFTWARE LIFECYCLE

SAFETY IN THE SOFTWARE LIFECYCLE

THE FUNDAMENTAL STEPS:

1. ANALYSE RISKS
2. SPECIFY SAFETY REQUIREMENTS
3. DESIGN AND IMPLEMENT SAFETY FUNCTIONS
4. DESIGN SAFETY RELATED TEST CASES
5. PERFORM SAFETY ASSESSMENT INTERNALLY OR TOGETHER WITH CERTIFICATION AUTHORITIES

THE OUTCOMES:

1. RECORD SAFETY REQUIREMENTS INTO THE SRS
2. RECORD SAFETY FUNCTIONS INTO THE SAD
3. RECORD SAFETY TEST CASES INTO THE SWTP

SAFETY IN THE CODE

SAFE CODE IS OFTEN ROBUST CODE, SO ALL THE ROBUSTNESS IMPLEMENTATION RULES WORK FOR THIS UNIQUE TARGET.

THE RUN-TIME REFRESHING OF THE OUTPUTS CONFIGURATION REGISTERS TO AVOID UNWANTED COMMANDS TO ACTUATORS.

POSSIBLY AVOID INTERRUPTS ON EXTERNAL SOURCES: TRY TO ALLOCATE THE EXTERNAL READINGS IN A SUFFICIENTLY FAST ROUTINE BASED ON AN INTERNAL INTERRUPT.

PUT FLAGS ON TOP AND BOTTOM OF THE STACK IN ORDER TO VERIFY TOO MUCH NESTED CALL OR OTHER CAUSES OF OVERWRITING.

ALLOCATE ARRAYS FAR FROM DECISIONAL VARIABLES. CHECK ARRAYS' POINTERS BEFORE USING THEM.

ALWAYS CHECK FOR ZERO DIVISION BEFORE COMPUTATIONS.

SAFETY IN THE CODE cont'd

POSSIBLY USE SEPARATE PATHS TO GENERATE COMPLEMENTARY COPIES OF THE SAME VARIABLE IN DIFFERENT MEMORY AREAS.

ALWAYS USE TIMEOUTS IN LOOPS.

PROTECT CONFIGURATION DATA BY MEANS OF CHECKSUM AND/OR DUPLICATE THE MEMORY AREAS CONTAINING SUCH DATA.

PERFORM A Built In Test (BIT) AT POWER ON, CHECKING MEMORIES BY MEANS OF WRITE/READ OPERATION IN RAM AND CHECKSUM IN FLASH.

A FAILURE IN THE INITIAL BIT SHALL PRODUCE A WD INTERVENTION.

DON'T TRUST IN CPU OR MEMORY TEST PERFORMED AT RUN-TIME: DON'T WASTE CPU TIME TO MAKE USELESS TESTS.

AVOID RAM RUNNING ROUTINES AND RECURSIVE CODE.

SAFETY IN THE CODE cont'd

DIGITALLY FILTER ALL INPUTS (i.e. DEBOUNCE ON BUTTONS)

PERFORM CONGRUITY TESTS ON INPUTS (i.e. THRESHOLD TESTS)

PERFORM RATE OF CHANGE TESTS ON ANALOGUE INPUTS

MANY MORE…

RECOVERY ACTIONS

GREAT IMPORTANCE HAVE RECOVERY ACTIONS:

IF ONE OF THE SAFETY COUNTERMEASURES (HW OR SW) DETECTS A MALFUNCTION THE APPROPRIATE RECOVERY ACTION SHALL TAKE PLACE.

MAINLY THE RECOVERY ACTION SHALL MINIMIZE THE EFFECTS OF THE HAZARDOUS EVENT

THIS CAN BE DONE:

1. **BY TRYING TO RESTORE WORKING CONDITIONS AS SOON AS POSSIBLE (i.e. WD RESET)**
2. **BY LEAVING THE ECU IN A SAFE CONDITION JUST WARNING OUT TO OTHER CAR COMPONENTS ITS MALFUNCTION IN THE SIMPLEST WAY.**

SPICE AND SAFETY

THE RELATIONSHIP BETWEEN SPICE AND SAFETY ARE, AT THE MOMENT, ONLY CONFINED AT PROJECT MANAGEMENT, RISK MANAGEMENT AND VALIDATION PROCESS AREAS.

THERE ARE NO LINKS ON TECHNICAL MATTERS: SIMPLY GENERALLY SPEAKING “A WELL ORGANISED SOFTWARE DEVELOPMENT PROCESS LEADS TO A SAFER PROJECT RATHER THAN ONE NOT FOLLOWING THIS APPROACH”

IF SYRS, SRS, SAD, CODE AND SWTP ARE WELL DONE, THEY WILL BE ABLE TO EXPLAIN AND TRACE ALL THE SAFETY REQUIREMENTS IN A CLEAR WAY. THE SIMPLEST , THE BEST.

A DEEPER VALIDATION HELPS IN FINDING OUT, AT EARLY PHASES, PROBLEMS AND DEFECTS WHICH COULD BE VERY DANGEROUS AND EXPENSIVE, IF FOUND LATER ON.

SAFETY AND THE RULES

THE ISO WD 26262 IS NOT AVAILABLE YET: GUIDELINES CAN BE FOUND IN THE IEC61508 WHICH IN ANY CASE WAS NOT INTENDED FOR AUTOMOTIVE USE

ROBUST DESIGN AND COUNTERMEASURES GUIDELINES, INCREASING PROPORTIONALLY TO THE CRITICALITY OF THE FUNCTIONS, CAN BE FOUND IN THE EN60730 Annex H

AGAIN IS A DOCUMENT NOT SPECIFIC FOR AUTOMOTIVE USE, BUT AT LEAST IT GIVES TECHNICAL GUIDELINES TO UNDERSTAND WHAT CAN BE DONE IN HW AND SW TO BUILD A SAFE DESIGN

MISRA GUIDELINES DOCUMENT ALSO GIVES INDICATIONS ON HOW TO DETERMINE THE CRITICALITY LEVEL OF AN ECU OR FUNCTION.

BY WRITING MISRA-C SOFTWARE IS AN IMPROVEMENT IN THE READABILITY AND MAINTAINABILITY OF THE SOURCE CODE