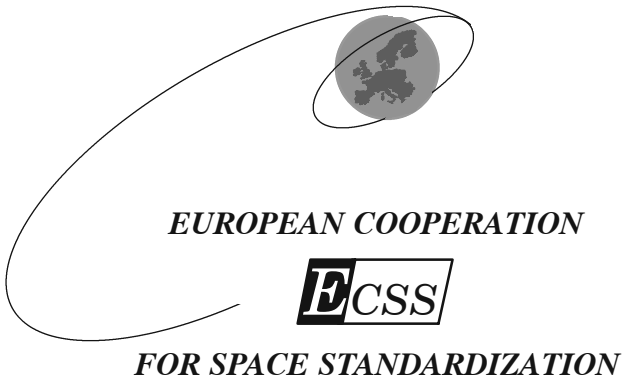
ECSS-Q-40-04A Part 2
14 October 1997



Space Product Assurance

Sneak analysis - Part 2: Clue list

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Published by: ESA Publications Division
ESTEC, P.O. Box 299,
2200AG Noordwijk,
The Netherlands

ISSN: 1028-396X

Price: DFl 50

Printed in the Netherlands

Foreword

This standard is one of the series of ECSS standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, National Space Agencies and European industry associations for the purpose of developing and maintaining common standards.

The application of Sneak Analysis is required by ECSS-Q-40 “Safety”.

This standard has been prepared by editing the ESA Standard PSS-01-411 Issue 1, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Contents List

1

Scope

The aim of Sneak Analysis is to identify “sneak circuits”, i.e. unexpected paths for a flow of mass, energy, data or logical sequence that under certain conditions can initiate an undesired function or inhibit a desired function. Sneak circuits are not the result of failure, but are latent conditions, inadvertently designed into the system.

This standard establishes a procedure for performing sneak analysis and specifies the required output.

The standard is composed of two parts:

- part 1 (i.e. the document ECSS-Q-40-04 Part 1 “Sneak analysis - Part 1: Method and procedure”) that contains the method and procedure for performing sneak analysis;
- part 2 (i.e. this document ECSS-Q-40-04 Part 2 “Sneak analysis - Part 2: Clue list”) that contains a basic clue list to be used during sneak analysis.

This standard is applicable when the performance of sneak analysis is required by ECSS-Q-40 or by the business agreement between the customer and the supplier.

Alternative clue lists proposed by the supplier may be accepted by the customer provided that equivalence, for the intended application, with the one presented in this standard is shown by the supplier.

(This page is intentionally left blank)

2

Normatives references

This ECSS Standard incorporates by dated or undated reference, provisions from other publications. These normative references to the extent specified in the text are cited at the appropriate places and publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these apply to this ECSS Standard only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

ECSS-P-001	Glossary of terms
ECSS-Q-40-04 - Part 1	Sneak analysis - Part 1: Method and procedure

(This page is intentionally left blank)

3

Definitions and abbreviations

3.1 Definitions

For the purposes of this standard, the definitions given in ECSS-P-001 and in ECSS-Q-40-04 - Part 1 apply. In particular, it should be noted that the following terms have a specific definition for use in ECSS standards.

Configuration Item

Failure

Severity

Software

System

The following terms are defined in ECSS-Q-40-04 - Part 1 and shall be applied.

Clue

Design concern

Design error

Facilitation condition

Sneak circuit

Sneak indication

Sneak label

Sneak path

Sneak timing

Target

3.2 Abbreviations

The following abbreviations are defined and used within this standard.

Abbreviation	Meaning
CAD	Computer Aided Design
CMOS	Complementary metal-oxide silicon
EEE	Electrical, electronic and electromechanical
FMECA	Failure Modes, Effects and Criticality Analysis
HW	Hardware

I/O Matrix	Input/Output Matrix
PA	Product Assurance
PCB	Printed Circuit Board
RAMS	Reliability, Availability, Maintainability and Safety
SW	Software
TTL	Transistor-Transistor Logic
V**CC**	Voltage controlled current

In addition Annex A defines the abbreviations that are to be used as keywords when searching in the clue lists given in Annexes B, C and D for the clues relevant to a specific item.

4

Clue list structure

4.1 Taxonomy of items

Annex A contains the taxonomy of "items" namely EEE and hydraulic components, software instructions) relevant to the clues listed in this document.

For EEE equipment and software written in the ADA language the clues contained in Annexes B and C shall be used.

When Sneak Analysis is to be applied to a hydraulic system or subsystem the clues contained in Annex D may be used.

The Annexes of this document may be obtained, upon request from the ECSS secretariat, either as word-processor file or as a database for personal computers.

4.2 Structure of the entries of the clue list

A clue is defined in ECSS-Q-40-04A - Part 1, 3.1 as a: "**question** pointing at a possible way through which design errors associated with one or more **items** of a system can lead to a system malfunction".

To apply a particular clue, it is necessary to clearly identify:

- the text of the question;
- to which items the questions applies (the taxonomy of these items is contained in Annex A).

To facilitate the management of the clue list and its application other attributes are attached to each clue, i.e.:

- an unambiguous alphanumeric identifier (clues for EEE equipment have identifiers in the range 1-999, clues for software have identifiers in the range 1000-1999, clues for hydraulic equipment have identifiers in the range 2000-2999);
- a "clue short title" which provides a short description of the content of the clue;

the "clue explanation", i.e. a short explanation of the clue text;

To restrict the use of the various clues to the sneak analysis procedure for which they are intended (see ECSS-Q-40-04 - Part 1, 4.1), the attribute "clue type" has been associated to each entry of the list.

- If a clue type is "path-component" then it is intended for use during the application of the sneak path analysis;
- If a clue type is "component-only" then it is intended for use during the application of the design concern analysis.

It is noted that some clues are intended for use both during sneak path analysis and design concern analysis and these are typed by two keywords “path-component” and “component-only”.

Some “component-only” clues need to be applied only once to each member of the taxonomy and not to each component in the system under analysis. These clues are identified by the keyword “once-only” and are to be used only during the design concern analysis. For an example, see clue 60 in Annex B.

The “path” clues (see ECSS-Q-40-04 - Part 1, 4.1) can be derived, according to the approach described in Annex A of ECSS-Q-40-04 - Part 1, from the causal relation between “source” and “target” that is of interest. Therefore the “path” clues are not listed in this document.

The coding of an entry of the clue list is illustrated by the following example:

EXAMPLE

identifier ①	30
Title ②	protection against reverse voltage
Clue type ③	component-only
Item ④	regulator+OpAmp
Clue Text ⑤	Is a regulator protected against reverse voltage?

Explanation: ⑥If a voltage drop or a short circuit occurs at the regulator input, the reverse voltage applied to the regulator can exceed the breakdown voltage. If the regulator has no internal protection diode, an external protection diode shall be added.

The table entries are:

① = univocal alphanumeric identifier

② = clue short title

③ = clue type

④ = items to which the question applies

⑤ = the question pointing at a possible way through which design errors can lead to a system malfunction

⑥ = clue explanation

Annex A (informative)

Taxonomy

This Annex presents the taxonomy of three classes of "item", EEE and hydraulic components, ADA language instructions to which the clues contained in this document apply.

The taxonomy is present in the form of a tree in which the "hierarchical level" (currently ranging from 0 till 7) is given next to the name of the item. The level of a particular item within the hierarchy is shown by the amount of indentation from the left hand marging, lower level items being more indented than an item in the level above.

When a clue pertains to a parent item, it also pertains to the daughter items.

0,"Component",
1,"Part",
2,"signal"
2,"label"
3,"Offpage" (connection symbol between different drawings)
2,"Electronic"
3,"Active"
4,"IC" (integrated circuits)
5,"Digital"
6,"driver"
6,"tristate"
6,"gate"
7,"buffer"
7,"and"
7,"nand" (negated AND)
7,"or"
7,"nor" (negated OR)
7,"not"
7,"xor" (exclusive OR)
6,"memory"

7,"RAM" (random access memory)
8,"DRAM" (dynamic RAM)
8,"SRAM" (static RAM)
7,"ROM" (read-only memory)
8,"PROM" (Programmable ROM)
8,"EPROM" (Erasable PROM)
8,"EEPROM" (Electrically EPROM)
6,"Array"
7,"PLA" (Programmable logic array)
7,"LCA" (Logic cell array)
7,"EPLD" (Electrically programmable logic device)
7,"PAL" (Programmable array logic)
6,"Static"
7,"latch"
7,"JK" (J-K flipflop)
7,"register"
7,"flipflop"
7,"monoflop"
7,"bistable"
7,"RS" (Reset-Set flipflop)
5,"Counting"
6,"counter"
6,"mux" (multiplexer)
6,"shift"
6,"adder"
6,"Clock"
6,"Oscillator"
5,"Processing"
6,"micropro" (microprocessor)
6,"ASIC" (Application specific IC)
6,"DAC/ADC" (digital to analog converter/analog to digital converter)
6,"regulator" (voltage regulator)
6,"communication"
5,"Analogue"
6,"amplifier"
6,"OpAmp" (operational amplifier)
6,"comparator"
4,"Transistor"
5,"bipolar"
6, "PNP"
6, "NPN"
5,"Darlington"
5,"MOS" (metal-oxide semiconductor)

```
                    5,"FET"             (field effect transistor)
                4,"Diode"
                    5,"Zener"
                    5,"LED"             (light emitting diode)
                    5,"optocoupler"
                4,"Rectifier"
                    5,"Thyristor"
                    5,"Triac"
                    5,"GTO"             (gate turn-off thyristor)
                    5,"Thyratron"
            3,"Passive"
                4,"Resistor"
                4,"Capacitor"
                4,"Heater"
                4,"Thermistor"
                4,"Potentiometer"
                4,"Varistor"            (variable resistor)
                4,"Inductor"
                    5,"coil"
        2,"Electromechanic"
            3,"Contactor"
                4,"Breaker"
                4,"Limiter"
                4,"Relay"
                    5,"bistabrel"       (bistable relay)
                    5,"monostable"      (monostable relay)
                    5,"monofloprel"     (monoflop relay)
                    5,"Relaycoil"
                    5,"Relaypole"
                        6,"Singlepole"
                        6,"Multipole"
                4,"Switch"
                4,"Contact"
                4,"Button"
            3,"Transducer"
                4,"Motor"
                    5,"Motorcoil"
                    5,"Actuator"
                4,"EED"         (electroexplosive device)
                    5,"Squib"
                    5,"Explosive"
                    5,"Detonator"
                    5,"Initiator"
                    5,"Exbolt"      (explosive bolt)
```

4,"Speaker"
5,"Loudspeaker"
5,"Buzzer"
5,"Bell"
4,"Microphone"
4,"Detector"
4,"Sensor"
5,"CSens" (current sensor)
5,"FSens" (fire sensor)
5,"VSens" (voltage sensor)
5,"TSens" (temperature sensor)
5,"PSens" (pressure sensor)
5,"PoSens" (position sensor)
5,"XSens" (concentration sensor)
5,"LSens" (level sensor)
4,"Threshold"
2,"Electric"
3,"Binding"
4,"Fuse"
4,"Connector"
5,"Multiconnector"
5,"Interlock"
5,"Malecon" (male connector)
5,"Femalecon" (female connector)
5,"Plug"
5,"Terminal"
5,"Strap"
5,"Testpoint"
5,"Testgap"
4,"Wire"
4,"Cable"
4,"Bundle"
4,"Splice"
4."Node" (node of the electrical schematic)

3,"Transformation"
4,"Transformer" ("trafo" is a synonym of transformer)
4,"Autotransfo" (auto transformer)
4,"Lamp"
5,"Neon"
5,"Indicator"
4,"Tube"
4,"Antenna"
3,"Earth"

4,"Ground"
4,"Chassis"
3,"Energy"
4,"power"
5,"Battery"
5,"Supply"
4,"Load"
4,"Regulator"
1,"Software"
2,"OUTPUT"
2,"OUTREG" (output register)
2,"INPUT"
2,"INREG" (input register)
2,"LOOP"
3,"FOR"
3,"REVERSE"
3,"END LOOP"
3,"EXIT"
3,"EXIT WHEN"
2,"GOTO"
2,"RETURN"
2,"CALL"
3,"PACKAGE"
3,"END"
3,"PROCEDURE"
3,"FUNCTION"
3,"EXCEPTION"
3,"RAISE"
3,"TASK"
3,"BEGIN"
3,"GENERIC"
3,"SEPARATE"
3,"SEMAPHORE"
2,"BOX" (software instruction implementing algorithmic operations, e.g. additions, divisions)
2,"ASSIGN" (software instruction that assign values to variables)
2,"DIAMOND"
3,"IF"
3,"ELSE IF"
3,"CASE"
3,"WHEN"
3,"WHILE"
3,"OTHERS"
2,"ENDCONDITIONAL"

```
                3,"ELSE"
                3,"END IF"
                3,"END CASE"
                3,"END LOOP"
                3,"NULL"
            2,"THEN"
            2,"DECLARATION"
                3,"CONSTANT"
                3,"TYPE"
                    4,"NEW"
                    4,"DIGITS"
                    4,"DELTA"
                    4,"RANGE"
                    4,"SUBTYPE"
                    4,"IS"
                    4,"RECORD"
                    4,"ACCESS"
                    4,"PRIVATE"
                    4,"RANGE"
                3,"RENAME"
                3,"IS SEPARATE"
        1,"hydraulic"
            2,"tank"
                3,"tankpres"    (sealed container)
                3,"tankbladder"
                3,"vessel"
            2,"valve"
                3,"sv"          (relief valve)
                3,"cvalve"      (control valve)
                3,"checkv"      (check valve)
            2,"pump"
            2,"turbine"
            2,"vent"
            2,"drain"
            2,"pregulator"      (pressure regulator)
```

Annex B (normative)

Clues for electrical, electromechanical and electronic equipment

Identifier	23B
Title	place of the switching items
Clue type	component-only path-component
Item	switch+contact+breaker
Clue Text	Is the switch placed in the lower branch that closes the circuit for two or more upper (power dome) branches

Explanation: If a switching item is placed in the common branch, it may lead to a general current interruption in the multiple branches.

Identifier	24
Title	transient exceeding max current
Clue type	component-only
Item	transistor
Clue Text	Can a current transient exceed transistor max current?

Explanation: During power transition or switching for instance, high inrush current may occur (capacitor charging): this current transient can induce a voltage transient, exceeding a breakdown voltage of the transistor. If a transistor is used to switch an inductive load without appropriate transient suppression measures being taken, there is a risk that the transistor may fail. When a resistor is used as a current path, and is connected in parallel with the emitter and the base of a transistor, if a reverse current flows through the resistor (temporary short circuit), the reverse base-emitter breakdown voltage can easily be exceeded (about 5 Volts).

Identifier	24A
Title	transient exceeding breakdown voltage
Clue type	component-only
Item	transistor
Clue Text	Can a voltage transient exceed transistor breakdown voltage?

Explanation: If a transistor is used to switch off an inductive load without appropriate transient suppression measures being taken, there is a risk that the transistor may fail.

Identifier	24B
Title	reverse current through collector
Clue type	component-only
Item	transistor
Clue Text	Can a voltage transient exceed emitter breakdown voltage?

Explanation: When a resistor is used as a current path, and is connected in parallel with the emitter and the base of a transistor, if a reverse current flows through the resistor (temporary short circuit), the reverse base-emitter breakdown voltage can easily be exceeded (about 5 Volts).

Identifier	25
Title	permanent electrical link across a contact
Clue type	once-only
Item	relay+switch+contact+button
Clue Text	Does a permanent low current flow through the contact?

Explanation: The contact resistance may become significant if the current is low and the current won't be sufficient for the contact regeneration; RESET and SET cycles shall be scheduled for the contact regeneration if no other possibility exists.

Identifier	26
Title	parallel MOSFET transistors
Clue type	component-only
Item	transistor
Clue Text	Are the oscillations generated by two parallel MOSFET transistors damped out by an appropriate circuit?

Explanation: Two parallel MOSFET transistors can create an oscillating circuit.

Identifier	27A
Title	voltage compatibility between different IC families
Clue type	component-only
Item	IC
Clue Text	Is the voltage compatibility between circuits of different families respected?

Explanation: A problem of voltage compatibility can occur between different circuit families and it may lead to a sneak current path. Particular attention should be paid during power transition or when different voltage values are used at interfaces. Voltage differences at interface often occur:

- during power on/off, some parts of the circuit may have reached their operational voltage while others are still changing
- during power on/off, within a circuit supplied with separated voltages, one voltage may have reached its operational value while others are still changing
- separated parts of a circuit can be independently supplied, one being powered while the others are not.

Identifier	27B
Title	collector-base junction reverse biased
Clue type	component-only
Item	transistor
Clue Text	Can the collector-base junction be reverse biased?

Explanation: A transistor receiving on its base an active signal while it is not nominally powered may induce a sneak current path towards a load, a power source or the ground through the collector-base junction if reverse biased. Particular attention should be paid during power transition or when different voltage values are used at interface. Voltage differences at interface often occur:

- during power on/off, some parts of the circuit may have reached their operational voltage while others are still changing
- during power on/off, within a circuit supplied with separated voltages, one voltage may have reached its operational value while others are still changing
- separated parts of a circuit can be independently supplied, one being powered while the others are not.

Identifier	27C
Title	excessive reverse bias
Clue type	component-only
Item	diode
Clue Text	Can the diode junction be biassed beyond breakdown?

Explanation: This can particularly occur if there are multiple voltages, or possibilities for voltage spikes.

Identifier	28
Title	non-linear transfer function
Clue type	component-only
Item	OpAmp+transistor
Clue Text	Is a compensation network implemented to correct a non-linear transfer pattern, that supplies the lower branches?

Explanation: Either a non-linear function is designed to be non-linear (pre-accentuation of high frequencies for instance), either the non-linearity is unexpected and then a compensation network should be added. Multiple circuits in series (OpAmp) generally induce non linear transfer functions.

Identifier	29
Title	feedback network on separated boards
Clue type	component-only
Item	signal+node+amplifier+OpAmp+transistor
Clue Text	Is the feedback network implemented on separated boards?

Explanation: The wire length used to connect the separated boards can induce variable inductive and capacitative effects, modifying the feedback characteristics. The response for the circuit may be altered and oscillation may arise.

Identifier	30
Title	protection against reverse voltage
Clue type	component-only
Item	regulator+OpAmp
Clue Text	Is a regulator protected against reverse voltage?

Explanation: If a voltage drop or a short circuit occurs at the regulator input, the reverse voltage applied to the regulator can exceed the breakdown voltage. If the regulator has no internal protection diode, an external protection diode shall be added.

Identifier	32A
Title	filtering of a power source
Clue type	component-only
Item	power+supply+battery
Clue Text	Is there a filter at the output(s) of the power source?

Explanation: Filters shall be added in order to smooth ripple and avoid spikes to propagate outside the power source through the wiring.

Identifier	32AA
Title	filtering of a power source
Clue type	component-only
Item	power+supply+battery
Clue Text	Is there a filter at the output(s) of the power source?

Explanation: Filters shall be added in order to smooth ripple and avoid spikes to propagate outside the power source through the wiring.

Identifier	32B
Title	filtering of cables and long lines
Clue type	component-only
Item	buffer+connector
Clue Text	Is there a radio frequency (RF) filter provided on circuit output(s) interfacing cables and long lines?

Explanation: A RF filter shall be added in order to avoid RF to propagate through the wiring.
Note: you will need to check wire or cable length for this clue.

Identifier	33
Title	frequency pass band for measurement
Clue type	component-only
Item	sensor+OpAmp+comparator
Clue Text	Is the frequency pass band of the measurement circuit adapted to the physical phenomenon?

Explanation: The acquisition frequency of a measurement / instrumentation circuit shall be at least twice the frequency of the measured phenomenon (Shannon theorem)

Identifier	34
Title	delay of a signal
Clue type	component-only
Item	signal+cable+connector+offpage+malecon+femcon
Clue Text	Can the time constant of a signal path induce a critical delay for the signal?

Explanation: A long signal path between circuit boards can cause signal delays and resultant timing sneaks. Digital devices, analog switches comparators and transistors may exhibit unpredictable behaviour due resulting glitches.

Identifier	34AA
Title	delay of a signal
Clue type	path-component component-only
Item	signal+cable+connector+offpage+malecon+femcon
Clue Text	Can the time constant of a signal path induce a critical delay for the signal?

Explanation: A long signal path between circuit boards can cause signal delays and resultant timing sneaks. Digital devices, analog switches comparators and transistors may exhibit unpredictable behaviour due resulting glitches.

Identifier	34A
Title	RC/LC time constant
Clue type	path-component component-only
Item	capacitor+inductor
Clue Text	Can the time constant of a resistor-capacitor or inductor-capacitor circuit induce a critical delay for the signal?

Explanation: If a resistor-capacitor network is implemented on the signal path, a delay is induced that may introduce a sneak timing. The rise and fall times may be affected, especially for digital circuits, and the operating frequency may not be achieved. Moreover, with low rise and fall times, digital circuit may deliver erroneous signals. Digital devices, analog switches comparators and transistors may exhibit unpredictable switching times and excessive power dissipation due to imprecise switching caused by excessive input time constants.

Identifier	4
Title	command input implementation
Clue type	component-only
Item	bistable+flip-flop+register+latch+counter+JK+RS+bistabrel
Clue Text	Are both the SET/START command and the RESET/STOP command implemented?

Explanation: As an example, if only the SET/START command is implemented, once the function has been activated, it will always remain in the same state as the RESET/STOP command is not available!

Identifier	5A
Title	maximum frequency delays
Clue type	component-only
Item	IC+gate+and+or+nand+nor+not
Clue Text	Have the propagation time, the rise time and fall time been taken into account for the maximum frequency calculation?

Explanation: There may be sneak timing problems if the expected signal frequency is close to a component maximum frequency limit.

Identifier	34B
Title	delay due to parasitic capacitance
Clue type	path-component component-only
Item	diode
Clue Text	Can the time constant of a signal path induce a critical delay for the signal due to parasitic capacitance?

Explanation: The forward resistance and the parasitic capacitance of a diode can induce a delay on the signal path.

Identifier	34C
Title	delay of a signal, high output resistance
Clue type	path-component component-only
Item	battery+power+supply+psens+tsens+lsens+fsens+xsens
Clue Text	Can the time constant of a signal path induce a critical delay for the signal due to high output resistance?

Explanation: A high output impedance state can cause slow operation due to the long RC time constant. Digital devices, analog switches comparators and transistors may exhibit unpredictable switching times and excessive power dissipation due to imprecise switching caused by excessive input time constants.

Identifier	35
Title	voltage protection on inputs
Clue type	component-only
Item	OpAmp+comparator
Clue Text	Is the component protected against erroneous voltages on its inputs?

Explanation: When multiple signals are connected to the same input through resistors (summator, subtractor), a sneak current path can occur between these multiple signals if one of them delivers a voltage higher than expected:
(Zener) diodes can be connected across each signal input.
Protection diodes can also be implemented to limit the differential voltage between inputs.

Identifier	36A
Title	location of monitoring circuit
Clue type	component-only
Item	sensor+detector+indicator+lamp+psens+fsens+tsens+xsens+lsens +posens
Clue Text	Is a monitoring circuit located and connected so that it delivers the status of the function to be monitored?

Explanation: The monitoring circuit shall indicate only the status of the monitored function, not the status of another function.

Identifier	40A
Title	disconnection from signal source
Clue type	path-component component-only
Item	sensor+detector+lamp+indicator+psens+fsens+xsens+lsens+csens
Clue Text	Can the monitoring circuit be disconnected from the monitored signal or device?

Explanation: The monitoring circuit should not indicate the opposite state of the monitored function.

Identifier	41
Title	indication stability during transition
Clue type	component-only
Item	sensor+indicator+lamp+detector
Clue Text	Is the information delivered by the monitoring circuit stable and consistent during signal or state transitions?

Explanation: During power or mode transitions, the monitoring circuit shall give appropriate information to the system.

Identifier	42
Title	digital distributed signal
Clue type	path-component component-only
Item	clock+oscillator
Clue Text	Are the rise and fall times of a clock signal acceptable?

Explanation: For instance, if a clock signal is distributed to many circuits, the input capacitances of each circuit add and the clock generator may deliver a degraded clock signal with a slow leading and trailing edges and possibly a distorted waveform and no clear leading edge.

Identifier	43
Title	unused inputs
Clue type	component-only
Item	IC+and+or+nand+nor+not+JK+RS+flipflop+register+latch
Clue Text	Are integrated circuits unused inputs correctly polarized or grounded?

Explanation: Some integrated circuits include internal polarization on their inputs/outputs. For others, integrated circuit unused inputs shall not be left floating: open inputs cause decreased noise immunity, unnecessary power dissipation due to instability. For instance:

- feedback between the output "-" of an OpAmp and "+" correctly polarized through a resistor
- unused digital circuit inputs connected to the ground/power through a resistor.

Identifier	43A
Title	unused inputs tied to other inputs
Clue type	component-only
Item	IC+and+or+nand+nor+not+JK+RS+flipflop+register+latch
Clue Text	Are unused inputs tied to other inputs?

Explanation: Tying unused inputs to used inputs of the same circuit is not advisable as it reduces AC noise immunity due to increased input coupling capacitance.

Identifier	44A
Title	protection against transient voltage
Clue type	component-only
Item	power+supply+battery
Clue Text	Is there a protection against transient voltages?

Explanation: Fast protective diodes (TRANSIL) can be used to protect against transient overvoltages which may cause latch-up or even permanent failure. Zener diodes can also be used. A voltage protective device on each voltage source shall be implemented to prevent the circuits using these voltages from being damaged due to overvoltage.

Identifier	3B
Title	overflow
Clue type	component-only
Item	counter+shift+adder
Clue Text	Is there an overflow detection circuit?

Explanation: The out of limits detection circuit should ensure detection if the nominal range of measurement is saturated.

Identifier	44C
Title	protection against transient currents
Clue type	component-only
Item	power+supply+battery
Clue Text	Is there a protection against current transients?

Explanation: During switching, high currents may flow, especially if the load is partly capacitative, or if there are large motors. Sneak conditions may mean that more than the planned number of loads of this type are connected at one time.

Identifier	45
Title	tristate outputs for multi-user line/bus
Clue type	component-only
Item	buffer+driver
Clue Text	Are interface circuits of tristate type when used on a bus?

Explanation: To avoid a short circuit between the different users sharing a single line or bus, tristate outputs shall be used.

Identifier	45A
Title	tristate outputs for multi-user line/bus
Clue type	component-only
Item	buffer+driver
Clue Text	Can tristate outputs to a bus be activated at the same time?

Explanation: To avoid a short circuit between the different users sharing a single line or bus, tristate outputs shall be only be activated one at a time.

Identifier	46
Title	pull-up resistor for multi-user line/bus
Clue type	component-only
Item	buffer+and+or+nand+nor+not+IC+RAM+ROM
Clue Text	Is there one pull-up/down resistor attached to tristate outputs?

Explanation: There shall be a pull-up/down resistor attached to tristate outputs in order to polarize the line output during the high impedance state. When there is a bus, only one pull-up/down resistor is necessary per bus line in complex circuits, duplicate pull-up/down resistors may have been implemented on separated drawing sheets.

Identifier	47
Title	pull-up resistor impedance
Clue type	component-only
Item	buffer+driver
Clue Text	Is the pull-up resistor value low compared with the high impedance value of the line/bus?

Explanation: If the pull-up resistor value is high or close to the high impedance value of the line/bus, the tri-state outputs connected to the line/bus may be polarized to a middle voltage value during the high impedance state of the bus and it may lead to a short circuit, especially for CMOS devices. The pull-up resistor value shall be lower than one tenth of the high impedance value of the line/bus.

Identifier	47A
Title	pull-up resistor impedance
Clue type	component-only
Item	buffer+driver
Clue Text	Is the pull-up resistor value low compared with the high impedance value of the line/bus?

Explanation: If the pull-up resistor value is high or close to the high impedance value of the line/bus, the tri-state outputs connected to the line/bus may be polarized to a middle voltage value during the high impedance state of the bus and it may lead to a short circuit, especially for CMOS devices. The pull-up resistor value shall be lower than one tenth of the high impedance value of the line/bus.

Identifier	50
Title	decoupling capacitor values
Clue type	component-only
Item	IC+and+nand+or+nor+not+JK+RS+flipflop+register+latch
Clue Text	Has a decoupling capacitor been provided?

Explanation: The high processing frequency of the logic circuits leads to current spikes and then to voltage spikes because of the inductive coupling between conductors at high frequency. Only a decoupling capacitor close to the power pins can prevent the spikes from propagating to the other circuits.

Identifier	51
Title	timing compatibility
Clue type	component-only
Item	IC+and+nand+or+nor+not+JK+RS+flipflop+register+latch
Clue Text	Is the timing compatibility between circuits respected?

Explanation: This problem is likely to occur between circuits of different families or when an analogue output is connected to a digital input. If one of the specified parameters cannot be guaranteed, it can lead to a sneak timing. For CMOS digital circuits, rise and fall time shall not exceed 15 microseconds; otherwise, an erroneous output can be generated, and power dissipation increases.

Identifier	52
Title	energy storage/release
Clue type	path-component component-only
Item	capacitor
Clue Text	Can the energy stored by the component be released without damage?

Explanation: As capacitors may retain stored charge once the power is removed, capacitors can lead to latch up, destroy sensitive cir-

cuits, delay the power off of the function or create sneak current paths. A discharge circuit (bleed resistor in parallel with a high value capacitor) may be provided to drain away the charge after the circuit is switched off.
The system or circuit shall be designed such that the connection between the capacitor and its bleed resistor cannot be broken except during repair.
When a circuit output connected to a capacitor changes state (digital circuit), the capacitor may generate an unexpected voltage spike, dangerous for the components receiving this spike.
A capacitor may keep circuit inputs powered while the circuit is not powered. This can induce sneak current paths through internal circuits protection diodes,resistors, transistors, ...

Identifier	52A
Title	energy storage/release
Clue type	path-component component-only
Item	inductor+coil+relay+transformer+motor+trafo
Clue Text	Can the energy stored by the component be released without causing damage?

Explanation: A magnetic field is the energy source that can produce large voltage transients when it collapses, particularly when an equipment is shut down or switched to standby.

Identifier	52B
Title	lack of surge resistor
Clue type	path-component component-only
Item	capacitor
Clue Text	No surge resistor to protect an IC?

Explanation: Integrated circuits should be protected against large capacitances connected to their input by placing a resistor in series.

Identifier	52C
Title	diode prevents energy release
Clue type	path-component component-only
Item	capacitor
Clue Text	Can a diode prevent energy release from the component?

Explanation: If a diode is connected in series with a capacitor (to protect it against reverse voltage perhaps), check that it does not prevent the capacitor from releasing its energy.

Identifier	53
Title	activation by leakage current
Clue type	path-component component-only
Item	diode+resistor+transistor+gate+and+or+nand+nor+capacitor
Clue Text	Can the leakage current of the component activate or inhibit digital devices and lead to (un)expected functions or loss of function?

Explanation: For instance, during unusual operating modes, the relay coil may be fed from a low voltage or a high impedance source and can lead to a sneak current path. Sensitive amplifiers, FETs, and high input impedance devices are particularly susceptible to problems.

Identifier	54
Title	acceptable charge/discharge current
Clue type	component-only
Item	capacitor
Clue Text	Is the charge/discharge current flowing through the capacitor within the specified rating of the capacitor and other involved components to which it is connected?

Explanation: Depending on the capacitor technology, the current flowing through the capacitor shall not exceed a specified value. As this current may reach high intensity, its influence on other items (fuses, transistor, voltage spikes,...) shall be carefully studied in order to respect the appropriate ratings.

Identifier	54A
Title	high switching current for tantalum capacitors
Clue type	component-only
Item	capacitor
Clue Text	Is there a possibility for a high switching current, and is the capacitor a tantalum type?

Explanation: For polarized solid tantalum capacitors, the charge and the discharge current flowing through the capacitor should be limited under 0.1 Ω/V (a resistor can be used to limit the current). Current through ceramic capacitors should not exceed 50mA.

Identifier	55
Title	voltage delay during power transition
Clue type	component-only
Item	capacitor
Clue Text	Are different capacitor charge and discharge times within a circuit acceptable?

Explanation: If some capacitors reach operating voltage before others, the designer shall ensure that it will not lead to an unexpected current path or a temporary wrong processing of a function.

Identifier	55A
Title	capacitor used as status indicator
Clue type	component-only
Item	capacitor
Clue Text	Is a capacitor voltage used to feed a status indicator or sensor?

Explanation: If a capacitor voltage is used (directly or not) as a status information by a monitoring circuit, the capacity may induce a delay in monitoring.

Identifier	56
Title	protection against reverse voltage
Clue type	component-only
Item	inductor+coil+relay+transformer+motor
Clue Text	Is the overvoltage generated when switching a winding suppressed?

Explanation: If the current drift/direction changes or if the current is switched off in inductors, coils or transformers, an unlimited reverse voltage is generated, with possible oscillations. This reverse overvoltage is likely to destroy any sensitive components located nearby.
To suppress this overvoltage, a diode (with a reverse coupled Zener diode in series) is usually implemented in parallel as a protection. The Zener diode increases the forward resistance of the diode in order to lower the oscillation time constant. Without Zener diode, the time constant is increased by a factor of 5 to 10, and the reverse voltage burn-out of the diode shall be carefully considered.

Identifier	56A
Title	protection against reverse voltage
Clue type	component-only
Item	inductor+coil+relay+transformer+motor
Clue Text	Is the overvoltage generated when switching a winding suppressed?

Explanation: If the current drift/direction changes or if the current is switched off in inductors, coils or transformers, an unlimited reverse voltage is generated, with possible oscillations. This reverse overvoltage is likely to destroy any sensitive components located nearby.
To suppress this overvoltage, a diode (with a reverse coupled Zener diode in series) is usually implemented in parallel as a protection. The Zener diode increases the forward resistance of the diode in order to lower the oscillation time constant. Without Zener diode, the time constant is increased by a factor of 5

to 10, and the reverse voltage burn-out of the diode shall be carefully considered.

Identifier	57
Title	correct signal for mode
Clue type	path-component
Item	switch+capacitor+battery+power+supply
Clue Text	Does the signal remain within its expected voltage range for the expected switching conditions?

Explanation: During particular phases (e.g. testing) or change of modes, some switching combinations may be activated with a sequence or order quite different from that expected by the designer. Then, the signal may:
1) exceed (positive or negative) the voltage supply of a circuit dealing with this signal, leading to a sneak current path or an erroneous processing (operational amplifier, comparator, digital circuit, transistor)
2) remain within a medium voltage range unacceptable for the circuit (digital circuit, MOSFET,...)
3) remain floating, indeterminate
4) simply activate the wrong function(s) for this mode. Reference signal or polarization signals shall be checked as well. Normally, bias conditions should not be dependent to circuit configuration and switching modes, except after particular and careful study. The collector junction of a bipolar transistor shall not be inadvertently forward biased under some switching, operational or testing modes.

Identifier	58
Title	fan out/fan in rating
Clue type	component-only
Item	IC+and+or+nand+nor+not+RS+JK+flipflop+register+latch+buffer+active+EED
Clue Text	Does the component loading remain within the specified ratings?

Explanation: The common assumption that a TTL device can drive ten devices is not always true. Fan-out limits should be calculated by summing input current requirements and comparing with the output source current

Identifier	10B
Title	spike on the initialization signal
Clue type	component-only
Item	digital+IC+and+nand+or+nor+not+gate+RS+JK+flipflop+register+latch+tristate
Clue Text	Can a spike occur on the initialization signal?

Explanation: The initialization signal shall be protected against spikes to prevent spurious initialization of the equipment.

Identifier	13
Title	transient current through a relay contact
Clue type	component-only
Item	relay+contact
Clue Text	Is an unregulated flow of current through the relay contacts acceptable?

Explanation: During power transition or switching for instance, high inrush current may occur when capacitive loads are switched. The relay shall be operated within the manufacturer's specified ratings.

Identifier	58AA
Title	load rating
Clue type	component-only
Item	IC+and+or+nand+nor+not+RS+JK+flipflop+register+latch+buffer+active+EED
Clue Text	Does the component load remain within the specified ratings?

Explanation: Is the fan out rating exceeded.

Identifier	58A
Title	load ratings
Clue type	component-only
Item	flipflop+register+latch+buffer+OpAmp+IC
Clue Text	Are load ratings exceeded during abnormal or unusual operational states?

Explanation: During unscheduled sequences and modes (e.g. testing) or switching, a load with an impedance lower than expected or with different characteristics (inductive instead of resistive) can lead to permanent failure or a sneak current path with potential hazards.
Particular attention should be paid to integrated circuits (e.g. OpAmp, comparator) or semiconductors connected to capacitors; during power transition for instance, if a capacitor is used as a feedback with an OpAmp/comparator, the drive capability of the OpAmp/comparator output may be exceeded. The same is true if the capacitor is connected from input to ground, or from output to ground. To provide a series limiting resistance is a solution in some cases.

Identifier	58AAA
Title	load ratings
Clue type	component-only
Item	flipflop+register+latch+buffer+OpAmp+IC
Clue Text	Are load ratings exceeded during abnormal or unusual operational states?

Explanation: During unscheduled sequences and modes (testing, ...) or switching, a load with an impedance lower than expected or with different characteristics (inductive instead of resistive) can lead to the circuit destruction or a sneak current path, with potential hazards.
Particular attention should be paid to integrated circuits (OpAmp, comparator,...) or semiconductors connected to capacitors; during power transition for instance, if a capacitor is used as a feedback with an OpAmp/comparator, the drive capability of the OpAmp/comparator output may be exceeded. The same is true if the capacitor is connected from input to ground, or from output to ground. To provide a series limiting resistance is a solution in some cases.

Identifier	58B
Title	load ratings for EED
Clue type	component-only
Item	active+EED
Clue Text	Can the circuit supply sufficient energy to blow the EED under all operational conditions?

Explanation: For a squib component, sufficient energy shall be delivered by the output to blow it. For some switching conditions, there may be too much resistance or inductance in the activating circuit.

Identifier	59
Title	internal unexpected link of ICs pins
Clue type	once-only
Item	IC+path+JK+buffer+RS+flipflop+register+counter
Clue Text	Has a possible internal link of ICs pins been taken into account for the design?

Explanation: An unexpected internal link between pins of an integrated circuit can lead to a circuit malfunction or a sneak current path.

Identifier	60
Title	low voltage drift with time
Clue type	once-only
Item	capacitor
Clue Text	Have appropriate capacitors been used when a circuit needs a low voltage drift with time?

Explanation: For instance, for sample & hold amplifiers with low voltage drift with time, teflon, polyethylene or polycarbonate capacitors are the best suited.

Identifier	61
Title	temperature stability problems
Clue type	once-only
Item	capacitor
Clue Text	Is an appropriate capacitor type used if the circuit needs a good temperature stability?

Explanation: For instance, for low passing active filter needing a good temperature stability, silvered mica capacitors are the best suited.

Identifier	62
Title	balanced pair of transistors
Clue type	component-only
Item	transistor+PNP+NPN
Clue Text	If there are differential instrumentation entrance or push-pull output stage made with transistors, are the transistors perfectly balanced?

Explanation: The transistors shall be balanced to avoid saturation or clamping.

Identifier	63
Title	connected tristate outputs enabled
Clue type	component-only
Item	buffer+driver
Clue Text	Can connected tristate outputs be enabled at the same time?

Explanation: On multi-user line/bus, only one user provide an output to the line; otherwise, if two users provide simultaneous outputs, erroneous information may be transmitted and a short circuit may also occur.
Tying totem-pole outputs together may cause a power-to-ground short-circuit, if one output drives a “1” logic level and another a “0” logic level.

Identifier	65
Title	correct state during initialization
Clue type	component-only
Item	breaker+relay+switch
Clue Text	During power on or initialization, is the component in a correct predefined state?

Explanation: During initialization, the relay state shall be clearly established.

Identifier	65A
Title	correct state during initialization
Clue type	component-only
Item	transistor
Clue Text	During power on or initialization, is the component in a correct, predefined state?

Explanation: During initialization, high impedance outputs shall have appropriate polarization resistors: e.g. not to bias a NPN base.

Identifier	20D
Title	switching item dedicated to a function
Clue type	component-only
Item	switch+contact+breaker
Clue Text	When a protective device is activated, are other functions than those expected affected?

Explanation: With elaborate equipments, some combinations may lead to unexpected behaviour of functions or inhibition of functions.

Identifier	21
Title	saturated or clipped signal
Clue type	component-only
Item	OpAmp+amplifier+transistor
Clue Text	Can an output signal be saturated or clipped?

Explanation: For instance, with an integrator, the saturation of the feedback capacitor induces a saturated signal and an erroneous output signal.
When amplifiers are used (OpAmp, transistor), if the gain is not correctly adjusted, the output signal may be saturated. If the amplifier polarization is not symmetrical, the output signal may saturate asymmetrically.

Identifier	21A
Title	saturated or clipped signal input
Clue type	component-only
Item	OpAmp+amplifier+transistor
Clue Text	Can an input signal be saturated or clipped?

Explanation: For instance, with an integrator, the saturation of the feedback capacitor induces a saturated signal and an erroneous output signal.

Identifier	22
Title	self-healing of plastic film capacitors
Clue type	component-only
Item	capacitor
Clue Text	Is there enough energy in the capacitor for self healing?

Explanation: Recommended minimum energy for self-healing is about 500μJ.

Identifier	65B
Title	correct state during initialization
Clue type	component-only
Item	IC+latch+flipflop
Clue Text	During power on or initialization, is each item/circuit in a correct predefined state?

Explanation: During initialization, latch/register inputs shall have appropriate polarization resistors in order to retain the correct logic state when the initialization phase is completed and the computer has still not accessed to the latch/register, or they shall be initialised dynamically.

Identifier	66
Title	correct initialization time
Clue type	component-only
Item	JK+RS+latch+register+counter+flipflop+and+RAM+ROM+micro pro
Clue Text	Is the initialization time long enough to be compatible with each component signal specification and the longest transition time of the power sources?

Explanation: Some circuit pins need a minimum initialization time (RESET, CLEAR, SET,...). A too short initialization time may not correctly reset a microcontroller or a register state ; it may enable outputs which are connected to circuits not still nominally powered.

Identifier	66A
Title	correct power settling time
Clue type	component-only
Item	JK+RS+latch+register+counter+flipflop+and+RAM+ROM+micro pro
Clue Text	Is the initialization time long enough to be compatible with the settling time of the power supply?

Explanation: The initialization signal (RESET, CLEAR, SET,...) needs to be held until the power supply level is steady at all parts of the circuit. A too short initialization time may not correctly reset a

microcontroller or a register state ; it may enable outputs which are connected to circuits not still nominally powered.

Identifier	67
Title	switching item shared by several function
Clue type	path-component component-only
Item	switch+contact+relay+and+gate+breaker
Clue Text	Is a change of state of a switching item for one function acceptable for correct performance off other functions?

Explanation: A switching item can be shared through a same contact, or through multiple contacts activated at the same time.
If a circuit-breaker is triggered, its change of state will affect all the functions connected to it. Check that it does not steal power from a function that should still be powered.

Identifier	19A
Title	sufficient available power
Clue type	component-only
Item	transformer+power+supply+battery
Clue Text	Can the power source meet the maximum demand?

Explanation: Under some particular conditions (e.g. test, reconfiguration), more power than expected may be consumed by the loads:

- in the case where multiple loads are to be supplied, an unfavourable combination of loads may exceed the capability of the power supply
- a load may draw much more power than normal under anomalous circumstances (resistive torque on a motor). If the power equipment contains a current limiter, the power source shall also be able to support the activation of the current limiter, specially if the source is shared by other equipments.

Identifier	69
Title	false indication during switching
Clue type	component-only
Item	relay+switch+breaker+button
Clue Text	During switching, can a false indication occur or an unintended function be activated?

Explanation: If the contact “chatters” or “bounces” during switching, the signal may be detected as multiple inputs. Using an electronic switch (such as a transistor) instead of a relay may provide a solution.
If a monitoring circuit checks a relay status just after the relay has changed of state, erroneous information may be transmitted as the relay contacts can rebound for a short time after switching. A delay in the status acquisition is necessary to monitor a stable status.
A capacitance filter or a monostable circuit may be fitted to produce a reliable deterministic switching signal.

Identifier	70
Title	label ambiguity
Clue type	component-only
Item	label+lamp+indicator
Clue Text	Have each electrical indicator, command and signal its own unique label?

Explanation: To allow an easier management of the electrical drawing and sneak label detection, each signal and connection shall have its own unique label.
Labelling shall be precise : for instance, the wires attached to either side of a fuse shall have different labels.
Quasi-similar labels for independent indicators, commands and signals shall be avoided.

Identifier	71
Title	unterminated leads
Clue type	component-only
Item	electric+electromechanical+electronic
Clue Text	Are there any open ended or nonterminated outputs?

Explanation: In a circuit each extremity of a wire shall normally be connected to a component. If a lead is connected to a flag that makes it available for another sheet of the drawing, the lead shall continue on the new sheet under the same label.

Identifier	71A
Title	unconnected leads due to switching
Clue type	component-only
Item	IC+OpAmp+JK+RS+flipflop+component
Clue Text	Is there any open ended or nonterminated outputs for some switching state?

Explanation: Component terminal wires shall be connected in all switch states.

Identifier	72
Title	consistent labelling
Clue type	component-only
Item	label+indicator+lamp+speaker
Clue Text	Is the label wording consistent with others labels?

Explanation: The wording labels should have uniform style, be unique, and identifiable. As a suggestion, the master equipment which delivers the signal can be used as a common root for the label wording.

Identifier	73
Title	exhaustive labelling
Clue type	component-only
Item	label+lamp+indicator+speaker
Clue Text	Are all the circuit applications clearly indicated in a label name?

Explanation: To allow an easier management of the electrical drawing and sneak label detection, each indicator, command and signal shall be clearly labelled to indicate all of its functions.
For instance, if a switch is on a ground return of several loads (Y pattern or power dome configuration), its command label shall indicate all of the loads affected.

Identifier	74B
Title	independence of timing of switching functions
Clue type	path-component component-only
Item	switch+button+relay+gate+and
Clue Text	Is independent timing of switching items justified?

Explanation: When multiple switches shall be activated, if a confusion in the activation order can have critical impacts, then the temporal independence between these switches shall be suppressed, or safety barriers shall be added.
If several switches shall be activated at the same moment (to cut off of the 3 phases of the main power for instance), these switches should be activated by the same command or signal.

Identifier	75
Title	coherent labelling of inter-board leads
Clue type	component-only
Item	label+connector
Clue Text	Is an interface label used on separated boards the same on all boards?

Explanation: If the labels are different, there may be problems during the routing on the board ; signals may not be connected together.

Identifier	76
Title	uniform logic conventions
Clue type	component-only
Item	lamp+switch+button
Clue Text	Do the indications provided by all the monitoring circuits following the same common logic conventions?

Explanation: Usually, the level “1” corresponds to “power presence” and the level “0” to “lack of power”. A red lamp lights up for a problem and a green lamp indicated that the monitored function is OK.

Identifier	77
Title	impedance matching
Clue type	component-only
Item	buffer+amplifier+driver
Clue Text	Are interface lines terminated correctly?

Explanation: If the rise time of a digital signal is short compared with the propagation time of the signal (on a long line or through an interface), signal reflections may induce parasite voltages and erroneous information.

Identifier	78
Title	truth table for digital function
Clue type	component-only
Item	IC+and+or+nand+nor+not+ASIC+PLA
Clue Text	Has each state of a truth table for a digital function been checked?

Explanation: The truth table allows an exhaustive check of every possible input state.

Identifier	81
Title	undesired state inhibition
Clue type	component-only
Item	IC+flipflop+JK+RS+register+latch+counter
Clue Text	Is the change of the component to an undesired state inhibited?

Explanation: For instance, resetting a counter may be undesired due to its effects on the equipment: consequently, the counter reset shall be inhibited and additional circuits may be necessary to prevent the counter from passing by the “0” state when counting.

Identifier	1
Title	simultaneous activation of mutually exclusive inputs
Clue type	component-only
Item	bistable+flip-flop+register+latch+counter+JK+RS+bistabrel
Clue Text	Can mutually exclusive commands (STOP/START & RESET/SET) be generated at the same time?

Explanation: The RESET/SET & STOP/START shall not occur at the same time otherwise the item state will be undetermined.

Identifier	2
Title	transient current through a fuse or breaker
Clue type	component-only
Item	fuse+breaker
Clue Text	Is a transient current flowing through a fuse (a breaker) within specified limits?

Explanation: A fuse shall withstand without rapturing the high transient currents which may occur during power switching or during a power transition. The fuse should be chosen in accordance with the manufacturer's recommendations.

Identifier	3A
Title	saturation detection
Clue type	component-only
Item	sensor+fsens+psens+tsens+vsens
Clue Text	Is there an out-of-limits or saturation detection circuit?

Explanation: The sensors should be selected in such a way that the detection circuit ensures detection of the out-of-limits or saturation in the system.

Identifier	15A
Title	discharge circuit for a power-source
Clue type	path-component component-only
Item	power+battery+supply
Clue Text	Is the power source provided with a circuit that can isolate it from its load?

Explanation: For safety reasons and to avoid sneak current paths at interface between circuits with different supplies, once an equipment has been switched off, the power source shall be prevented from continuing to supply power.

Identifier	16
Title	stray capacitance
Clue type	component-only
Item	IC+and+or+nand+nor+not+flipflop+JK+RS+register+latch
Clue Text	Are circuits using capacitors at pF levels sensitive to the capacitor tolerance?

Explanation: When the circuit is to be implemented on a PCB, the parasitic capacitance of the PCB tracks may alter the proper functioning of the circuit. The input capacitance of circuits may also induce parasitic capacitance. Parasitic capacitance may cause delay in functioning, failure to switch, poor signal form, oscillation.

Identifier	165
Title	secondary load viewed from the transformer primary
Clue type	component-only
Item	transformer
Clue Text	Is the secondary load viewed from the transformer primary acceptable?

Explanation: To determine the load seen by the transformer primary, the transformation ratio shall be taken into account.
If a capacitor is connected in parallel with a secondary winding of a transformer (filter in a direct current converter), during power on, the capacitor charging induces a "short circuit" at the transformer primary: a current limiter may be implemented to cancel this problem.

Identifier	166
Title	energy received by an indicator
Clue type	component-only
Item	lamp+LED+loudspeaker+speaker+buzzer+bell
Clue Text	Is the energy received by the indicator correct?

Explanation: If a low current flows through a lamp or LED, the indicator may not be seen if lights up, depending of the room brightness. An audible alarm (loud-speaker, buzzer) shall have enough power available for the transducer, especially if it is placed in a noisy room. This may have critical effects if it is an alarm indicator!

On the other hand, a limitation resistor may sometimes be implemented (LED).

Identifier	167
Title	command duration adapted to circuit characteristics
Clue type	component-only
Item	relay+flipflop+JK+RS+register+monoflop
Clue Text	Is the command duration matched to the circuit characteristic?

Explanation: For monostable relays, the command shall be maintained as long as the change of state is desired. For bistable relays, once the state has changed, the command is no longer needed; but to change state of bistable relay, a minimum duration command is necessary to reach a sufficient magnetic field on the coil.

Identifier	168
Title	current limiters in series
Clue type	component-only
Item	limiter+fuse+relay+breaker
Clue Text	Are current limiters in series correctly set?

Explanation: Both the maximum current limit and the reaction delay shall be considered. Normally, down-stream current limiter shall first react before other up-stream current limiters.

Identifier	82
Title	multiple paths of a signal
Clue type	path-component component-only
Item	connector+malecon+femcon
Clue Text	Does the same signal flow through separated lines or connectors?

Explanation: This arrangement shall be avoided as the separated wires of the signal can recombine through other boards and it can lead to sneak current paths. Also, low current and high current returns connected in parallel shall be avoided in case of the high current disconnection.

Identifier	82A
Title	multiple earth returns for a signal
Clue type	path-component component-only
Item	earth+chassis
Clue Text	Is there an earth return flow through separated lines or connectors?

Explanation: This arrangement shall be avoided as the separated wires in the earth return can lead to inductance effects, conduction path overload, and errors during disconnection.

Identifier	82AA
Title	multiple earth returns for a signal
Clue type	path-component component-only
Item	earth+chassis
Clue Text	Is there an earth return flow through separated lines or connectors?

Explanation: This arrangement shall be avoided as the separated wires in the earth return can lead to inductance effects, conduction path overload, and errors during disconnection.

Identifier	82B
Title	connector in earth return line
Clue type	path-component component-only
Item	connector+malecon+femalecon
Clue Text	Is there a connector in the earth return line, and a parallel path which bypasses it?

Explanation: This arrangement shall be avoided as the parallel earth return can cause a sneak timing or a sneak circuit.

Identifier	82BB
Title	connector in earth return line
Clue type	path-component component-only
Item	earth+chassis+ground
Clue Text	Is there a connector in the earth return line, and a parallel path which bypasses it?

Explanation: This arrangement shall be avoided as the parallel earth return can cause a sneak timing or a sneak circuit.

Identifier	83
Title	signal on a power line
Clue type	path-component component-only
Item	and+or+nand+nor+gate+flipflop+RS+JK+register+amplifier+ transistor+comparator
Clue Text	Is the signal perturbation due to the power line acceptable?

Explanation: Spikes occurring on a power line can generate high frequency interference which can alter signal characteristics. The potential difference due to the interference current flowing through the line may not be negligible compared to the signal.

Identifier	84A
Title	power and signal lines in separated connectors
Clue type	component-only
Item	multiconnector
Clue Text	Does the connector contain both power and signal lines?

Explanation: It is necessary to route signal and power lines through separate connectors. It can lead to the complete destruction of the equipment if a short circuit between a signal and a power line occurs. The electromagnetic interferences may induce random/false data on digital signals and modify an analogue signal characteristic.

Identifier	84B
Title	disconnecting separated connectors
Clue type	component-only
Item	multiconnector+connector+interlock+malecon+femalecon
Clue Text	Is it possible to disconnect power lines in separated connectors?

Explanation: Opening just one connector from a set of power and earth or return connectors is a frequent cause of sneaks.

Identifier	86A
Title	irreversible state after switching
Clue type	path-component component-only
Item	relay+and+nor+flipflop
Clue Text	Can switching lead to an irreversible state?

Explanation: For instance, the command circuit of a relay may be powered through the relay; once the relay has been activated, the command circuit is no more powered and can no longer be activated, so the relay remains in an irreversible state. A relay contact or gate on a single path branch shall not be commanded by a circuit supplied through another branch: once the relay contact is open, the command circuit of the relay is no more supplied and the relay contact can never be closed.

Identifier	89
Title	decoupling capacitor for each board
Clue type	component-only
Item	supply+battery+power
Clue Text	Has a decoupling capacitor been provided for each direct current power signal at the entrance of each board?

Explanation: Install a decoupling capacitor for each power line at the point where it enters each board to ensure a "clean" power supply free of spikes (μF) and radio-frequency parasites (nF).

Identifier	89A
Title	decoupling capacitor for each board
Clue type	component-only
Item	connector+multiconnector+malecon+femcon
Clue Text	Has a decoupling capacitor been provided for each direct current power signal at the entrance of each board?

Explanation: To install a decoupling capacitor for each power signal at the point where it enters each board ensure a "clean" power supply free of spikes (μF) and radio-frequency (nF).

Identifier	92
Title	quality of the contact material
Clue type	once-only
Item	relay+switch+interlock+contact+button
Clue Text	Is the contact material correctly chosen with respect to the signal characteristics and the relay application?

Explanation: For low loads (e.g., 1 mA, 5 V) gold plated contacts are required.
For very low loads (e.g. a few μA, 1 Volt), use gold or silver/gold contacts (e.g. thermo-couple switching).
For repetitive functioning, use silver/cadmium contacts.

Identifier	93
Title	contacts and inductive load switching
Clue type	component-only
Item	switch+contact+breaker
Clue Text	Are the contacts protected against high voltage spikes?

Explanation: If the load seen by the contacts is inductive, a resistor with a capacitor in series or a voltage suppression diode can be added in parallel to the relay contacts; but magnetic blowing relays or high cut distance relays are preferable.

Identifier	98
Title	low impedance between power sources
Clue type	path-component component-only
Item	power+supply+battery
Clue Text	Can a low impedance tie two power sources?

Explanation: Under some switching conditions, a low impedance load may be connected between two power sources and create a short circuit: relay-coil, inductor, motor, transformer, diode, wire, ...

Identifier	99
Title	temperature limit for multi layer tantalum capacitors
Clue type	once-only
Item	capacitor
Clue Text	Can the temperature of a multi layer tantalum capacitor exceed 38 C?

Explanation: The anode wire of multi-layer tantalum capacitors intersects when temperature is above 38 C.

Identifier	100
Title	reverse voltage on a polarized capacitor
Clue type	component-only
Item	capacitor
Clue Text	Can a reverse voltage be applied to the polarized capacitor?

Explanation: If a reverse voltage is applied to a polarized capacitor, the capacitor will burst. A protection diode against reverse voltage in parallel with the capacitor can be added.

Identifier	101
Title	capacitive feedback between an amplifier's input and output
Clue type	component-only
Item	OpAmp+amplifier
Clue Text	For an amplifier with a capacitive feedback, does the amplifier output remain stable?

Explanation: Capacitive feedback between the input and the output of an OpAmp can lead to instability in an unexpected frequency range. These oscillations may superpose upon the nominal signal and induce an erroneous processing.

Identifier	102
Title	compensation of amplifier input capacitance
Clue type	component-only
Item	OpAmp+transistor+amplifier
Clue Text	Has the amplifier input capacitance been compensated?

Explanation: Capacitive feedback compensates for input capacitance of an OpAmp or a transistor (FET), but also increases the risk of instability. A check is necessary to prevent this risk.

Identifier	103
Title	hysteresis for noise immunity
Clue type	component-only
Item	comparator+OpAmp
Clue Text	Has hysteresis been implemented to improve noise immunity?

Explanation: For a comparator, an hysteresis can be implemented by positive feedback (usually a resistor) between the output and the non-inverting input. If no hysteresis is implemented, depending of the signal noise at the inputs, the output may "bounce" during the change of state.

Identifier	104
Title	adjustment of input impedance
Clue type	component-only
Item	OpAmp+transistor+amplifier
Clue Text	Has the input impedance been adjusted?

Explanation: For instance, to compensate the input offset errors of an amplifier, equalizing input resistors shall be implemented to allow adjustment. If the offset has an effect on the correct circuit processing, these input resistors are imperative. Voltage converters or current converters made with OpAmps should have a resistor on the non-inverting input adjusted with the feedback resistor.

If the feedback is made via a complex network, a complex network should also be provided on the input impedance.

Identifier	105
Title	commutation time of transistor
Clue type	component-only
Item	transistor
Clue Text	Are the turn-on and turn-off times for the transistor low compared with the stable state time?

Explanation: During a commutation in a (power) transistor, the power dissipation partly comes from the switching times, as both voltage and current are applied to the transistor during the switching. To improve the efficiency, turn-on and turn-off times shall be as small as possible: use commutation accelerators. To reduce the switching times also allows to lower the transistor case temperature.

Identifier	109
Title	plug
Clue type	path-component component-only
Item	latch+register+flip-flop+monoflop+bistable+JK+RS+counter+transistor+rectifier+breaker+limiter+relay+monostable+switch+contact+button+fuse+interlock
Clue Text	Can switching lead to an unstable state?

Explanation: Feedback around a loop of digital components can lead to instability if the number of signal reversals is zero or even.

Identifier	109A
Title	unstable or irreversible state
Clue type	path-component component-only
Item	relay
Clue Text	Can a switching lead to an unstable/irreversible state?

Explanation: The switching of a relay can activate an unwanted series of events in which another relay changes of state and subsequently activates the first one.
If the relays are monostable, this situation leads to an unstable state. If one relay is bistable, the switching leads to an irreversible state.

Identifier	110
Title	continuous current path via an autotransformer
Clue type	path-component component-only
Item	autotransfo
Clue Text	Can an unexpected continuous current flow through the autotransformer?

Explanation: An autotransformer has no galvanic isolation between input and output. A continuous current can flow through the windings and create an unexpected/sneak current path.

Identifier	111
Title	parallel diodes for redundancy/power sharing
Clue type	component-only
Item	diode
Clue Text	Is the current flowing through parallel diodes equally divided or does it flow only through one diode?

Explanation:
- Either one diode can carry all the current itself and the other diode is for redundancy: then no current should (not obligatory) flow through the second diode to improve its life time as a "cold" redundancy.
- Or one diode cannot carry all the current itself and the current shall be shared with the other diode: half the current flowing through the two diodes and then a balance device shall be implemented as the two diodes will not have the same diode voltage. One shall insure that unequal division will not occur.

Identifier	112
Title	correct biasing of Zener diodes
Clue type	component-only
Item	Zener
Clue Text	Is the Zener diode correctly biased?

Explanation: When a Zener diode is used as voltage reference it shall conduct a sufficiently large current to ensure that it operates in the breakdown region of its characteristic sufficiently far from the "knee". This ensures a stable reference voltage. However, the power dissipated in the Zener diode should not exceed the maximum permitted value.

Identifier	113
Title	inductance of a wire wound resistor
Clue type	component-only
Item	resistor
Clue Text	Has the inductive effect of the wound wire resistor been taken into account?

Explanation: For a quasi direct current signal, the inductance should have negligible effect. At high frequencies, the inductance will not be negligible and will add to the impedance of the resistor, possibly leading to unexpected results.

Identifier	115A
Title	connected power sources
Clue type	path-component component-only
Item	power+supply+battery
Clue Text	Is it acceptable to connect one reference voltage of the power source to a reference voltage of an other power source?

Explanation: Some power sources may be separated by galvanic isolation. To connect these power sources (power-to-power or ground-to-ground) may undo the benefit of galvanic isolation. It can also create unexpected high current paths as the reference point of each power source may not have exactly the same voltage.

Identifier	5B
Title	maximum signal frequency
Clue type	component-only
Item	IC+gate+and+or+nand+nor+not
Clue Text	Have the maximum signal frequency been taken into account?

Explanation: There may be problems of low output signal levels if the expected signal frequency is close to the component maximum frequency limit.

Identifier	7B
Title	location of the protection device
Clue type	component-only
Item	load
Clue Text	Are the protection devices missing?

Explanation: When a signal or input is distributed to circuits, the first component attached to the input line shall be a protective device in order to protect the input against a short circuit on the component.

Identifier	116
Title	correct signal attachment on drawing
Clue type	component-only
Item	signal+connector+label+offpage
Clue Text	Is each circuit using the right signal on its inputs and delivering the right signal at the correct output?

Explanation: – As a system is usually documented on several drawings, flags are used to identify corresponding signal lines on the various drawing.

- When using a register to latch the data of a bus (for instance), the input <i> of the latch shall deliver on the corresponding output a signal with the same number <i>.
- Sometimes, labels seem to be at the correct place on the drawing, but within computer, labels may be mis-attached.
- In case of hierarchical design, the flags of a level shall be coherent with the flags of the upper and lower level

Identifier	117A
Title	one path for separate power returns
Clue type	component-only
Item	earth+ground+chassis
Clue Text	Are independent power supplies sharing a current return path or chassis return?

Explanation: The return lines for digital and low-level analogue signals shall be kept separate. Spikes due to digital circuits will not then propagate to analogue circuits through a common power line. High inrush currents due to power switching will not affect the voltage stability of other sensitive circuits.

Identifier	117B
Title	one earth path for separate power source
Clue type	component-only
Item	earth+chassis
Clue Text	Are separate power source lines mixed?

Explanation: Independent power supplies should not share a common line/conductor to supply their loads.
The return lines for digital and low-level analogue signals shall be kept separate. Spikes due to digital circuits will not then propagate to analogue circuits through a common power line. High inrush currents due to power switching will not affect the voltage stability of other sensitive circuits.
Usually, CAD provides the designer with a "star" component. It allows several separate signals with different labels to be created from a single signal. It shall be used to distribute a power source with a star net.

Identifier	117D
Title	one path for separate signal returns
Clue type	component-only
Item	earth+ground+chassis
Clue Text	Is a single earth return long or high resistance?

Explanation: Independent signal return paths should be kept separate, to avoid cross talk until they reach a common low resistance earth point. Cross talk can in some cases lead to feedback oscillations.

Identifier	119A
Title	monitoring circuit independent of monitored function
Clue type	component-only
Item	sensor+psens+fsens+tsens+lsens
Clue Text	Does the monitoring circuit depend upon the function it monitors?

Explanation: A failure of the monitored circuit shall not prevent the monitoring circuit from operating correctly: for instance through a common power source if the monitored function is shorted. The monitoring circuit should not depend on the monitored function for its proper functioning. On the other hand, means shall be provided to detect a failure of the monitoring circuit.

Identifier	121
Title	ICs needing external component
Clue type	component-only
Item	IC+gate+and+or+nand+nor+not+buffer+clock+JK+RS+flipflop+register+driver+counter
Clue Text	For ICs needing an external component, has the appropriate component been implemented?

Explanation: Some TTL outputs are “open -collector”: A pull-up resistor shall be added between the output (transistor collector) and + VCC. Some TTL outputs are also sometimes “open emitter”: a pull-down resistor then shall be added. The value of the resistor depends of the load to drive.
Tristate outputs also require a pull-up or pull-down resistor.
A transistor base-driven by an open collector transistor should also have a pull-up/down resistor to assure proper switching.
If an open collector TTL output drives a CMOS input, a pull-up resistor shall be added.

Identifier	122
Title	noise compatible with device noise immunity
Clue type	component-only
Item	IC
Clue Text	Is the signal noise acceptable for the circuit dealing with this signal?

Explanation: When a signal contains extraneous noise, its upper and lower bounds may exceed specified limits, making the signal unacceptable.
To increase the noise immunity of a receiver, Schmitt trigger gates may be used on inputs. On the same principle, a hysteresis cycle may be implemented in comparators. In any case, a noise margin should always be maintained.

Identifier	123
Title	internally unsuppressed pins
Clue type	component-only
Item	IC
Clue Text	For ICs with internally unsuppressed pins, has a suppression device been implemented?

Explanation: Some integrated circuits do not have internal protection diodes fitted to the inputs and outputs. These integrated circuits are vulnerable to transient voltages which may exceed maximum permitted limits causing latch-up or even permanent damages.
External protection devices (diodes, resistors in series, ...) shall be attached to pins with such "dangerous" signals.

Identifier	124
Title	load characteristic after use
Clue type	path-component component-only
Item	EED+squib+explosive+detonator
Clue Text	Are the after-use EED characteristics compatible with the circuit implementation?

Explanation: After firing, squib components may be open- or short-circuited. Depending of this state, the circuit implementation will not be the same, nor the protection devices (current limiter). A short circuit in a squib shall not cause damage other circuit components. Capacitor voltage discharge sources are not as likely to burn a squib "open" as is a battery or generator supply.

Identifier	125A
Title	static energy protection
Clue type	component-only
Item	EED+squib+detonator
Clue Text	Is a static energy protection for electroexplosive device implemented?

Explanation: Without static energy protection, the electroexplosive device may ignite or detonate without being commanded. For instance, a pull-down resistor to ground of 100kΩ may be used.

Identifier	125B
Title	disconnection of a static energy protect
Clue type	component-only
Item	EED+squib+detonato
Clue Text	Can a static energy protection for electroexplosive device be disconnected?

Explanation: Without static energy protection, the electroexplosive device may ignite or detonate without being commanded. Unintended

disconnection or switching out the protection (for test purposes) may introduce a hazard.

Identifier	126
Title	"no fire" current protection
Clue type	component-only
Item	EED+squib+detonator+exbolt
Clue Text	Is a "no fire" current protection for the device implemented?

Explanation: Depending on the duty, EED's may require:
- an out-of-line firing chain
- a separate mechanical arming device
- diverse redundant switches in the firing chain
- sterilisation or guaranteed cut-out circuits.

Identifier	127
Title	unexpected activation
Clue type	component-only
Item	rectifier+thyristor+thyratron+triac+GTO
Clue Text	Can a rectifier change state without being commanded?

Explanation: Some rectifiers need a command to turn-on (thyristor, triac) and to turn-off (GTO). Turn-on occurs in the presence of a short-duration, low-valued gate current. Such low-valued current shall not be generated by a spike. However, they can also activate without being commanded, if for instance they see a significant voltage transition (dV/dt too high). Such conditions may be obtained during testing, for instance.

Identifier	129
Title	drawing consistency with part list
Clue type	component-only
Item	part
Clue Text	Does the parts list correspond to the components used in the circuit?

Explanation: As CAD tools are usually generating automatically the parts list, each component of the circuit shall be listed in the parts list. The acronym associated to each part shall also correspond to the expected symbol.

Identifier	130
Title	component direction
Clue type	component-only
Item	transformer+diode+transistor+IC
Clue Text	Is the component implemented with the correct polarisation on the drawing?

Explanation: Some components are not polarised: resistor, inductor, not polarized capacitor (they are bidirectional). On the other hand, some components can only be used in one way: polarized capacitors, diode, transistor, integrated circuit, transformer (with primary and secondary windings,...).

Identifier	132
Title	current limiter shared by multiple loads
Clue type	component-only
Item	limiter+regulator+csens+breaker+fuse
Clue Text	Is the current limiter sensitive to each load?

Explanation: Whatever the considered load, a short circuit shall trigger the current limiting circuit. No load pattern should exist which can mask a short circuit.

Identifier	133
Title	operating range of a limiting device
Clue type	component-only
Item	fuse+breaker+Zener+regulator
Clue Text	Is the operating range of a limiting device correctly adjusted?

Explanation: Spurious activation of a limiting device shall be avoided: during power switching of an equipment, the spike of inrush current shall not trigger the current limiter otherwise the equipment shall never be turned on! On the other hand, any permanent short circuit shall be detected.

Identifier	136A
Title	response time of a monitoring circuit
Clue type	component-only
Item	sensor+threshold
Clue Text	Is the response time of the monitoring circuit acceptable for the system?

Explanation: If a capacitor voltage is used (directly or not) as a status information by a monitoring circuit, the capacity may induce a delay.
If a monitoring circuit checks the status of a relay just after the relay has changed of state, erroneous information may be transmitted if the relay contacts suffer “contact bounce”after switching. A delay for the status acquisition is necessary to monitor a stable status.

Identifier	136B
Title	start up latency
Clue type	component-only
Item	sensor+threshold
Clue Text	Is the start up latency of the sensor acceptable for the system?

Explanation: Many sensors for physical variables, particularly concentration and temperature, have a latency time before they register correctly.

Identifier	138
Title	transient current path through switches
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+interlock+plug
Clue Text	During change of state of switches, can transient current paths exist?

Explanation: As switches have not the same speed (when switching):

- a switch can still be in the same position whereas another has already changed of state.
- a switch can be "Open" during changing of state, whereas another has contacts touching.

Make-before-break switches create a transient current path between contacts during switching. If a short circuit occurs through contacts during a transitory current path, it may weld the contacts and maintain the short circuit. If there is a switch in an upper branch and in a lower branch, a short circuit may appear if both switches let the current flow at the same time (due to the switching reaction delay).

Identifier	138A
Title	transient current path through switches
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+interlock+plug
Clue Text	During change of state of switches, can transient current paths exist?

Explanation: As switches have not the same speed (when switching):

- a switch can still be in the same position whereas another has already changed of state.
- a switch can be "Open" during changing of state, whereas another has contacts touching.

Make-before-break switches create a transient current path between contacts during switching.
If a short circuit occurs through contacts during a transient current path, it may weld the contacts and maintain the short circuit.
If there is a switch in an upper branch and in a lower branch, a short

circuit may appear if both switches let the current flow at the same time (due to the switching reaction delay).

Identifier	139
Title	transient current gap while switching
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+ interlock+plug
Clue Text	During change of state of switches, can transient current gap exist?

Explanation: While the pole of the relay moving piece is in transit between two contacts, both contacts are momentarily floating. Then the load may not be supplied during a brief moment, which may not be acceptable, or may create the possibility for another current path to occur.

Identifier	140
Title	(un)expected switch/command activation
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+ interlock+plug
Clue Text	Can a switch or its command be activated when not desired or inhibited when expected?

Explanation: During power transition, the transient current which flows (for instance to charge capacitors) can briefly activate a switch command. If a part of a circuit is powered while another part is not, it can inhibit a current path or create new ones.
Unexpected sequences (testing, check-out, contingency,..) can lead to an unscheduled switch combination. Conduction may be required for one load, but may be unwanted for other loads.

Identifier	140A
Title	(un)expected switch/command activation
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+ interlock+plug
Clue Text	Can a switch or its command be activated when not desired or inhibited when expected?

Explanation: During power transition, the transient current which flows (for instance to charge capacitors) can briefly activate a switch command. If a part of a circuit is powered while another part is not, it can inhibit a current path or create new ones.
Unexpected sequences (testing, check-out, contingency,..) can lead to an unscheduled switch combination. Conduction may be required for one load, but may be unwanted for other loads.

Identifier	140AA
Title	(un)expected switch/command activation
Clue type	path-component component-only
Item	transistor+rectifier+breaker+relay+switch+contact+button+ interlock+plug
Clue Text	Can a switch or its command be activated when not desired or inhibited when expected?

Explanation: During power transition, the transient current which flows (for instance to charge capacitors) can briefly activate a switch command. If a part of a circuit is powered while another part is not, it can inhibit a current path or create new ones.
Unexpected sequences (testing, check-out, contingency,..) can lead to an unscheduled switch combination. Conduction may be required for one load, but may be unwanted for other loads.

Identifier	140AAA
Title	(un)expected switch/command activation
Clue type	path-component component-only
Item	and+nor
Clue Text	Can a switch or its command be activated when not desired or inhibited when expected?

Explanation: During power transition, the transient current which flows (for instance to charge capacitors) can briefly activate a switch command. If a part of a circuit is powered while another part is not, it can inhibit a current path or create new ones.
Unexpected sequences (testing, check-out, contingency,..) can lead to an unscheduled switch combination. Conduction may be required for one load, but may be unwanted for other loads.

Identifier	141A
Title	power transient
Clue type	path-component component-only
Item	gate+AND+mux
Clue Text	Can a transient pick-up or drop-out voltage unintentionally energize/de-energize a load or a switching item?

Explanation: During a power transition a capacitor behaves as a low impedance: a capacitor implemented as a static protection (against direct current) may allow an unexpected current flow through a load in dynamic (transient) conditions.
Voltage differences within a circuit often occur:

- during power on/off, some parts of the circuit may have reached their operational voltage while others are still changing
- during power on/off, within a circuit supplied with separated voltages, one voltage may have reached its operational value while others are still changing
- separated parts of a circuit can be independently supplied, one being powered while the others are not.

Such voltage differences, normal or unexpected, can create sneak current paths through diodes, transistor base-collector junction, circuit interfaces where the voltage difference occurs, rectifier due to a high dV/dT, transformer, internal protections (diodes) or connected pins of integrated circuits.

Identifier	142
Title	disconnection of electrical interlocks
Clue type	path-component component-only
Item	interlock+connector+switch+contact
Clue Text	Can the disconnection arising from electrical interlocks create sneak current paths, depending of the disconnection order?

Explanation: If simultaneous disconnections are scheduled, one disconnection may occur before others creating, for a brief moment, unexpected current paths: for instance, suppression of a ground return path.

Identifier	143
Title	connection of testing circuits
Clue type	path-component component-only
Item	testpoint+connector
Clue Text	Can (external) testing circuits energize parts other than those intended to be tested?

Explanation: Usually, protective devices are installed on lines carrying test signals: e.g. diodes connected to VCC either externally or internally to integrated circuits. If an erroneous voltage is applied to the test signal input, a sneak current path through the test interface and the protective devices may energize unexpected functions.

Identifier	146A
Title	loss of ground
Clue type	path-component component-only
Item	ground+earth+chassis
Clue Text	Does loss of ground allow feedback into the path?

Explanation: If the ground is used to determine the potential of a branch, the loss of a ground contact (after switching or disconnection for instance) will leave the junction point floating, allowing an unexpected current to flow through the other branches. It may also mis-bias some circuits and destroy them.

Identifier	146B
Title	loss of ground
Clue type	path-component component-only
Item	node
Clue Text	Does loss of ground allow feedback into the path?

Explanation: If the ground is used to determine the potential of a branch, the loss of a ground contract (after switching or disconnection for instance) will leave the junction point floating, allowing an unexpected current to flow through the other branches. It may also mis-bias some circuits and destroy them.

Identifier	147
Title	loss of power source
Clue type	component-only path-component
Item	transistor+OpAmp+diode+Zener+capacitor
Clue Text	Does loss of one power source mis-bias the circuit?

Explanation: Losing a power source (unexpected switching or disconnection) may create an intermediate bias voltage, allowing an unwanted current path in the other branches or component malfunction.

Identifier	148
Title	high value resistor
Clue type	component-only
Item	resistor
Clue Text	Is a high-value resistor compatible with a low parasitic capacitance?

Explanation: Parasitic capacitor is generated by a circuit input and the board wiring which, when combined with a high value resistor can create an unexpected time constant.

Identifier	151
Title	turn-on delay of a diode
Clue type	component-only
Item	diode
Clue Text	Is the turn-on delay acceptable for the diode?

Explanation: Sometimes, a current versus time curve gives information on a necessary turn-on delay for the diode.

Identifier	153
Title	reference potential for chassis
Clue type	component-only
Item	chassis
Clue Text	Is the chassis reference tied to the adequate reference potential?

Explanation: If the chassis ground is not tied to the equipment ground, some components using the chassis as a heat sink and current return path may not be operational. The metallic case of transistors is sometimes used for a current path as it is tied to the transistor collector.

Identifier	153A
Title	reference potential for power supply
Clue type	component-only
Item	battery+power
Clue Text	Is the power supply reference tied to the adequate ground?

Explanation: If the power return is not tied to the equipment ground, some components using the chassis as a heat sink and current return path may not be operational. The metallic case of transistors is sometimes used for a current path as it is tied to the transistor collector.

Identifier	155
Title	reverse current in a relay coil
Clue type	component-only
Item	relay
Clue Text	Has a protection against reverse current been implemented in series with a relay coil command?

Explanation: A relay coil may receive several commands (through a wired "OR"). To avoid unexpected reverse current from one command to another, a diode is generally added in series with the relay coil on the current path of the command signal.

Identifier	156
Title	bias/polarization signal
Clue type	component-only
Item	transistor+Zener+MOS+FET+OpAmp+analogue
Clue Text	Is a bias/polarization signal correct?

Explanation: Part of the current used to fix a bias/polarization signal may be derived by a component using this reference signal (transistor, OpAmp, Zener, diode). The bias/polarization current shall be high enough to provide a stable reference with the correct voltage. A capacitor may also be added for decoupling.

Ensure that a (scheduled) disconnection or switching will not modify the correct functioning of the circuit.

Identifier	157
Title	reaction delay of one-shot items
Clue type	component-only
Item	EED
Clue Text	Has delay time of one-shot items or electroexplosive devices been considered during design?

Explanation: The following topics should be checked:
- sufficient pulse duration
- explosion duration

Identifier	159
Title	protective and polarization device
Clue type	component-only
Item	buffer+driver+connector+plug+malecon+femalecon
Clue Text	Have interfaces with the outside world a protective and polarization device?

Explanation: To prevent component damage or erroneous information, unterminated inputs at interface may require a polarization resistor (pull-up or pull-down).
Resistor in series with the inputs/outputs shall protect the components from static discharge. Protection diodes may also be added on unsuppressed inputs/outputs. In case an erroneous signal is applied to the circuit through a test interface, a protection shall prevent the circuit from being damaged.

Identifier	161
Title	splitting and recombining of a digital signals
Clue type	path-component component-only
Item	digital+connector+interlock
Clue Text	Does a digital signal sharing a common source and load split and later recombine?

Explanation: Glitches often occur as a result of the separating and later recombining of digital signals having a common source and load. Glitches may results in false logic causing sneak-timing. Glitches are usually detected by drawing a timing diagram.

Identifier	162
Title	switch function for target
Clue type	path-component component-only
Item	switch+breaker+fuse+button+relay+contact+path
Clue Text	Is the switch function directly related to the target operation?

Explanation: The switch may have other functions not related to the target or may be intended for some other purpose entirely. The other function can be activated/deactivated at a time when the target is required/not required.

Identifier	164
Title	correct polarization with coupling capacitor
Clue type	component-only
Item	capacitor
Clue Text	Are circuits using a signal coming through a joining (coupling) capacitor correctly polarized?

Explanation: Sometimes, coupling capacitors are used between circuits to transmit an a.c. signal without any direct current component. In such cases, the direct current component shall be restored by connecting the secondary side of the capacitor to ground via a suitable resistor.

Identifier	7C
Title	location of the protection device
Clue type	component-only
Item	load
Clue Text	Is the circuit located upstream of protection device(s) on a power bus?

Explanation: When power is distributed to circuits, the first item on the power path shall be a protective device in order to protect the power bus against a short circuit in the sensor.

Identifier	9
Title	resynchronization of a sequential logic
Clue type	component-only
Item	IC+and+or+nand+nor+not+flipflop+JK+RS
Clue Text	Is a sequential digital signal safely resynchronized?

Explanation: When a digital signal passes through many logic gates, a delay occurs. Within systems/circuits using a common clock, sequential digital signals shall be resynchronized as soon as the propagation time uncertainty may lead to sneak timing problems. The resynchronisation signal may be missing in some modes.

Identifier	9A
Title	resynchronization of sequential logic with long logic train
Clue type	component-only
Item	IC+and+or+nand+nor+not+flipflop+JK+RS
Clue Text	Is a sequential digital signal safely resynchronized for a long logic train?

Explanation: When a digital signal passes through many logic gates, a delay occurs. Within systems/circuits using a common clock, sequential digital signals shall be resynchronized as soon as the propagation time uncertainty may lead to sneak timing problems. This is especially true if the logic train is very long.

Identifier	169
Title	explicit wording of a label
Clue type	component-only
Item	label+lamp+indicator
Clue Text	Is each label wording explicit?

Explanation: Instead of writing for example “function 2” for a label, it is preferable to identify the function precisely: “door opening”. This is important for indicators or command

Identifier	171
Title	indicator correct function label
Clue type	path-component component-only
Item	lamp+indicator+switch+button
Clue Text	Does the label of the indicator reflect the function of the TARGET?

Explanation: If the label does not properly reflect the function, the TARGET may be activated or deactivated at the wrong time.

Identifier	172
Title	indicator for a unique function
Clue type	path-component component-only
Item	lamp+indicator+switch+button
Clue Text	Does the label of the indicator reflect other functions than the one(s) intended?

Explanation: If the label reflects other functions, some equipment may be activated or deactivated at the wrong time.

Annex C (normative)

Clues for software in ADA language

Identifier	1001
Title	memory mapped register
Clue type	path-component component-only
Item	outreg
Clue Text	Is the register memory mapped? If so, can it be addressed in error as a result of array Identifier errors?

Explanation: Memory addressing errors can cause false output, and require data flow tracing to potential erroneous array addressing locations and pointer assignments.

Identifier	1002
Title	address code control
Clue type	path-component component-only
Item	outreg
Clue Text	Are the codes addressing the register modifiable by several parts of the software?

Explanation: If the address codes are present in other places or can be created by modification, the register values could be modified erroneously.

Identifier	1003
Title	register number modification
Clue type	path-component component-only
Item	outreg
Clue Text	Are any register numbers treated as parameters, or used as updatable table entries?

Explanation: If so, it may be possible to modify the number so that the register is addressed wrongly, or is not addressed when it should be.

Identifier	1004
Title	synthesis of control codes
Clue type	path-component component-only
Item	outreg
Clue Text	Are the operation codes for the register fixed codes, or are they constructed from constants by bit manipulation?

Explanation: If they are constructed, they may be incorrect, resulting in the incorrect output signal.

Identifier	1005A
Title	register sequence dependency
Clue type	path-component component-only
Item	outreg
Clue Text	Are there constraints on the register operation sequence?

Explanation: It is often the case that separate outputs to the same device shall be in the correct sequence in order to establish the correct sequence of system states. If this is not done it may lead to stop of operations, or to incorrect system operation.

Identifier	1006
Title	memory mapped register
Clue type	path-component component-only
Item	inreg
Clue Text	Is the register memory mapped? If so, is it possible to read from the wrong register due to an addressing error?

Explanation: If so a spurious input value will be obtained.

Identifier	1007
Title	register address modification
Clue type	path-component component-only
Item	inreg
Clue Text	Are the register addresses hard coded, or are they stored in a table? Is the table updated?

Explanation: If so, the wrong register may be addressed.

Identifier	1008
Title	register timing
Clue type	path-component component-only
Item	inreg
Clue Text	Is it possible to read register values while they are partially updated?

Explanation: In some cases, registers are updated gradually, for example one bit at a time. If this occurs, then it is important to synchronise read operations so that they occur when an input cycle has been completed.

Identifier	1009
Title	register use coordination
Clue type	path-component component-only
Item	inreg
Clue Text	Are there two programs which read the same register values?

Explanation: If so, are the read operations coordinated, or can the programs disagree about the register value due to differences in the read time?

Identifier	1010
Title	fixed data read cycle
Clue type	path-component component-only
Item	inreg
Clue Text	For data acquisition, is the cycle of data reading fixed? Is the delay time between read operations fixed?

Explanation: If not, then data series will not be made according to a fixed time base and noise will be introduced into data. Interrupts and variable length loops can cause variations in read cycle.

Identifier	1011
Title	data read frequency
Clue type	path-component component-only
Item	inreg
Clue Text	Is the delay time between read operations always short compared with the natural time constants for the system being monitored?

Explanation: As a rule of thumb the delay should be less than one tenth of the shortest significant time constant in the controlled system.

Identifier	1012
Title	input register read timing
Clue type	path-component component-only
Item	inreg
Clue Text	Can exceptions, overflows or special handling upset the timing or sequence of input?

Explanation: If there are unusual operations, there may be excessive time delays in treating time critical input, or in providing safety critical outputs.

Identifier	1013
Title	register overflow
Clue type	path-component component-only
Item	inreg
Clue Text	Can the input register overflow?

Explanation: Register overflow will cause erroneous input data values.

Identifier	1015
Title	function side effects
Clue type	path-component component-only
Item	assign+box
Clue Text	Can expression evaluation order cause variations in function side effects?

Explanation: Is the order of evaluation of parts of the expression fixed? If not, does the sequence of evaluation of terms in the expression affect the result? This can occur if there are functions in the expression which have side effects.

Identifier	1015A
Title	exception side effects
Clue type	path-component component-only
Item	assign+box
Clue Text	Can exceptions cause variations in function side effects?

Explanation: Is the order of evaluation of parts of the expression fixed? If not, does the sequence of evaluation of terms in the expression affect the result? This can occur if there evaluation can result in exceptions are functions in the expression.

Identifier	1016
Title	type coercion
Clue type	path-component component-only
Item	assign+box
Clue Text	Does expression evaluation or assignment involve type coercion?

Explanation: If so, is there any loss of precision or potential for overflow?

Identifier	1017
Title	overflow
Clue type	path-component component-only
Item	assign+box
Clue Text	Can evaluation of the expression cause arithmetic overflow or underflow?

Explanation: Overflow or underflow may cause errors in output, spikes or steps in control signals, and delays in output or loss of processing.

Identifier	1018
Title	division by zero
Clue type	path-component component-only
Item	assign+box
Clue Text	Is there divide operation in the statement? Can division by zero occur?

Explanation: Division by zero will cause an exception, which could lead to delay, loss of processing, or erroneous results.

Identifier	1019
Title	string character 0
Clue type	path-component component-only
Item	assign+box
Clue Text	For strings, is it possible to address before the first string character?

Explanation: Some string handling systems allow free indexing to access particular characters in a string. A typical error is to access the zeroth character. Generally such an error will cause an exception, but in some cases it may corrupt program or data.

Identifier	1019A
Title	string length
Clue type	path-component component-only
Item	assign+box
Clue Text	For strings, is it possible to address beyond the last string character?

Explanation: Some string handling systems allow free indexing to access particular characters in a string. A typical error is to access the zeroth character. Generally such an error will cause an exception, but in some cases it may corrupt program or data.

Identifier	1020
Title	string termination
Clue type	path-component component-only
Item	assign+box
Clue Text	For strings, is there a proper string termination?

Explanation: Strings should preferably have a termination character, or a string length counter, which prevents access beyond the end of the string. Otherwise the program may access invalid characters, or corrupt data or program.

Identifier	1021
Title	array limits
Clue type	path-component component-only
Item	assign+box
Clue Text	For arrays, is it possible to address beyond the array limit?

Explanation: Addressing beyond array limits will retrieve erroneous data or corrupt data or programs. Some compilers prevent addressing outside the array limits, in which case an exception will result

Identifier	1022
Title	array zero element
Clue type	path-component component-only
Item	For arrays, is the zero the element addressed without being defined?
Clue Text	assign+box

Explanation: The addressing convention for arrays shall be well defined. Addressing a non-existent zeroth element in an array is a typical error, especially if programmers work in a multi-language environment.

Identifier	1023
Title	multidimensional arrays
Clue type	path-component component-only
Item	assign+box
Clue Text	For multi dimensional arrays, is the array Identifier sequence clear?

Explanation: A common error is to confuse the order of array indexes.

Identifier	1025
Title	aliasing
Clue type	path-component component-only
Item	assign+box
Clue Text	Are any data elements aliassed or overloaded?

Explanation: If so, the mapping between data types may be in error, with shifts of byte boundaries or value representation.

Identifier	1026
Title	pointer data access
Clue type	path-component component-only
Item	assign+box
Clue Text	Are any data elements aliassed, or addressed by assembler code or by pointers?

Explanation: If so, and all possible bit patterns are allowed some patterns may not be relevant for both aliases?

Identifier	1027
Title	initialization of values
Clue type	path-component component-only
Item	assign+box
Clue Text	Are data values entering into the expression initialized along every flow path leading to the statement?

Explanation: Uninitialized data may contribute to an erroneous calculation. The problem may be missed in a test environment where data has a fixed default value, and then show the error during actual operation.

Identifier	1028
Title	numeric constants
Clue type	path-component component-only
Item	assign+box
Clue Text	Are numeric constants formatted properly, avoiding commas, and with the correct number of zeros?

Explanation: Numeric constants can be given different internal values, depending on format, even for nominally identical numbers.

Identifier	1029
Title	decimal point placement
Clue type	path-component component-only
Item	assign+box
Clue Text	Are commas and decimal points confused?

Explanation: This can be a problem especially if there is an interchange between English speaking and European programming environments.

Identifier	1030
Title	mismatch in parameter list
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Does the call parameter list match the function definition list? In number, types, and number of array indices?

Explanation: Mismatch between the call and declaration of a procedure, in number and type of parameters, is a typical programming error. It is especially prevalent when procedures shall be extended.

Identifier	1031
Title	overloading
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Is a function name or operator symbol overloaded? Can confusion of type then occur?

Explanation: Overloading (multiple typing) of procedures, operators, etc can systematically lead to error, if the code is not modified accurately to reflect the change in operand or parameter types.

Identifier	1032
Title	assignment to constants
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Can new values be assigned to constants when they are used in the parameter list?

Explanation: When constants are used in a parameter list for a procedure or function call, it may be possible to assign a new value to the "constant". This can cause an error which is very difficult to locate, with erroneous calculation in later unrelated functions.

Identifier	1033
Title	recursive call
Clue type	path-component component-only
Item	assign+box+call
Clue Text	If a function in the statement is recursive (or indirectly recursive), is data space allocated dynamically?

Explanation: Recursive functions may accidentally reuse a fixed data area. Runaway or excessive recursion may also lead to running out of stack or heap space.

Identifier	1034
Title	stack overflow
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Is there a possibility for stack overflow on assignment or call?

Explanation: If so memory exceptions may be raised or misaddressing may occur.

Identifier	1034A
Title	heap space exhaustion
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Is there a possibility for exhaustion of heap space when memory is allocated dynamically?

Explanation: If so, a memory allocation exception will occur.

Identifier	1035
Title	freeing memory
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Is all dynamically allocated memory also freed?

Explanation: Memory which is not freed may be needed by other procedures. This can arise because:

- the free instruction is omitted;
- the free instruction can be bypassed exception exits from the procedure.

Identifier	1036
Title	endless recursion
Clue type	path-component component-only
Item	assign+box+call
Clue Text	For the recursive function, is the termination condition guaranteed?

Explanation: The number of recursion levels shall be predictable.

Identifier	1037
Title	case coverage in nested IF
Clue type	path-component component-only
Item	if+diamond+case
Clue Text	For a nested If or case statement, is the list of conditions exhaustive?

Explanation: For safety-related programs, the list of possible cases should be made explicit, rather than relying on a final "other" or "else" clause. Then any non-allowed condition can lead to error handling.

Identifier	1038
Title	test sequence and priority
Clue type	path-component component-only
Item	if+diamond+case
Clue Text	For nested IF statements, is the sequence or priority of tests correct or consistent?

Explanation: The actual sequence of condition nesting may be irrelevant, provided that the logic is completely correct. However, lack of clarity and consistency often lead to error, for example neglecting some special case.

Identifier	1039
Title	function calls in IF test
Clue type	path-component component-only
Item	assign+box+call
Clue Text	Are there repeated function calls within the IF condition? Does the function allow side effects?

Explanation: Function calls with side effects within conditional statements are almost guaranteed to give erroneous values for side effect variables at some stage of processing.

Identifier	1040
Title	floating point equality
Clue type	path-component component-only
Item	if+diamond+case
Clue Text	Are there tests for equality between floating point numbers? If so, how is equality guaranteed?

Explanation: Two real numbers will in general never be equal unless values are assigned identically.

Identifier	1040A
Title	zero representation
Clue type	path-component component-only
Item	if+diamond+case
Clue Text	Are both positive and negative zero values possible?

Explanation: On some computers, there is a possibility for a sign difference, even when the numbers represent zero. This can make equality comparison incorrect.

Identifier	1041
Title	TRUE and FALSE representation
Clue type	path-component component-only
Item	if+diamond+case+assign+box
Clue Text	Is the coding for TRUE and FALSE values consistent, and used consistently?

Explanation: Bit coding for representation TRUE and FALSE varies from system to system, and programmers often make errors when transferring between systems.

Identifier	1043
Title	loop termination
Clue type	path-component component-only
Item	while+for+loop
Clue Text	Is loop termination guaranteed?

Explanation: An endless loop can cause a stop of all processing on a processor, or, if time slicing is used, it can cause a single task to fail.

Identifier	1043A
Title	loop termination
Clue type	path-component component-only
Item	while+for+loop
Clue Text	Does the loop deal with precisely all elements of an array? For loops that deal with arrays, does the loop Identifier track the array precisely, and deal with all loop elements, including the zero'th and the last?

Explanation: Take special care on loops which relate the i'th and the (i+1)'th array elements, or similar offset access to arrays

Identifier	1045
Title	variable loop Identifier limit
Clue type	path-component component-only
Item	while+for+loop
Clue Text	For the FOR loop Identifier, is the Identifier limit value fixed, or can it vary, and if so, can the variation result in a loop Identifier error?

Explanation: Changing the limit value for a for loop can often result in difficult logic, in which it is not clear whether a final limit will be reached. The usual result is an array Identifier overflow error, but in some cases, the program may request all available memory, before an exception occurs.

Identifier	1046
Title	control transfer into a loop
Clue type	path-component component-only
Item	while+for+loop
Clue Text	Are there labels within the loop, and can control transfer into the loop?

Explanation: Transfer of control into a program loop will in virtually all cases result in errors due to lack of loop initialization. Some programs allow for transfer of control out of a loop and then back again, but this is generally bad practice, since some compilers produce undefined results in such cases.

Identifier	1047
Title	loop termination
Clue type	path-component component-only
Item	while+for+loop
Clue Text	Is the loop Identifier used outside the loop and if so, is its value also undefined outside the loop?

Explanation: Some languages and some compilers allow an Identifier in a FOR loop to be incremented, and the resulting value to be available on leaving the loop. This is not always the case though, and for some compilers, the loop Identifier value is undefined when the loop is excited.

Identifier	1048
Title	loop termination
Clue type	path-component component-only
Item	while+for+loop
Clue Text	Are there exits from inside the loop? If so, are the loop terminations identical or are they separated on purpose (completion, success, failure) with appropriate processing?

Explanation: Flags or labelled exit points are two alternative ways of implementing multiple exits from loops.

Identifier	1049
Title	event processing
Clue type	path-component component-only
Item	software
Clue Text	For event driven programs, does the processing depend on the sequence of events? If so, are all sequences allowed?

Explanation: Event driven programs can be difficult to write, because the programmer has one step by step sequence in mind, for example that described in the program user manual. However, alternative sequences will generally occur, and if the program is sequence dependent, the alternative sequences shall be catered for.

Identifier	1051
Title	shared data processing
Clue type	path-component component-only
Item	assign+box
Clue Text	Are shared variables semaphore protected?

Explanation: If not, it may be possible for two tasks to attempt to update shared variables at the same time, so corrupting the values.

Identifier	1052
Title	shared data processing
Clue type	path-component component-only
Item	assign+box
Clue Text	Are groups of variables which shall be updated consistently semaphore protected?

Explanation: If not, multiple tasks may attempt to update records at the same time,and the relations between variable values may then be inconsistent.

Identifier	1053
Title	shared table processing
Clue type	path-component component-only
Item	assign+box
Clue Text	Can the current task address a table element which has been deleted by another?

Explanation: Deletion is a particularly difficult operation in a multitasking environment, particularly if tasks maintain their own Identifier variables into a table or array.

Identifier	1054
Title	semaphore/lock matching
Clue type	path-component component-only
Item	assign+semaphore
Clue Text	Can a program reserve or lock data and fail to free it?

Explanation: Matching of requesting and releasing commands s essential. Release may be missing on some program paths, or if an exception arises in a program.

Identifier	1055
Title	event processing
Clue type	path-component component-only
Item	assign+box+semaphore
Clue Text	Can the program fail to free reserved data due to exceptions or errors?

Explanation: Matching of requesting and releasing commands s essential. Release may be missing on some program paths, or if an exception arises in a program.

Identifier	1056
Title	deadlock
Clue type	path-component component-only
Item	semaphore+task
Clue Text	Can deadlock arise?

Explanation: Deadlock arises when two or more tasks are competing for two or more resources. If task A has resource X and waits for resource Y, and task B has resource Y and waits for X, neither task can proceed. Solutions to the problem are to request resources in groups, or to use a fixed order for resource requests. Typical resources are memory, data areas, data base records, indexes, buffers,and peripheral devices.

Identifier	1058
Title	shared data access protection
Clue type	path-component component-only
Item	assign+box
Clue Text	Are all program data interactions synchronised by semaphores or rendezvous, or are some dependent on timing?

Explanation: If dependent on timing, is the timing insensitive to load, processor type, or priority changes.

Identifier	1059
Title	buffer overflow
Clue type	path-component component-only
Item	input+output
Clue Text	Can the pipe, buffer, or queue be overfilled if input load increases?

Explanation: Heavy input, bus or transaction loads can lead to queue or buffer overfilling. This can in turn lead to addressing errors, to loss of input, or to corruption of entries

Identifier	1060
Title	overload data loss
Clue type	path-component component-only
Item	input
Clue Text	Can processing overload delay response so that short inputs are missed?

Explanation: Input signals which only exist for a short time may be lost completely if the computer is overloaded, and does not scan inputs fast enough. Interrupts maybe missed if interrupt processing is slow.

Identifier	1061
Title	overload delay of response
Clue type	path-component component-only
Item	input+task
Clue Text	Can overload delay response so that response frequency becomes comparable to a natural frequency of the controlled system?

Explanation: If the delay grows to approach the time constant for a controlled system, then oscillation can result. With large delays, this can lead to an equivalent problem in transaction processing, where queries are returned faster than the system can process the original request.

Identifier	1062
Title	overload delay of espouse
Clue type	path-component component-only
Item	input+task
Clue Text	Can overload delay an output so that a critical deadline is missed?

Explanation: Critical deadlines are typical of cyclic or one-shot controlled systems, in which there is a time window for correct input or output to the computer.

Identifier	1063
Title	error handling interruption
Clue type	path-component component-only
Item	exception+assign
Clue Text	Does error handling stop processing? IF so, is the stop hazardous?

Explanation: Exception handling cannot always lead to system restart or recovery.

Identifier	1064
Title	error handling lockout
Clue type	path-component component-only
Item	exception+assign+box
Clue Text	Can reserved data or memory be frozen due to error handling?

Explanation: Semaphores which are not released can lead to lock out, as can bus contention, and memory contention lines.

Identifier	1065
Title	error recovery reinitialization
Clue type	path-component component-only
Item	exception+assign+box
Clue Text	Are all data values reinitialized on error recovery?

Explanation: If a restart occurs, reinitialization is necessary.

Identifier	1066
Title	data consistency on error recovery
Clue type	path-component component-only
Item	exception+assign+box
Clue Text	Does error handling restore data consistency?

Explanation: In some cases, stored or shared data will be corrupted. In this case, restart programs should at least restore consistency, so that further software exceptions do not occur, and the data can be accessed reliably.

Identifier	1067
Title	deep level errors
Clue type	path-component component-only
Item	procedure+function+call
Clue Text	Can the procedure terminate the task?

Explanation: A typical example arises in error processing, especially when a low level subroutine terminates on error.

Identifier	1068
Title	error codes on procedure exit
Clue type	path-component component-only
Item	procedure+function+call
Clue Text	Are there any error conditions and codes on procedure exit comparable to a natural frequency of the controlled system?

Explanation: A consistent philosophy for treating exceptions is necessary. This is particularly difficult to achieve if library or generic routines are used.

Identifier	1073
Title	data corruption
Clue type	path-component component-only
Item	assign+box
Clue Text	Can memory be corrupted, so that wrong data values are used?

Explanation: Corruption can arise due to addressing errors, data transmission errors, or memory failure. Transient memory failure may not always be detectable, even when redundancy is used.

Identifier	1074
Title	erroneous control transfer
Clue type	path-component component-only
Item	goto+return
Clue Text	Can random control transfers be made into critical sections of code?

Explanation: Go to statements can lead to unexpected transfers of control, particularly if label or procedure arrays (switches) are used. Erroneous control transfers can also arise due to hardware error in calculating jump addresses.

Identifier	1075
Title	computed address error
Clue type	path-component component-only
Item	return+goto
Clue Text	Is the address for the control transfer computed or taken from an array? If so can the address be corrupted?

Explanation: A corrupted address will lead to a random transfer of control.

Identifier	1077
Title	use of access types and pointers
Clue type	path-component component-only
Item	assign+box
Clue Text	Does the assignment make use of access types?

Explanation: Access types and pointers are one of the biggest sources of errors in delivered software, and in safety related software should be used only where strictly necessary, e.g. in list processing packages. The dangers with the use of pointers is that simple arithmetic, initialization, and usage errors can lead to corruption of data and programs in an untraceable and seemingly random fashion.

Identifier	1078
Title	predefined exceptions
Clue type	path-component component-only
Item	assign+box
Clue Text	Is it possible to activate predefined exceptions?

Explanation: The processing of predefined exceptions is often wrong for safety related programs, e.g. the reporting and termination of tasks which often takes place is generally wrong. The program

needs to be able either to take safety action, or to continue monitoring.

(This page is intentionally left blank)

Annex D (informative)

Clues for hydraulic equipment

Identifier	2000
Title	evaporation of a liquid
Clue type	component-only+path-component
Item	tank+tankbladder+tankpres+vessel
Clue Text	Is there any device which protects against the decrease of pressure?

Explanation: If the pressure decreases below the liquid steam pressure, it would produce a change of phase which could have catastrophic consequences if the necessary measures are not taken into account (for instance, part of the obtained vapour could circulate upstream the tank and mix with other liquids or vapours).

Identifier	2001
Title	pressure relief
Clue type	component-only
Item	checkv+cvalve+pregulator+sv
Clue Text	Has any device been foreseen in order to quickly reduce overpressure peaks?

Explanation: To avoid the failure in a hydraulic system, a safety valve or device should be installed to relieve overpressure.

Identifier	2003
Title	engine's efficiency
Clue type	component-only
Item	pump+turbine
Clue Text	Are the characteristic parameters the correct ones?

Explanation: An engine has optimum efficiency in some specific conditions of its parameters (for instance in the case of a pump, for a specific height, flow, work pressure, the efficiency, the efficiency will be maximum or not depending on its characteristic graph).

Identifier	2004
Title	cavitation
Clue type	component-only
Item	pump+turbine
Clue Text	Are there any regions where the vapour pressure is lower than the vapour tension of a liquid?

Explanation: If pressure is lower than the vapour tension, vapour bubbles are produced within the liquid. These bubbles are drag down with the liquid to a region where a higher pressure is reached. If the bubbles are close to a wall the pressure that the liquid produces when it enters the cavities might create very high local pressures which could damage the solid surface. Additionally, vibration, noise and a decrease of efficiency of the hydraulic engine occur.

Identifier	2005
Title	water hammer
Clue type	path-component
Item	cvalve+valve
Clue Text	Has the 'water hammer' effect caused by the sudden closure of a valve been considered?

Explanation: When a flow is quickly decelerated due to the closure of a valve, the liquid compressibility and the elasticity of the pipe walls might produce a phenomenon called a "water hammer". This produces a wave of high pressure downstream that could damage the piping and the equipment mounted on it.

Identifier	2006
Title	wear out
Clue type	component-only
Item	checkv+cvalve+drain+pump+sv+tank+tankbladder+tankpres+ turbine+valve+vessel
Clue Text	Has the wear out of mechanical components and piping in hydraulic systems been considered?

Explanation: With use piping, valves, tanks, etc. are affected by corrosion, incrustations and deposit of material on their walls. This could also impact the friction coefficients and therefore the characteristics of the fluid flow.

Identifier	2007
Title	reaction of corrosion products
Clue type	once only
Item	checkv+drain+pump+sv+tank+tankbladder+tankpres+turbine+valve+vent+vessel
Clue Text	Can corrosion products catalyse a reaction?

Explanation: Some corrosion products might catalyse a reaction with the fluid contained in the hydraulic system.

Identifier	2008A
Title	common drain or venting lines
Clue type	path-component
Item	drain+vent
Clue Text	Do common drain, vent, pressurisation, blanketing, connect several sources?

Explanation: If several fluid sources are connected through common lines, the unintended mixture or reaction of two (or more) of them could damage the system or affect the required performance of the system. If the common lines are unavoidable, precautions (e.g. installation of valve allowing only one-way flow) should be taken to prevent unintended mass flow trough these “common lines”.

Identifier	2008B
Title	connected flow sources
Clue type	path-component
Item	tank+tankbladder+tankpres+vessel
Clue Text	Have sources of different fluids and/or at different pressures/temperatures been connected together?

Explanation: Some flow sources might require to be ’isolated’ from other sources. If this is not done undesired chemical reaction and/or an unintended change of the characteristic of the fluid flow might occur.

Identifier	2009
Title	loss of drains
Clue type	path-component
Item	drain
Clue Text	Does loss of drains allow backfeeding into the path?

Explanation: If the drains are used to control the pressure in a branch of the circuit, the loss of drains (after switching of a valve for instance) will let the junction point in a “floating state” and might induce an unintended current to flow in other branches of the circuit.

Identifier	2011A
Title	protection against reverse flow
Clue type	path-component
Item	cvalve+tank+tankpres+valve+vessel
Clue Text	Is each branch of the circuit protected against potential reverse flow?

Explanation: For instance, during the switching from one branch to another, there may be a reverse current between branches. This applies especially if there are multiple fluid sources that are connected or branches originating from the same source, that have different pressure drops, and later reconnect. When no protection against reverse flow is implemented downstream to each flow source there might be current flowing from other sources to the unprotected one(s). Usually, check valves are used to eliminate this problem.

Identifier	2012
Title	valve used for different functions
Clue type	path-component
Item	cvalve+valve
Clue Text	Is the valve used to implement different functions in different operating modes?

Explanation: If a valve implements different functions (e.g. isolation and flow control) in different operating modes of the system there is the possibility that a specific function might be unintentionally activated or deactivated in some operating modes of the system.

Identifier	2013
Title	pressure level during different operating modes
Clue type	path-component
Item	cvalve+tank+tankpres+valve+vessel
Clue Text	Does the pressure level remain in its expected range(s) during the various operating modes?

Explanation: During particular phase (e.g. testing) or changes of operating mode some unforeseen switching combinations might be triggered and this could lead the pressure of the system to exit from the expected range.

Identifier	2014A
Title	temporal gap between switching of valves
Clue type	path-component
Item	cvalve+valve
Clue Text	Is the temporal gap between the activation and deactivation of different valves in a system justified?

Explanation: When multiple valves shall be activated or deactivated, care should be taken that the temporal gap between their activation and deactivation does not lead to unintended effects (e.g. reverse flow, flow at the wrong time)

Identifier	2014B
Title	switching sequence of valves
Clue type	path-component
Item	svelte+valve
Clue Text	Is the activation or deactivation sequence of different valves in a system the proper one?

Explanation: When multiple valves in system shall be activated or deactivated the proper sequence of activation needs to be ensured either automatically or by manual procedures, otherwise unintended or untimely flow can occur.

Identifier	2015
Title	transient flow paths
Clue type	component-only+path-component
Item	cvalve+pump+turbine+valve
Clue Text	Has the flow transient time when an item changes state been taken into account?

Explanation: When a valve is opened or closed a certain time is needed for the flow to be fully established or stopped as the case may be. This transient time could cause problems of synchronization with other equipment (e.g. other valves) in the circuit that have different response times. Similar considerations apply also to other items (e.g. pumps, turbines, etc). The synchronisation problems could cause unintended flow (or no flow) to occur during the transient.

Identifier	2016
Title	leakage flow
Clue type	component-only
Item	checkv+cvalve+drain+pump+sv+tank+tankbladder+tankpres+turbine+valve+vent+vessel
Clue Text	Can the leakage flow of the component lead to an undesired activation or inhibition of other equipment in the circuit?

Explanation: For instance when a circuit segment should be nominally isolated, internal leakage from the above segment can cause an unintended flow to other parts of the circuit.

Identifier	2017
Title	storage
Clue type	path-component
Item	tank+tankpres+vessel
Clue Text	Has the presence of internal storage devices been taken into account when designing the power off sequence of the system?

Explanation: As internal storage devices (e.g. vessels, containers, accumulators) might contain significant masses of fluids after external supply sources are removed or isolated a proper isolation sequence of these devices should be envisaged during the power off phase of the circuit.

INDEX

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W

Z

ECSS Document Improvement Proposal

1. Document I.D.	2. Document Date	3. Document Title
ECSS-Q-40-04A Part 2	14 October 1997	Sneak analysis - Part 2: Clue list

4. Recommended Improvement (identify clauses, subclauses and include modified text and/or graphic, attach pages as necessary)

5. Reason for Recommendation

6. Originator of recommendation

Name:	Organization:	
Address:	Phone: Fax: E-Mail:	**7. Date of Submission:**

8. Send to ECSS Secretariat

Name:	Address:	Phone: +31-71-565-3952
W. Kriedte	Keplerlaan 1	Fax: +31-71-565-6839
ESA-TOS/QR	2200AG Noordwijk	E-Mail: wkriedte@estec.esa.nl
	Netherlands	

Note: The originator of the submission should complete items 4, 5, 6 and 7.

This form is available as a Word and Wordperfect-Template on internet under
http://www.estec.esa.nl/ecss/improve/

(This page is intentionally left blank)