EDMS-2002392 (v12)

2019-06-18

dependable-design@cern.ch

Reliable Electronics Design – Worksheet & Checklist

B. Todd, W. Viganò, V. Schramm, L. Felsberger, A. Apollonio, J. Schwenk, D. Calcoen
(CERN, Geneva, Switzerland)

Keywords: reliability, availability, electronics design, worksheet.

Summary

This worksheet is to be used as part of electronic board design reviews, the worksheet is particularly appropriate if machine availability is a concern of the equipment being reviewed.

The worksheet produces a scorecard, giving guidance to the areas concerning reliability that may be improved; the final page of this document is a printable scorecard, which is also available as a separate spreadsheet.

This document has been prepared under the mandate of the *Machine Availability and Reliability Panel*, aiming to improve the overall reliability of systems throughout CERN's accelerator complex. This document has been authored by many individuals throughout CERN's *Accelerator Technology Sector*.

The worksheet poses questions across several domains, chosen to give indications and to trigger discussions concerning reliability aspects of an electronics design. In total, there are **44** questions in the form Q#; the questions are formulated as closed questions, ranked in three categories according to their importance: required (**R**), strongly advised (**SA**), advised (**A**). The goal of the worksheet is to produce a scorecard identifying reliability strengths and weaknesses; in general, the higher the score the more reliability has been considered as part of the design.

The domains considered are:

A. System-Level
B. Board-Level
C. Electronics Design – Schematic & Printed Board
D. Bill of Materials
E. Testing
F. Maintainability

A basic requirement before using this worksheet is that the electronic design being appraised is correct, that it meets its specification, and that the appropriate quality assurance steps are being carried out. In principle, a design that scores *zero* should still function adequately.

The board: The item being studied, and subject to review. Normally consisting of a schematic, a printed board, mechanical aspects, production files and assembly information.
The system: The equipment made by combining electronic boards. In this case, the system includes the board, which is the subject of the review.
The designer(s): The person or team of people responsible for the realisation of the board and system, this includes the specification as well as the technical work.

A. System-Level $\sum = 16$

Q1: Is there a block diagram of the system & board? **R [Y = 1]**

Block diagrams help build understanding, and show the relative importance of the parts of the design. This information can be used to ensure effort is being spent on those parts of the system and board that have the highest impact on reliability.

Q2: Are interfaces documented, with margins explained? **R [Y = 1]**

Interfaces are a key area, they can be difficult to test, and failures can be hard to diagnose. The designer must ensure that interfaces are appropriately specified and implemented. Operational margin must be foreseen electrically and optically. Document of interfaces, provides a basis for the engineering evaluation.

Q3: Is the system behaviour known for all operation modes? **R [Y = 1]**

The system specification should consider how the system behaves in all operational modes of the machine in which it is installed.

Q4: Are the connectors appropriate? **R [Y = 1]**

The designer should use appropriate connectors. Reliable data transfer may require impedances to be matched; reliable powering may require a minimum gauge, the finishing of connectors and pins may be important for reliability over time.

Q5: Has grounding, bonding & 0V been considered and documented? **R [Y = 1]**

Electronic systems, with rare exceptions, should have contiguous grounding with zero volts, chassis ground and earth potentials connected. Undesired compatibility issues, such as ground loops, are easier to identify via a global diagram. The designer should provide a diagram explaining the grounding strategy, and integration with system grounds. In cases where circuits can be parameterised, the designer should choose an appropriate solution, be that hardware or software driven parameters. Local potentiometers can be unreliable, inaccurate and hard to maintain. They should only be used with justification.

Q6: Is there a design/user manual available? **SA [Y = 1]**

A design manual represents an essential part to document and follow up a project. The document serves to track and control the progress as well as to transfer information to externals, e.g. during a design review.

Q7: Is the system robust when presented with flawed information? **SA [Y = 1]**

Data interfaces should be built with margins, and the system behaviour should be predictable even when these give erroneous information. *Emergent behaviour* may also be a concern, which should be considered as part of the system design.

Q8: Is the system designed using a "reliability" framework? **SA [Y = 1]**

Following a reliability framework, or lifecycle, gives a strong foundation for the work on reliability aspects.

Q9: Have potential misconnections been analysed? **SA [Y = 1]**

The designer should consider what happens to the system if interfaces are not correct, for example, swapping cables during maintenance, or plugging a board into an incorrect position. Effects should be understood, and where needed, mitigations proposed.

Q10: Is the board's impact on system-level availability understood? **A [Y = 1]**

The designer should know the functions the board contributes to, and the other aspects of the system with which the board has dependencies. This allows the designer to understand the effort to be put into reliability, and to consider the impact of failures of the board on the system. *Impact* should be considered as combination of *likelihood* and *consequence*.

Q11: -When related systems are maintained, are systems protected? **A [Y = 1]**

If neighbouring, or dependent systems are being maintained, or put into a service mode, the effect on this system should be known. Damage to this system should be mitigated. Equally, when *this system* is maintained, impacts on *other systems* should be understood.

Q12: Can the system switch *mode*, reducing stress levels? **A [Y = 1]**

High stress reduces the lifetime of electronic components. Applying a high stress level only when needed, thus increases the system reliability.

Q13: Have reliability calculations been used to drive the design? **A [Y = 1]**

Tools and methods exist to help the designer address reliability. Using the output from such analyses can lead to improvement in reliability. E.g. *Fault tree, failure mode...*

Q14: Are the pinologies of the connectors appropriate? **A [Y = 1]**

The designer should consider what happens if pins are shorted, and how the signals from connectors route through the printed board. A lower error rate may be achieved if impedances are controlled, and twisted pairs should be used consistently across the design.

Q15: Has the installation environment been sufficiently considered? **A [Y = 1]**

Physics environments are typically; *commercial*, *industrial*, and/or *radiation* exposed. The designer should consider the impact of this. Consideration should be given to risks related to *geographically close* equipment or effects, specifically *common-cause* issues.

Q16: Are configurations appropriately managed? **A [Y = 1]**

In cases where circuits can be parameterised, the designer should choose an appropriate solution, be that hardware or software driven parameters. Local potentiometers can be unreliable, inaccurate and hard to maintain. They should only be used with justification.

B. Board-Level $\sum = 6$

Q17: Is the board protected against Electro-Static Discharge? **R [Y = 1]**

The board should be adequately protected against damage due to Electro-Static Discharge, by the appropriate use of suppressors, impedance, isolation and/or protection diodes.

Q18: Is the board designed for the ambient temperature? **R [Y = 1]**

The board design should be appropriate for the ambient temperature. Circuits used in high temperatures should foresee appropriate cooling and ventilation; those being used in colder temperatures may need other mitigation, such as thermal regulation.

Q19: Have Electro-Magnetic Compatibility issues been considered? **SA [Y = 1]**

The board may be subject to, or produce, electro-magnetic radiation. The designer should take appropriate precautions, and carry out appropriate testing.

Q20: Has screening been considered to address infant mortality? **A [Y = 1]**

A better reliability should be achieved when boards only exhibit random-in-time failures. This may require infant mortality to be screened before boards are used, this should be considered by the designer.

Q21: Is the board designed for re-use? **A [Y = 1]**

Common, proven, reliable circuits should be shared amongst other projects. Elements of the board that may be used elsewhere should be designed with this in mind.

Q22: Are margins foreseen for incremental upgrades? **A [Y = 1]**

Electronics should aim to have margins, spare logic resources, extra memory, and so on. The designer should consider this as part of the design process.

C. Electronics Design – Schematic & Printed Board $\sum = 7$

Q23: What percentage of the schematic is already proven in use? **R [0-100%]**

Making use of circuits proven as reliable elsewhere should improve reliability. New circuit designs, or technology, may be an area to investigate. The designer should also check for *lessons-learned* from the failure of similar circuits and equipment.

Q24: Do all components have defined values? **R [Y = 1]**

A reliable design requires thorough documentation, in order to facilitate the repair and maintenance. The designer should not use undefined values in a production schematic; there should be complete component references throughout.

Q25: Is manufacturability considered in the printed board layout? **R [Y = 1]**

Latent manufacturing defects should be reduced, and over-stress of boards should be minimised during manufacture. The number of manufacturing steps should be reduced; and the location and size of components should be considered to facilitate manufacturing.

Q26: Do trace widths have margin, where possible? **R [Y = 1]**

Thinner traces tend to heat more as they are loaded, leading to wear out of the printed board material. The designer should consider the current requirements of each net, and should ensure that the track width is optimised. This may be a conflicting requirement when controlled impedance lines are used.

Q27: Are all ranges of values and tolerances considered? **R [Y = 1]**

Electronic components have tolerances, and timing margins. The design should function with worst-case combinations of each. The designer should prove this is the case.

Q28: Has the schematic been analysed for failure rates & modes? **A [Y = 1]**

Failure rate analysis reveals weak parts of a design, addressing these should improve the long-term reliability. Failure modes information can be used to improve *availability*.

Q29: Is the layout consistent with the design's reliability features? **A [Y = 1]**

The layout should address reliability features put in place by the designer. A system designed to have redundancy in case of failure must have a layout consistent with that redundancy, paying attention to *common cause* issues. Serviceable elements should be accessible without effecting the redundant sections of the design.

D. Bill of Materials ∑ = 4

Q30: Are voltages de-rated? **R [Y = 1]**

Components having a voltage rating should be checked, ensuring that there is sufficient margin. A larger de-rating tends to improve the longer-term reliability of electronics. It is recommended to use a de-rating factor of at least 2.

Q31: Are wattages de-rated? **R [Y = 1]**

Components having a power rating should be checked, ensuring that there is sufficient margin. This include supplies, as well as passive and active components. Higher de-rating tends to improve the longer-term reliability of electronics. It is recommended to use a de-rating factor of at least 2.

Q32: Has the expected production life been considered? **SA [Y = 1]**

The designer should consider the length of time that the board should be produced, to avoid reengineering. Parts should not be "end-of-life" during a board's first production.

Q33: Are the number of line items optimised? **A [Y = 1]**

Inventory management is simplified if fewer parts are used. This can improve the maintenance phases of a design, by requiring fewer parts to be stored.

E. Testing ∑ = 3

Q34: Is an appropriate test approach and equipment foreseen? **R [Y = 1]**

To achieve high reliability, latent failures should be minimised, and the initial quality of the board should be proven by testing. The designer should have chosen an appropriate test approach, and should foresee appropriate equipment.

Q35: What percentage can be easily tested after fabrication? **A [0–100%]**

The designer should ensure appropriate test points, and/or test system connectors.

Q36: Can the board be exercised via remote test mode? **A [Y = 1]**

To improve reliability, diagnosis of faults should be quick and accurate. Remote validation of board behaviour should be possible. Remote testing can be carried out at the level of the board, by internal stimuli (*self-test*), or at the level of the system, by external stimuli.

F. Maintenance $\sum = 8$

Q37: Has a maintenance plan been prepared? **SA [Y = 1]**

Long-term reliability may depend on regular servicing, or maintenance of a system. A plan should be put in place, to be followed for the system lifetime.

Q38: Can appropriate aspects of performance be remotely read? **A [Y = 1]**

Once in operation, the board performance should be able to be monitored remotely, typically monitoring temperature, load factors, error rates, faults and redundant signals. Appropriate signals should be foreseen, and made available for remote diagnostics.

Q39: Does the board have a remotely accessible unique identifier? **A [Y = 1]**

Maintenance is facilitated by assigning each board a globally unique identifier. Remote access to the unique identified allows a complete part inventory to be made in quasi-real-time, facilitating maintenance.

Q40: Is a database in place for failure data? **A [Y = 1]**

From the first pre-series of boards, useful failure information can be gathered in a database. The designer should foresee this, and plan its use accordingly.

Q41: Does the board have a remote reset and/or power cycle facility? **A [Y = 1]**

A useful feature is to be able to remotely reset and/or power cycle a board. If a failure does occur, and can be remotely cleared in this manner, it should reduce the time to repair.

Q42: After a failure, can the board "lifetime" be readily determined? **A [Y = 1]**

One of the key metrics for reliability is lifetime; it is an advantage if this information is readily available in the board. This could be an *up time* counter, read upon failure, giving direct access to lifetime information without reliance on external information.

Q43: After a failure, can board "load-lifetime" be readily determined? **A [Y = 1]**

In addition to lifetime, it is useful to have the loading factor of the board over time. This is typically electrical loading, such as power, or mechanical stress, such as cycles.

Q44: After a failure, can board "failure mode" be readily determined? **A [Y = 1]**

To ascertain the board reliability, a Weibull chart needs to be constructed from failure data. The failure modes of the board should be recorded, along with the lifetime and loading information. The designer should consider this requirement as part of the board design, and should ensure that this information can be readily ascertained after a failure occurs.

A	**System Level**		**[16]**
1	Is there a block diagram of the system & board?	**R**	…
2	Are interfaces documented, with margins explained?	**R**	…
3	Is the system behaviour known for all operation modes?	**R**	…
4	Are the connectors appropriate?	**R**	…
5	Has grounding, bonding and 0V been considered and documented?	**R**	…
6	Is there a design/user manual available?	**SA**	…
7	Is the system robust when presented with flawed information?	**SA**	…
8	Is the system designed using a “reliability” framework?	**SA**	…
9	Have potential misconnections been analysed?	**SA**	…
10	Is the board’s impact on system-level availability understood?	A	…
11	When related systems are maintained, are systems protected?	A	…
12	Can the system switch "mode", to reduce stress levels according to operational scenario?	A	…
13	Have reliability calculations been used to drive the design?	A	…
14	Are the pinologies of the connectors appropriate?	A	…
15	Has the installation environment been sufficiently considered?	A	…
16	Are configurations appropriately managed?	A	…
B	**Board Level**		**[6]**
17	Is the board protected against Electro-Static Discharge?	**R**	…
18	Is the board designed for the ambient temperature?	**R**	…
19	Has the designer considered Electro-Magnetic Compatibility issues?	**SA**	…
20	Has screening been considered to address infant mortality?	A	…
21	Is the board designed for re-use?	A	…
22	Are margins foreseen for incremental upgrades?	A	…
C	**Electronics – Schematic & Printed Board**		**[7]**
23	What percentage of the schematic has already been proven in use?	**R**	…
24	Do all components have defined values?	**R**	…
25	Is manufacturability considered in the printed board layout?	**R**	…
26	Do trace widths have margin, where possible?	**R**	…
27	Are all ranges of values and tolerances considered?	**R**	…
28	Has the schematic been analysed for failure rates, and failure modes?	A	…
29	Is the layout consistent with the design’s reliability features?	A	…
D	**Bill of Materials**		**[4]**
30	Are voltages de-rated?	**R**	…
31	Are wattages de-rated?	**R**	…
32	Has the expected production life been considered?	**SA**	…
33	Are the number of line items optimised?	A	…
E	**Test**		**[3]**
34	Is an appropriate test approach and equipment foreseen?	**R**	…
35	What percentage of the board can be easily tested after fabrication?	A	…
36	Can the board be exercised via remote test mode?	A	…
F	**Maintenance**		**[8]**
37	Has a maintenance plan been prepared?	**SA**	…
38	Can appropriate aspects of the board performance be remotely read?	A	…
39	Does the board have a remotely accessible unique identifier?	A	…
40	Is a database in place for failure data?	A	…
41	Does the board have a remote reset and/or power cycle facility?	A	…
42	After a failure, can the board “lifetime” be readily determined?	A	…
43	After a failure, can the board “load-lifetime” be readily determined?	A	…
44	After a failure, can the board “failure mode” be readily determined?	A	…

For the worksheet equivalent of this sheet, see EDMS 2002392.