High Reliability Design Guidance

White Paper

November 2023

-

Document Number: 792652-1.0

Contents

Figures

Tables

Revision History

Date	Revision	Description
November 2023	1.0	Initial release.

§

1.0 Introduction

This document provides the general information and methods to design for reliability of electronic products to OEM/ODM partners, not cover like RAS (Reliability, Availability and Serviceability) features in Intel Xeon CPU. You may learn about What is Reliability, how is it Measured and How to design high reliability electronic products. Specifically, for below mentioned reliability items.

- Reliability index: failure rate, MTBF, MTTR and Availability
- Bathtub Curve
- Design for reliability Concept
- System Reliability Validation
- MTBF Prediction
- Component derating
- Power rails monitoring
- Critical signals monitoring
- Thermal monitoring
- Dual SPI BIOS flash
- RTC reset and Global reset
- Protection for surprise power down
- Memory reliability and availability
- BIOS recovery
- OS recovery
- USB recovery
- EMS and EMI
- Stack-up and PCB consideration
- Solder Joint Reliability

1.1 Terminologies

The following listed terminologies are used in the document.

Table 1. Terminologies

Term	Description
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
HALT	Highly Accelerated Life Testing
DFR	Design for Reliability
UART	Universal Asynchronous Receiver/Transmitter
BIOS	Basic Input Output System

MCU	Microcontroller Unit
EC	Embedded controller
TMSDG	Thermal/Mechanical Specification and Design Guide
PECI	Platform Environment Control Interface
SPI	Serial Peripheral Interface
ME	Manageability Engine
MUX	Multiplexer
RTC	Real Time Clock
G3	Global System State 3. RTC battery power only.
GPIO	General Purpose Input/Output
I2C	Inter-Integrated Circuit
VR	Voltage Regulator
AC	Alternating Current
DC	Direct Current
EoM	End of Manufacturing
TXE	Trusted Execution Engine
IP	Intellectual Property
EHL	Elkhart Lake
ADL-N	Alder Lake-N
ADL-S	Alder Lake-S
KPMU	Intel® Kiosk Peripheral Management Utility
HW	Hardware
SW	Software
USB	Universal Serial Bus
EMC	Electromagnetic Compatibility
EMS	Electromagnetic Susceptibility
EMI	Electromagnetic Interference
ESD	Electrostatic discharge
TVS	Transient Voltage Suppression
PCB	Print Cricut Board
BGA	Ball Grid Array
LGA	Land Grid Array
MAS	Manufacturing Advantage Service
TMDG	Thermal Mechanical Design Guide
NCTF	Non-Critical to Function
SJ	Solder Joint
MRC	Memory Reference Code
IBV	Independence BIOS Vendor
FAT	File Allocation Table
NTFS	New Technology File System
EXT	Extended file system
SSD	Solid State Disk
PEI	Pre-EFI Initialization

UEFI	Unified Extensible Firmware Interface
POST	Power On Self Test

1.2 Reference Documents

The reference documents is listed in the table below.

Table 2. Reference Documents

Title and Link	Location or ID
Telcordia SR-332：2016 Reliability Prediction Procedure for Electronic Equipment	
GJB/Z 35-93：Derating criteria for electrical, electronic and electromechanical parts	
MIL-HDBK-217F: Reliability prediction of electronic equipment	
c3000 dual spi boot flash solution and poc wp	601001
Elkhart Lake Platform Design Guide	599710
Alder Lake N Platform Design Guide	646929
Alder Lake S Platform Design Guide	619508
Intel® Kiosk Peripheral Management (Intel® KPM) Utility - Overview	740544
Intel® Kiosk Peripheral Management Utility 2.0 Design Guide (KPMU 2.0)	735952
Intel® Kiosk Peripheral Management Utility Version 1.5 Design Guide	646176
Alder Lake, Raptor Lake and Raptor Lake-S Refresh Platform Thermal and Mechanical Design Guide	619907
Manufacturing with the Intel® Desktop Processor Family for Socket V0 Including: Alder Lake-S, Raptor Lake-S, Raptor Lake-S Refresh, and PCH	630369
Manufacturing with the Intel® Mobile Platform Code Named Alder Lake	636157
In-Band ECC (IBECC) for the Intel Atom® x6000E series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications - Technical Advisory	621436

NOTE: Other names and brands may be claimed as the property of others. Contact third party representatives for further support.

§

2.0 Overview

Why should a company commit resources for developing high reliability products? The answer is warranty costs and customer satisfaction. Field failures are very costly. Clearly, to be profitable, a company's products must be reliable, and reliable products require a formal reliability process.

The complexities of today's technologies make Design for reliability (DFR)more significant and valuable. Three main reasons include: 1) Product differentiation: As electronic technologies reach maturity, there are fewer opportunities to set products apart from the competition through traditional metrics - like price and performance. 2) Reliability assurance: Advanced circuitry, complicated power requirements, new components, new material technologies make ensuring reliability increasingly difficult.3) Reliability requirements of the customers and application scenarios, such as traffic and industrial control. Design for reliability ensures that products and systems perform a specified function within a given environment for an expected lifecycle.

2.1 Reliability Definition and Index

Definition of reliability is "The probability of a product performing without failure a specified function under given conditions for a specified period of time." Reliability has sometimes been classified as "how quality changes over time." The difference between quality and reliability is that quality shows how well an object performs its proper function, while reliability shows how well this object maintains its original level of quality over time, through various conditions.

2.1.1 Failure Rates

The failure rate is the number of failures in a component or piece of equipment over a specified period.

$$\text{Failure Rate} = \frac{\text{Number of Failures}}{\text{Time}}$$

It is a calculated value that provides a measure of reliability for a product. This value is normally expressed as failures per million hours but can also be expressed as a FIT (failures in time) rate or failures per billion hours. For example, if a component has a failure rate of two failures per million hours, then it is anticipated that the component fails two times in a million-hour period.

- can be defined as the anticipated number of times that an item fails in a specified period.

- This value is normally expressed as failures per million hours, but it can also be expressed as a FIT (failures in time) rate or failures per billion hours.
- A component manufacturer may sometimes provide a specified failure rate usually based on field or laboratory test data.

2.1.2 MTBF

MTBF (Mean Time Between Failures) stands for the average time between two failures of the repairable system, that is the ratio of the cumulative system operation time to the number of failures. This metric is used to measure the stability and reliability of a product. The higher the time between failures, the more reliable the system.

The formula to calculate Mean Time Between Failures is as follows:

$$\text{MTBF} = \frac{\text{Total uptime}}{\text{Number of failures}}$$

1. Total uptime – The total amount of time that the system or components were operating correctly under normal conditions. Usually measured in hours.

2. Number of failures – The total number of times that the equipment broke down unexpectedly.

Here's an example for MTBF. If you have 100 electronic devices. Over the past year, they have broken down a total of 10 times. So MTBF for this equipment is: MTBF=100x365x24 hours/10=87600 hours (about 10 years)

2.1.3 MTTR

Mean Time to Repair (MTTR) is an important failure metric that measures the time it takes to fix failed equipment or systems. By tracking MTTR, organizations can see how well they are responding to unplanned maintenance events and identify areas for improvement.

$$\text{MTTR} = \frac{\text{Total corrective maintenance time}}{\text{Number of repairs}}$$

Here's an example for MTTR.

Let's say you have a piece of electrical equipment. Over the past year, it has broken down a total of 5 times. The time that each repair took was (in hours), 1 hours, 0.5 hours, 2 hours, 0.5 hours, and 2 hours respectively, making a total maintenance time of 6 hours. So MTTR for this equipment is: MTTR=6 hours/5=1.2 hours

Assumptions

In calculating MTTR, the following is generally assumed.

Repairs are carried out by suitably trained technicians.

Technicians have access to the resources they need to complete the repairs.

2.1.4 Availability

Availability is related to reliability and is a measure of how much time a system is performing correctly, when it needs to be. MTBF can be used with MTTR to calculate availability for a system.

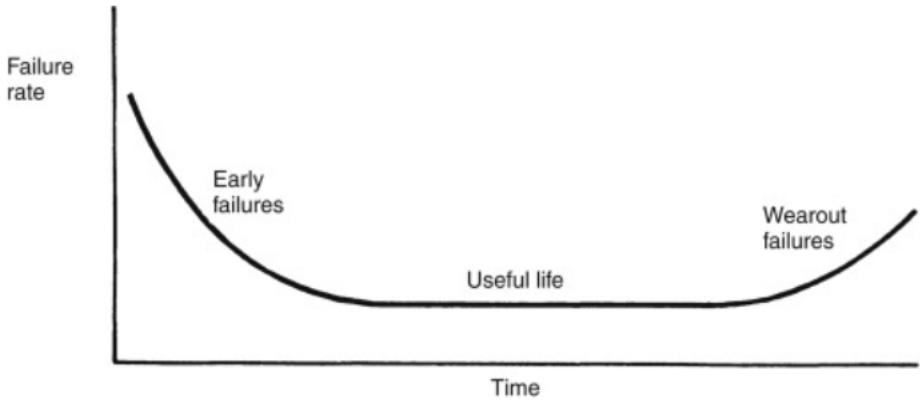
$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF+MTTR}}$$

Here's an example for MTTR. If you have a piece of electrical equipment. MTBF=50000hours (about 5 and a half years), MTTR=1hours.So, Availability for this equipment is: Availability =50000/ (50000+1) =0.99998

2.2 Bathtub Curve

A bathtub curve visually shows the failure rate of a product by plotting their failure occurrences over time. It has three stages: early failures period, useful lifetime period, and wear-out period. The graph goes by the name of 'the bathtub curve' because of its characteristic shape. Note that the highest failure rates correspond to premature failure (early failures), and to end-of life wear out.

Figure 1. Bathtub Curve



- **Early failure**:

The first part of the curve describes early failures. At this stage a high number of failures is seen due to errors in design or manufacturing. The failure rate is decreasing, because the products which have defects and are therefore failing fast are removed

from the population. Early failure can be Reduced by strengthening quality management and environmental stress test.

- **Useful life**

The middle part of the curve describes the useful lifetime of a product. During this period the failure rate is constant. The failures seen are random failures, which can be caused for example due to random external stresses or mishandling of a product.

- **Wear-out failures**

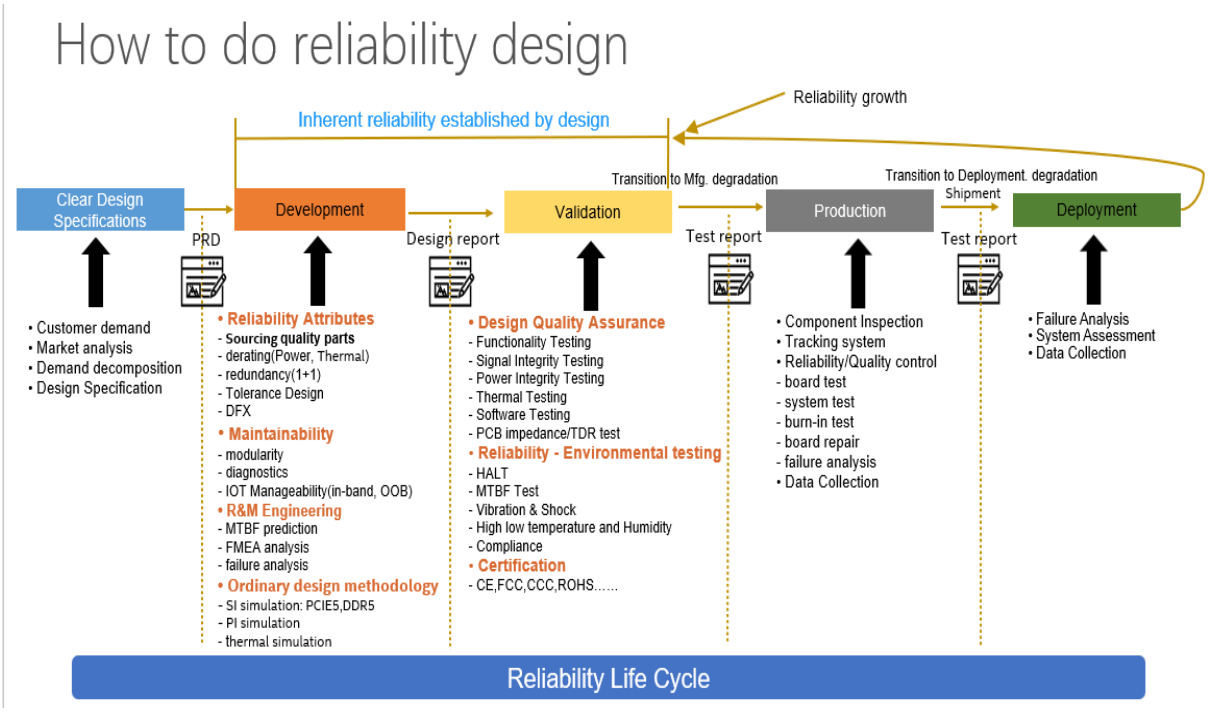
The last part of the curve describes the wear out failures of a product. At this stage the failure rate is increasing, as the aging of components and materials is accelerating the occurrence of failures. At this stage the failures can be caused, for example due to corrosion, oxidation and so on.

The failure rate rule shown by the bathtub curve is not what the customers want. Therefore, it can be said that reliability work is to change the bathtub curve. In other words, the purpose of reliability work is to reduce early failures, extend Useful life and reduce failure rates. Through preventive monitoring and maintenance, ensure the failure rate at wear out period is reduced.

2.3 Design for Reliability Concept

The establishment of product reliability is system engineering. It is an actual process. Specifically, Design for Reliability (DFR) describes the entire set of tools that support product and process design (typically from early in the concept stage all the way through to product obsolescence) to ensure that customer expectations for reliability are fully met throughout the life of the product with low overall life-cycle costs. The life cycle of an electronic product is divided into five stages which include Define Design specification, Development, Validation, Production and Deployment. The inherent reliability of a product is established in design and validation stages. Some factors may be introduced into the production process to affect reliability. Therefore, the manufacturing process should ensure consistency as much as possible. Although we have done a lot to ensure the quality and reliability of the product in design and validation stages, customers may still find some problems after the product is deployed in the actual working environment. Currently, we need to figure out the root cause. Then reflect and review the previous design and verify stages, and think about how to optimize the product, to further improve the reliability of the product.

Figure 2. How To Do Reliability Design



- Define Design Specification

The builder of product should clear and identify the customer demand in defining design specification stage. Maybe we need to do some market analysis and research. In short, a clear product specification is required in this phase.

- Development

In the development of a product, it is important to ensure its reliability in the design stage, which enables the concept of reliability throughout the full life cycle of product design, operation, and maintenance. Some methods and measures should be adopted to ensure the reliability of products in the development phase. Common methods include derating design, redundancy design, tolerance design. MTBF prediction is also necessary in the design stage. With the progress of technology, the signal rate on the circuit board is faster and faster, such as PCIE5 and DDR5, to ensure signal integrity, some simulation work is necessary. Thermal factor is an important aspect that affects the reliability of the device, so the thermal design of the product is very important. The lower the device temperature, the better reliability of the device.

- Validation

Validation is an important part in the product building process. Through test validation, we found some defects. Solving these defects and problems to ensure the reliability and quality of products. Validation tests usually include function test, signal integrity test, power integrity test, thermal test, software test, PCB TDR test and Compliance test. Some environmental stress validations are also necessary. For example, High or low

temperature and Humidity test, Vibration & Shock test, HALT (Highly Accelerated Life Testing) test, and so on.

- Production

In the production and manufacturing process, it is critical to ensure the consistency of product delivery via a lot of test work. For example, board test, system test, burn-in test.
Generally, an electronic product has thousands of electronic components. To ensure the quality of these components, supply chain management is also very important.

- Deployment

The actual deployment environment of the product is not equal to the lab test environment, so the product may still meet some problems in the deployment phase. We should collect data, analyze data, and then improve the previous design plan, test plan, and manufacturing plan to improve the reliability of products.

2.4 System Reliability Validation

As for Environmental adaptability, Environmental stress test and reliability validation, you could follow the standards below as a reference. Some test items are optional, not mandatory, such as MTBF identifying, HALT, Low air pressure test and so on. ODM/OEM can select the appropriate validation items according to the use condition of the products.

- The relevant standards of environmental stress are only a reference, not a basis/ judgement. You could spend some time understanding the test criterion.
- ODM/OEM could make a test plan for products, according to the use conditions of the products and standards listed pervious.
- Based on the experimental purpose, experimental principle, product characteristic and economy, consider the test stress.
- Selecting Environmental test items includes four aspects: test items choosing, test condition choosing, test procedure / step choosing and test sequence choosing.

For more validation information, please refer to
743956_NEX_IoT_Customer_Product_Validation_Handbook

Table 3. Reliability Standards

	IEC/MIL	GB	Validation Items	Category	Reference Notes
1	IEC 60068-2-1	GB/T2423.1	Low Temperature	Temperature	Storage, Operating, Power up Low Temperature-65~5°C;Duration 2/16/72/96h
2	IEC 60068-2-2	GB/T2423.2	High Temperature		Storage, Operating, Power up High Temperature:30~1000°C;Temperature change rate:3-5°C/min Duration:2/16/72/96/168/240/1000h
3	IEC 60068-2-14 IEC 60068-2-78	GB/T2423.22	Thermal Cycling Thermal Shock		Temperature change rate 1-5°/min, Cycling times 2~10(maybe 1000 Cycling) Shock: Temperature change rate 20-30°/min, Cycling times 5~10(1000 Cycling)
4	IEC 60068-2-3	GB/T2423.3	Damp heat, steady state	Humidity	Temperature 30/40°C;Humidity 85/93;Duration 12h/24h; 2/4/10/21days
5	IEC 60068-2-30	GB/T2423.4	Damp heat, Cyclic		Temperature 40/55°C;Humidity variety ;Cycling times 2~56
6	IEC 60068-2-6	GB/T2423.10	Sine Vibration	Vibration, Shock	frequency 0.1-5000Hz;0.1-5Grms;3 axes
7	IEC 60068-2-64	GB/T 2423.11	Random Vibration		frequency 20hz-5000Hz;3 axes
8	IEC 60068-2-27	GB/T 2423.5	Shock		half sine wave;2-26ms;1~1000Grms
9	IEC 60068-2-32	GB/T2423.8	Free Fall		fall with Package, fall w/o Package, drop times(5-30),Height(46-122cm),Drop angle
10	IEC 60068-2-13	GB/T2423.21	Low air pressure	Others	air pressure(variety with height) Duration:5min/30min/2h/4h
11	IEC 60068-2-11	GB/T2423.17/18	Salt mist		5% NaCl, Ph 6.5-7.2, Temperature 15-35°， Duration 48h
12	IEC 60529	GB/TGB-4208	Sand and Dust Test		level 3<2.5mm(Particle diameter)， level 4, <1mm, level 6
13	MIL-STD-781	GJB899A GB/T5080.7	MTBF identifying	Reliability	Time Censored Test, Sequential Test Method and Failure Censored Test, choose a Mature experimental scheme Sufficient experimental time and samples must be considered MTBF test is optional, not mandatory.
14	IEC 62506	GB/T 29309 GB/T 34986	HALT Test(Highly Accelerated Life Testing)		Temperature step stress-40~100° Vibration stress; Combined Environment HALT test is optional, not mandatory.

2.5 MTBF Prediction Methodology

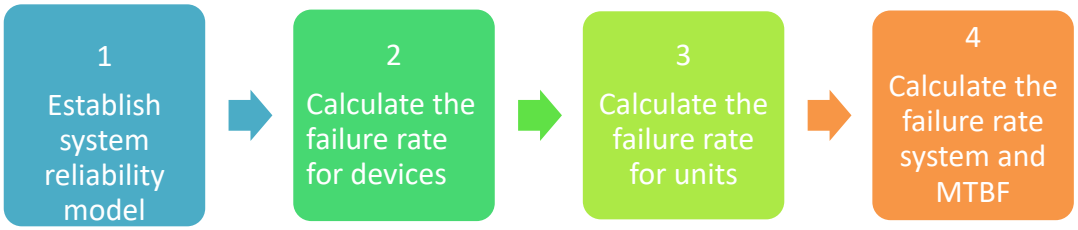
Reliability prediction methodology allows you to assess the reliability of your design prior to production. Reliability predictions enable you to build products with confidence. They assist in deciding which product to purchase from a list of competing products. As a result, it is essential that reliability predictions be based on a common procedure.

MIL-HDBK-217F and Telcordia SR-332 are the most popular MTBF prediction standards. Prediction using MIL-HDBK-217 or Telcordia® SR-332 provides a front-end look at mean time between failures. The model can predict MTBF using as little as the part type and count information. MIL-HDBK-217 is useful for both military and commercial electronics. Telcordia SR-332 prediction models address commercial electronics only.

2.5.1 Flow of Reliability Prediction

The reliability index MTBF can be predicted according to the following process. The failure rate of the unit or system is calculated first, and then converted to MTBF

Figure 3. Reliability Prediction Diagram



1. The reliability prediction unit is divided first, and then the system reliability model is established. The reliability model is generally series structure.
2. Calculate the failure rate of components in each unit.
3. Sum the failure rates of various components in the unit to obtain the failure rate of the whole unit.
4. According to the reliability model of equipment and system, the MTBF and other reliability indexes of the system can be obtained by level prediction

2.5.2 Steady State Failure Rate Prediction for Devices

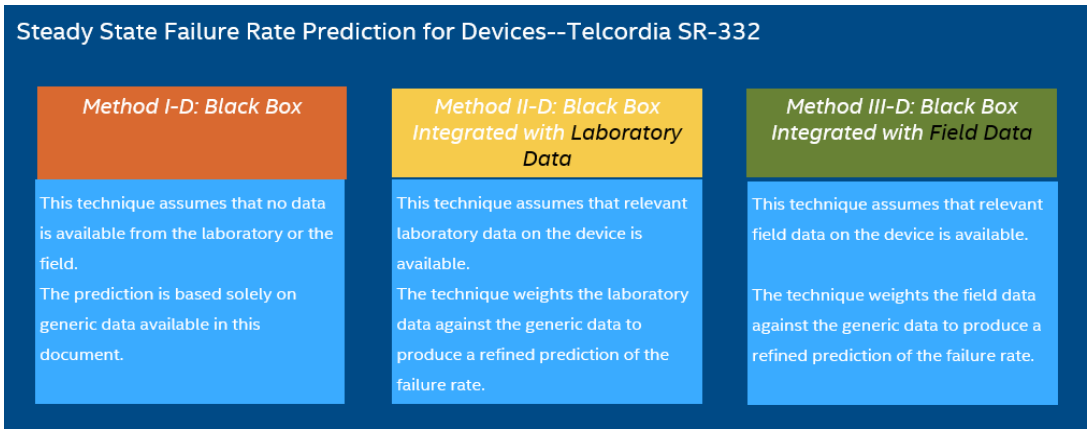
Depending on the amount of data available, the steady-state failure rate for device can be predicted using one of three techniques:

1.Method I-D: Black Box
This technique assumes that no data is available from the laboratory or the field. The prediction is based solely on generic data available in this document.

2. Method II-D: Black Box Integrated with Laboratory Data
This technique assumes that relevant laboratory data on the device is available. The technique weighs the laboratory data against the generic data to produce a refined prediction of the failure rate.

3.Method III-D: Black Box Integrated with Field Data
This technique assumes that relevant field data on the device is available. The technique weighs the field data against the generic data to produce a refined prediction of the failure rate.

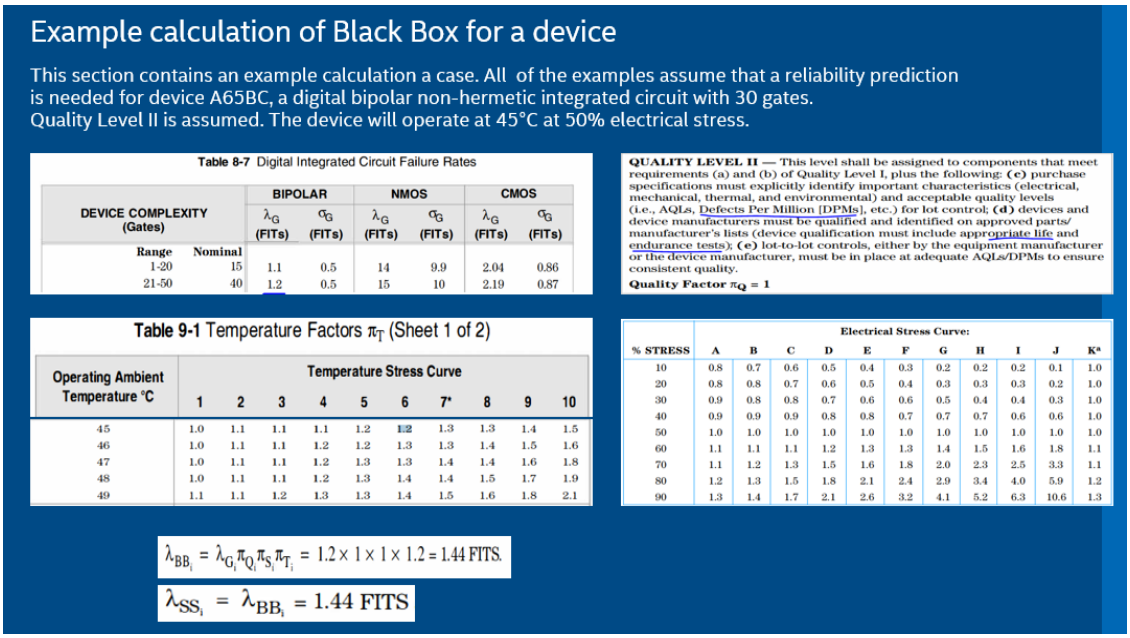
Figure 4. Failure Rate Prediction Method



Note that all three techniques require a black box prediction of the failure rate. The additional data in the other two techniques are used to improve the accuracy of the prediction for a particular device. Reliability Prediction Procedure attempts to use all the data available to improve the accuracy of the prediction. Device manufacturer's data, unit supplier's data may be particularly useful in adjusting Method I estimates for new technology devices where no substantial field data exists.

Here is an Example calculation of Black Box for a device A65BC. For more detail, please refer to Telcordia SR-332:2016

Figure 5. Example Calculation of Black Box



λ_{Gi} = mean generic steady-state failure rate for device i

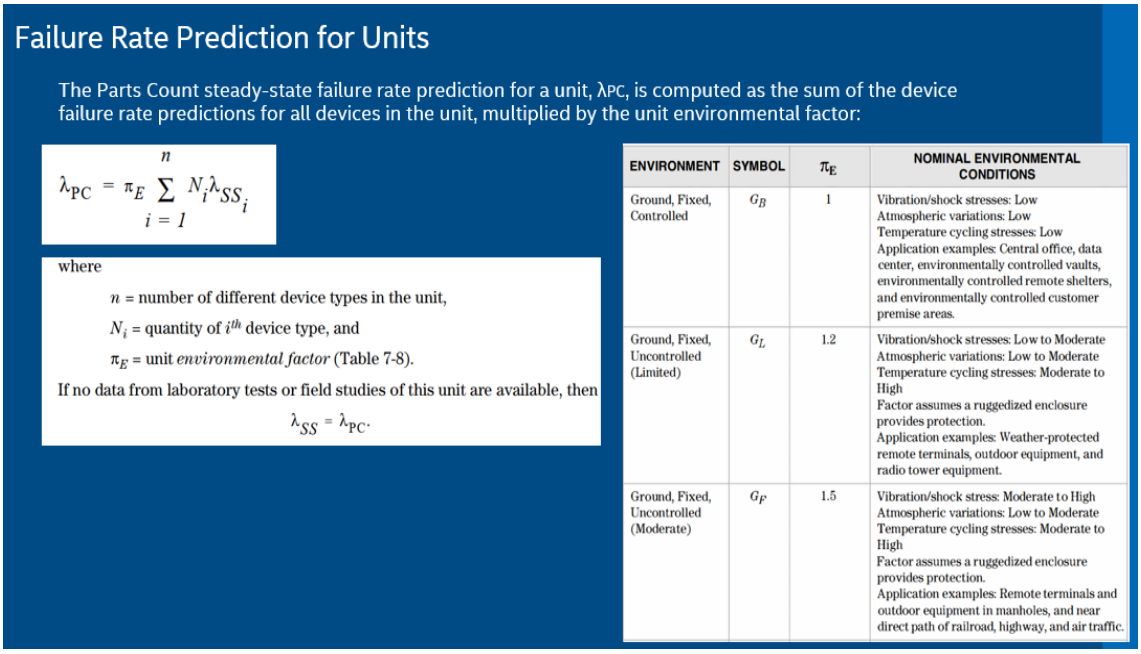
λ_{BBi} = the black box steady-state failure rate for device i
$\prod_{Qi}$ = Quality Factor for device i
$\prod_{Si}$ = Electrical Stress Factor for device i based on the percent electrical stress. If stress is unknown, use 1, which assumes 50% electrical stress.
$\prod_{Ti}$ = Temperature Factor for device i based on normal operating temperature during the steady state. If the temperature is unknown, use 1, which assumes 40°C.

2.5.3 Failure Rate Prediction for Units

The Parts Count steady-state failure rate prediction for a unit, λ_{PC} is computed as the sum of the device failure rate predictions for all devices in the unit, multiplied by the unit environmental factor.
When we get the failure rate for one unit, we can get the unit MTBF value through the following formula.

$\text{MTBF} = 10^9$ hours/Fits

Figure 6. Failure Rate Prediction



Note: for more details, please refer to Telcordia SR-332:2016

§

3.0 Derating for Electronic Component

Derating is the selection of components and materials according to a set of standardized safety-margin definitions. Derating increases the margin of safety between part design limits and applied stresses, thereby providing extra protection for the part. By applying derating in an electrical or electronic component, its degradation rate is reduced. Reliability and life expectancy are improved. Intuitively, if a component or system is operated under its design limit, it will be more reliable than if it is operated at or above the design limit.

Rating

Allowable maximum stress value of components.

Stress

Usually, failure happens when the applied load exceeds the strength. Load and strength should be considered in a general way. For electronic parts, "load" might refer to voltage, power or an internal stress such as junction temperature. "Strength" might refer to any resisting physical properties.

Stress ratio :

It is common to consider stress and strength (and hence “stress ratio”) to be point values. For example, consider a tantalum capacitor with an applied working voltage of 9V. If the maximum rated voltage (“strength”) is 10V, then the stress ratio can be calculated as:

$$\text{Stress Ratio} = \frac{\text{Applied Voltage}}{\text{Max Rated Voltage}} = \frac{9V}{10V} = 90\%$$

it might be concluded that the design is adequate since the applied stress is less than the maximum rated stress (stress ratio < 1.0)

3.1 Components Derating Standards

GJB/Z 35-93, published by National Defense Science, Technology and Industry Commission, derating criteria for electrical, electronic and electromechanical parts.

MIL-STD-975, published by NASA, focuses on selection of parts used in the design and construction of space flight hardware as well as mission-essential ground support equipment.

MIL-STD-1547, published by the Department of Defense, is targeted to aid in the design, development and fabrication of electronic systems with long life and/or high reliability requirements while operating under the extreme conditions of space and launch vehicles.

3.2 Derating Level

GJB / Z 35-93 divides the derating of components into three levels. The specific division is as follows:

Table 4. Derating Level and Comparison

	Level I	Level II	Level III
Derating degree	MAX	Mid	Min
Applicable conditions	Failure causes personal injury or serious damage to equipment	Failure causes damage to equipment	Failure don't cause damage to equipment
	Really High reliability requirements	High reliability requirements	General reliability requirements
	Equipment unable or unsuitable for maintenance	High maintenance costs	Low maintenance costs
	Poor thermal condition	/	/
	New technologies and processes are adopted	Some special designs	Mature standard designs
derating design implement	hard	Mid	easy
Derating increase cost	High	Mid	low

3.3 Example of Derating Design

Different components have different derating parameters. Different derating levels have different derating factors. The following table shows the derating parameters and derating factors of several different components. Refer to GJB/Z 35-93：Derating criteria for electrical, electronic and electromechanical parts for more detailed information.

Table 5. Derating Degree

Component Category			Derating Parameters	Derating Degree		
				I	II	III
IC	Analog	amplifier	Power voltage	0.7	0.8	0.8
			Input voltage	0.6	0.7	0.7
			Output current	0.7	0.8	0.8
			Power(W)	0.7	0.75	0.8
			MAX TJ(°C)	80	95	105
		comparator	Power voltage	0.7	0.8	0.8
			Input voltage	0.7	0.8	0.8
			Output current	0.7	0.8	0.8
			Power(W)	0.7	0.75	0.8
			MAX TJ(°C)	80	95	105
		Voltage regulator	Power voltage	0.7	0.8	0.8
			Input voltage	0.7	0.8	0.8
			Output current	0.7	0.75	0.8
			Output input voltage difference	0.7	0.8	0.85
			Power(W)	0.7	0.75	0.8
			MAX TJ(°C)	80	95	105
		Analog Switch	Power voltage	0.7	0.8	0.85
			Input voltage	0.8	0.85	0.9
			Output current	0.75	0.8	0.85
			Power(W)	0.7	0.75	0.8
			MAX TJ(°C)	80	95	105
			Frequency	0.8	0.9	0.9
			Output current	0.8	0.9	0.9

	Digital circuit	Bipolar transistor	MAX TJ(°C)	80	95	105

Table 6. Derating Degree (cont.)

Component Category			Derating Parameters	Derating Degree		
				I	II	III
IC	Digital circuit	MOS FET	Power voltage	0.7	0.8	0.8
			Frequency	0.8	0.9	0.9
			Output current	0.8	0.9	0.9
			MAX TJ(°C)	80	95	105
large-scale integrated circuit			MAX TJ(°C)	Optimize heat dissipation and reduce TJ		
resistor	Thin film resistor		voltage	0.75	0.75	0.75
			Power(W)	0.5	0.6	0.7
capacitor	MLCC		DC Power voltage	0.5	0.6	0.7
			TAM (°C)	TAM-10	TAM-10	TAM-10
	Aluminum electrolytic capacitor		DC Power voltage	-	-	0.75
			TAM (°C)	-	-	TAM-20
Inductor			Hot spot temperature (THS)	THS-(40~25)	THS-(25~10)	THS-(15~0)
			Operation current	0.6~0.7	0.6~0.7	0.6~0.7
			Transient current	0.9	0.9	0.9
			Operation voltage	0.7	0.7	0.7
Connector			Operation voltage	0.5	0.7	0.8
			Operation current	0.5	0.7	0.85
			Hot spot temperature (THS)	THS-50	THS-25	THS-20

3.4 Component Selection Criteria

- The product shall be in strict accordance with the enterprise's Component Selection Manual, and the universal components that have been reliably used and verified in other products shall be selected as far as possible.
- The components with national and industrial standards should be considered first. Try your best to reduce the number of parts.
- Try to replace discrete devices with integrated IC.
- Preferably select components with good anti-electromagnetic interference performance and small parameter dispersion.
- The device shall be of industrial grade (According to product specifications), with the operating temperature range of - 40 ℃ - 85 ℃, to ensure the low temperature and high temperature startup characteristics.
- The use of components should be considered to comply with the national military standard GJB/Z35-93 Derating Criteria for Components, and the derating level shall be level I to ensure the system margin.

§

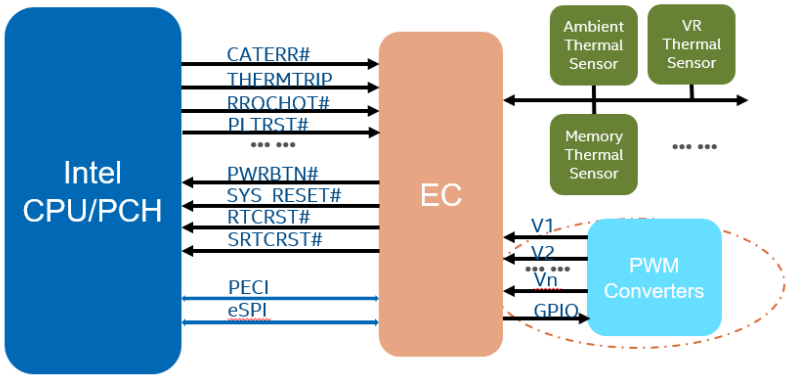
4.0 Power Rails Monitoring

The stability of power rails is very important to the reliability of the system. Monitoring power rails' value is necessary to improve or forecast reliability and health of the system. As the central device of monitoring, EC monitors key power rails, Such as PVCCIN, P1V8, P1V05, P3V3, PVDDQ and so on. if the monitored voltage exceeds the threshold (for example, +/-7% of nominal voltage), EC will take actions for management (below are only for example, ODM/OEM can implement their own design):

- Log the error
- Alarm

You could refer to the Monitoring flow in section 6.2 for power rails monitoring procedures.

Figure 7. Power Rails Monitoring



Key Components
Intel CPU/PCH - Intel CPU with PECI Interface and Platform Control Hub (PCH).
EC - Embedded controller for system Monitoring.
Power Supply Voltage Monitor - a system hardware monitor with ADC

There are many chips for power supply voltage monitors such as AMC80 which is Low power local temp sensor with fan speed and power supply voltage monitor. Customers choose the right components according to their own application scenario and supply chain. If MCU or EC have the function of voltage monitoring, there is no need for additional monitoring chips.

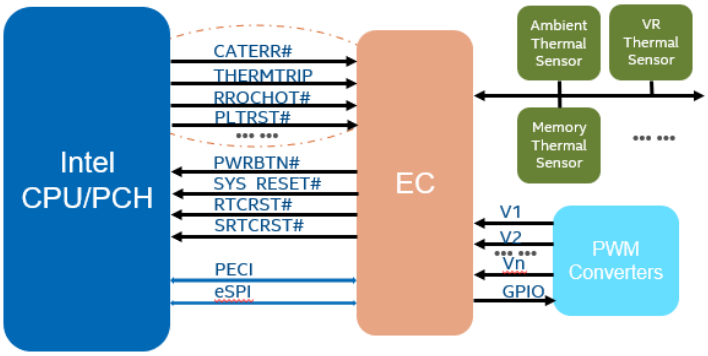
§

5.0 Critical Signals Monitoring

EC Monitor the critical signals of the platform to know the health status of the system. If the EC finds an abnormal signal, timely alarm and inform people to maintain in advance to reduce the probability of failure. This is great significant to improve the reliability of the system.

You could refer to the Monitoring flow in section 6.2 for critical signals monitoring procedures.

Figure 8. Critical Signals Monitoring



Key Components

Intel CPU/PCH- Intel CPU with PECI Interface and Platform Control Hub (PCH).

EC- Embedded controller for system Monitoring.

EC monitors the critical signals (such as CATERR#, THERMTRIP#, PLTRST#, etc.). If an abnormal status of those signals is encountered, EC will take actions for management (below are only for example, customer can implement their own design):

- Log the error
- Alarm

You could refer to the Monitoring flow section for critical monitoring procedures.

§

6.0 Thermal Design and Monitoring

A large number of engineering practices show that the temperature has a significant impact on the reliability of electronic products. Too high a temperature will greatly increase the failure rate of components. The thermal design of electronic products refers to controlling the temperature of all electronic devices inside the products to make them work at the maximum allowable temperature.

There are two methods to reduce components temperature. One is to reduce the temperature of components through derating design. The second is good thermal design to reduce the temperature of components, so as to improve reliability of electronic products.

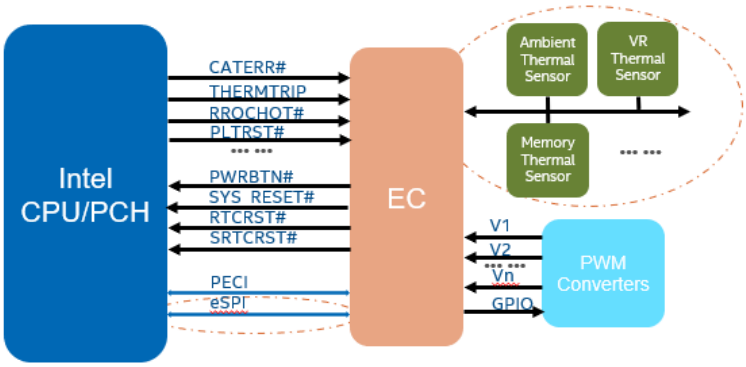
6.1 General Principles of Thermal Design

- Try to reduce various thermal resistances to achieve heat dissipation as soon as possible.
- Thermal design shall be carried out simultaneously with electrical and mechanical design.
- The product size, weight, heat consumption, circuit layout and maximum allowable temperature of components shall be considered.
- Put temperature sensitive components at low temperature place.
- You could refer to the Intel TMSDG document for specifications and guidelines for the design of thermal and mechanical solutions on different platforms.

6.2 System Thermal Monitoring

The temperatures of the platform are monitored by the management unit EC on the board to achieve temperature management, give early warning and improve the stability of the product. As the central device for monitoring, EC collects the temperature value of each component to determine whether it exceeds the device specification. If it exceeds the device specification, record the log, trigger an alarm, or take more stringent measures.

Figure 9. System Thermal Monitoring



Key components

Intel CPU/PCH- Intel CPU with PECI Interface and Platform Control Hub (PCH).

EC- Embedded controller for system Monitoring.

Ambient thermal sensor- digital temperature sensors for thermal Monitoring.

EC monitors the system temperature, including below parts temperature, but not limited.

- CPU & PCH Temp
- Ambient/VR/Memory

EC manages the system thermal strategy with actions (below are only for example, customer can implement their own design) according to the reading temps.

- Throttling
- Log the hot event
- Alarm
- Power down

The temperature data of intel CPU is delivered over PECI, in response to a GetTemp() command, and reported as a relative value to TCC activation target. The temperature data reported over PECI is always a negative value and represents a delta below the onset of thermal control circuit (TCC) activation, as indicated by the PROCHOT# signal. Therefore, as the temperature approaches TCC activation, the value approaches zero degrees.

For temperature monitoring and system control management purposes, the PECI 3.1 commands that are commonly implemented include Ping (), GetDIB(), GetTemp(), TCONTROL and TjMAX(TCC) read. The TCONTROL and TCC read command can be implemented by utilizing the RdPkgConfig() command

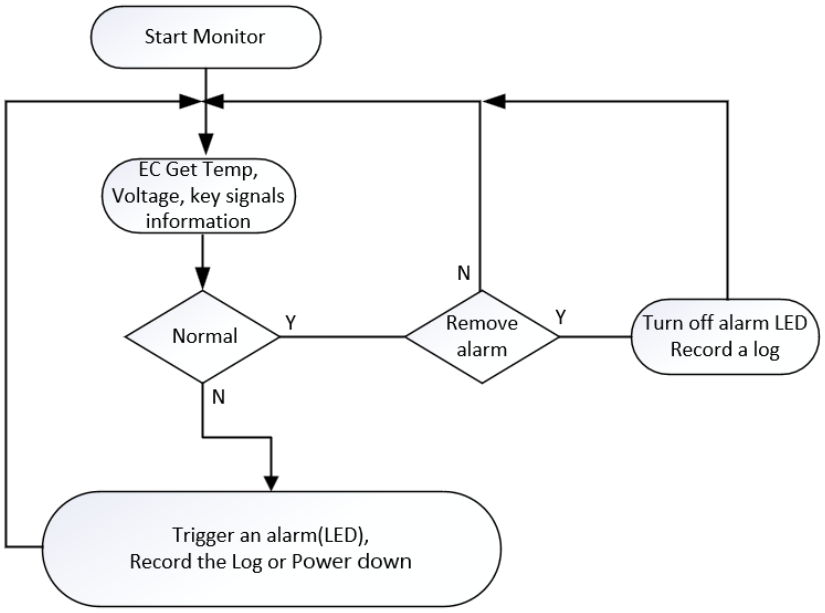
There are many digital temperature sensors for thermal Monitoring such as LM75A which is a digital temperature sensor and thermal watchdog with Two-Wire Interface.

Customers choose the right components according to their own application scenario and supply chain. If MCU or EC have the function of temperature sensors, there is no need for additional monitoring chips.

Monitoring Flow

The following figure shows an example of monitoring procedures. After the system is powered on, the EC monitor constantly obtains the information of temperature, voltage value, and critical signals status on the board. If there is any abnormality, EC monitor could choose to trigger the alarm, record the log and power down. If it is found that the monitored object changes from abnormal to normal, the EC determines whether the alarm should be clear, and then continues to monitor.

Figure 10. Monitoring Flow



§

7.0 Dual SPI Boot Flash Introduction

In common IA hardware design, one SPI boot flash image (including descriptor, ME FW and BIOS etc.) is enough to boot the system and run the system smoothly. Intel also provides a Platform Design Guide (PDG) for one SPI flash design for each platform, but a traditional one flash system cannot boot normally in the below cases due to a lack of redundant design:

- Flash image is damaged
- Boot flash is physically broken

Dual SPI boot flash is a necessary tolerance design to make the system more robust and stable. Even if one SPI boot flash is corrupted, the system can still boot normally with another SPI flash image, especially for IA based equipment deployed in harsh environments.

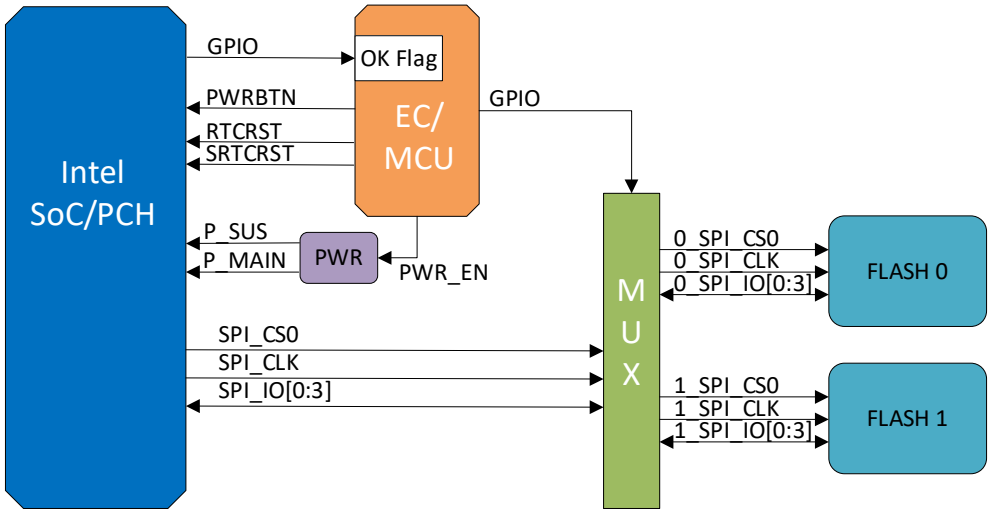
7.1 Value Provided by the Dual SPI Boot Flash Solution

The Dual SPI boot flash solution can provide more value compared to the traditional one flash BIOS solution:

- Slave boot flash image boot successfully
- Quick system recovery with catastrophic boot error
- Improved Reliability and Availability make system stay operational when boot error occurs

7.2 Dual Boot Flash Solution

Figure 11. Hardware Architecture



7.2.1 Hardware Architecture

1. Key Components Include:
   - Intel SoC/PCH: IA Platform component including SPI controller.
   - EC/MCU: control the dual boot flash switching.
   - MUX: SPI interface switches between two flashes. MUX component selection:
     - Analog switch with ps level delay
     - Bandwidth > 100MHz
   - Flash 0/1: SPI Master (Flash 0) and Slave flashes (Flash 1) for system boot
2. EC/MCU functions:
   - OK Flag: BIOS set this flag with GPIO or UART/I2C. It indicates master flash boot successfully and do not trigger flash switching for slave flash boot.
   - Timer: set the timer value according to the BIOS boot up time.
   - PWR_EN & RESET Control: Enable the IA system power off/on, reset PWRBTN, RTCRST and SRTCRST.
   - MUX Switch: GPIO controls switching the SPI interface to difference SPI flashes.

3. Operation Mode

   Normal Mode:

   Flash 0 is connected to SoC/PCH SPI CS0/CLK/IO (master), Flash 1 is not connected. Host can access Flash 0 by default.

   Backup Mode:

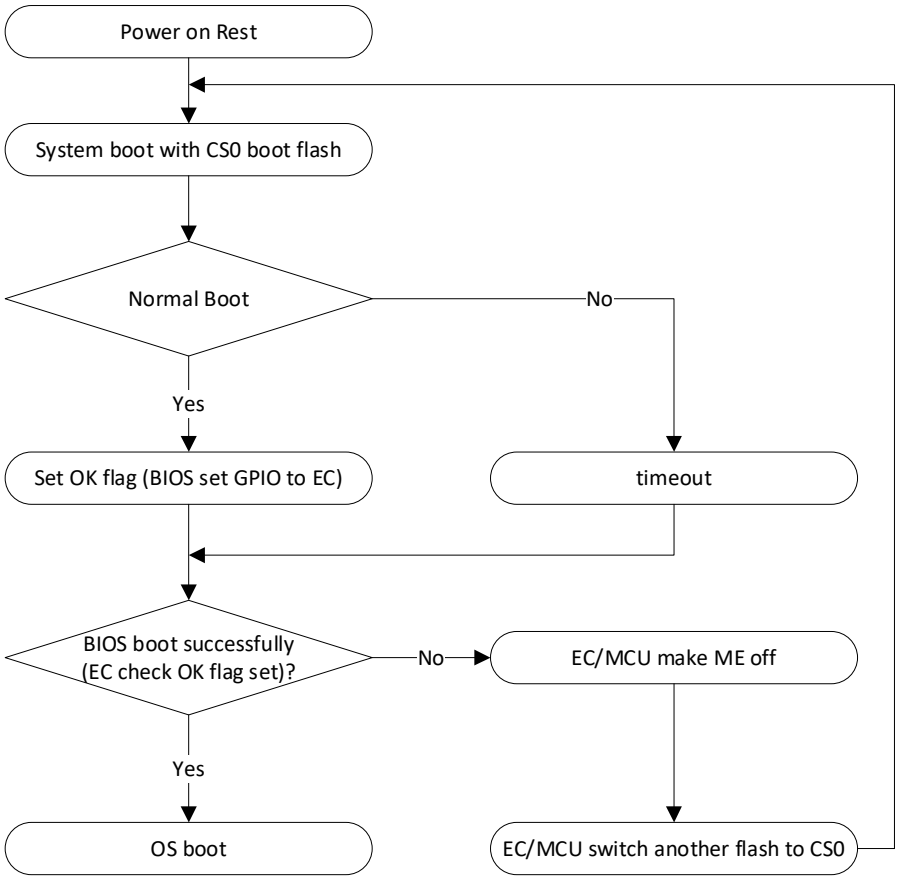
   If EC/MCU detects master BIOS flash boot failure (OK flag is not set within some time), it automatically powers off IA followed by BIOS flashes switching (Flash 1 is connected to CS0/CLK/IO) and system boot with Flash 1.

7.2.2 Software

BIOS need set OK flag to EC/MCU after normal boot to indicate master BIOS flash successful boot and no slave BIOS flash recovery boot required.

7.3 Dual Boot Flash Solution Working Flow

Figure 12. System Boot Flow



EC/MCU make ME off: ME is still working in S5 state, to avoid old ME FW accessing new flash part during switching, there are several methods:

1. EC/MCU triggers the RTC reset and global reset.
2. EC/MCU assert PWRBTN 6 seconds.
3. EC/MCU power off IA system and then power on.

Suggest customer keep these 3 methods. We recommend use method 3 to power off the IA system, then switch to another flash and power on.

§

8.0 RTC Reset and Global Reset

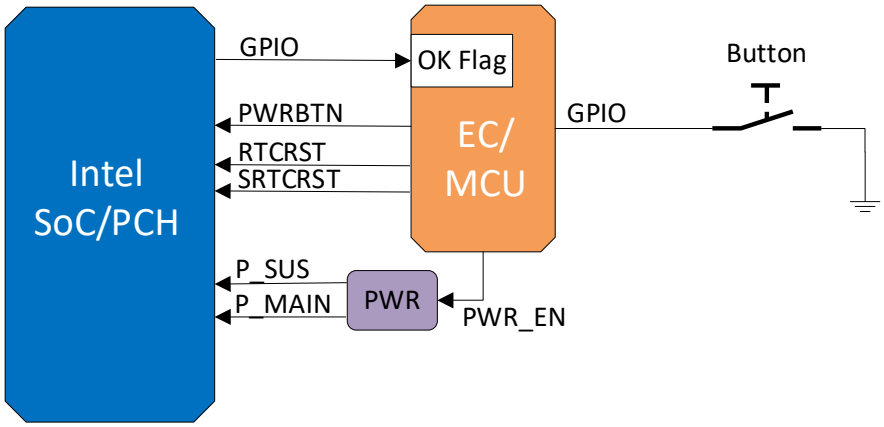
In some cases, the system with dual SPI boot flash still can't boot up, it's likely caused by RTC region corruption.

We should reserve a button in front panel, it can perform RTC reset (RTCRST, SRTCRST) or power cycle without open the chassis.

Notes: RTC reset is only done in G3 power state.

8.1 Reset Hardware Diagram

Figure 13. Reset Hardware Diagram



8.1.1 EC/MCU Functions

- OK Flag: BIOS set this flag with GPIO or UART/I2C. It indicates system boot successfully.
- Timer: set the timer value according to the system boot up time.
- PWR_EN & RESET Control: Enable the IA system power off/on, reset PWRBTN, RTCRST and SRTCRST.
- Button Input: receive button input and take actions.

8.1.2 Operation Process

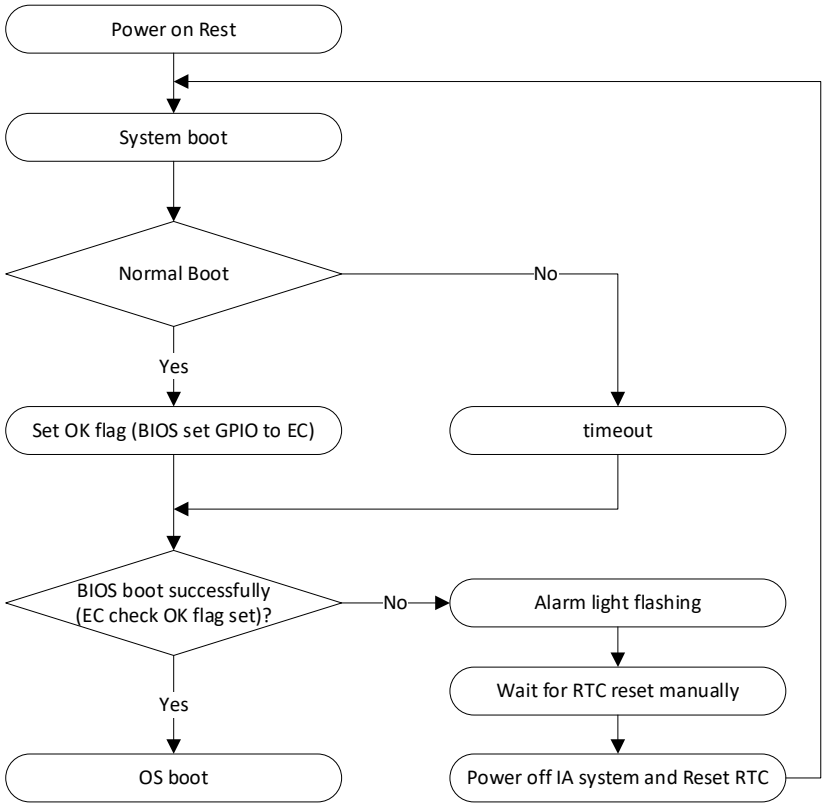
While booting up, EC/MCU can't receive OK Flag from CPU for a long time. The timer in EC/MCU will be timeout, there are some actions that can be implemented according to the requirement:

- Alarm light flashing.
- Press Button, EC/MCU can power off the system, then reset RTCRST/SRTCRST, and power on the system.

8.2 Reset Working Flow

The figure below shows the detailed reset working flow.

Figure 14. Reset Working Flow



§

9.0 Protection for Surprise Power Down

The main goal of the various power down timing specification is to ensure proper isolation between the associated power well and the RTC well to guarantee that RTC contents are not accidentally corrupted. There are many events that could cause a surprise power down. The following is a short list of some events, but is not exhaustive:

- VR failure (over current, over voltage, IC failure, and so on)
- AC removal with no DC Battery present
- Removal of the primary battery

The focus of this section is on the unexpected power removal caused by user interaction, which could be an end user, factory technicians and system level induced power down that removes all power from PCH.

To ensure RTC is not corrupted, the platform must de-assert the appropriate power good signals BEFORE the rails go out of their defined tolerance range.

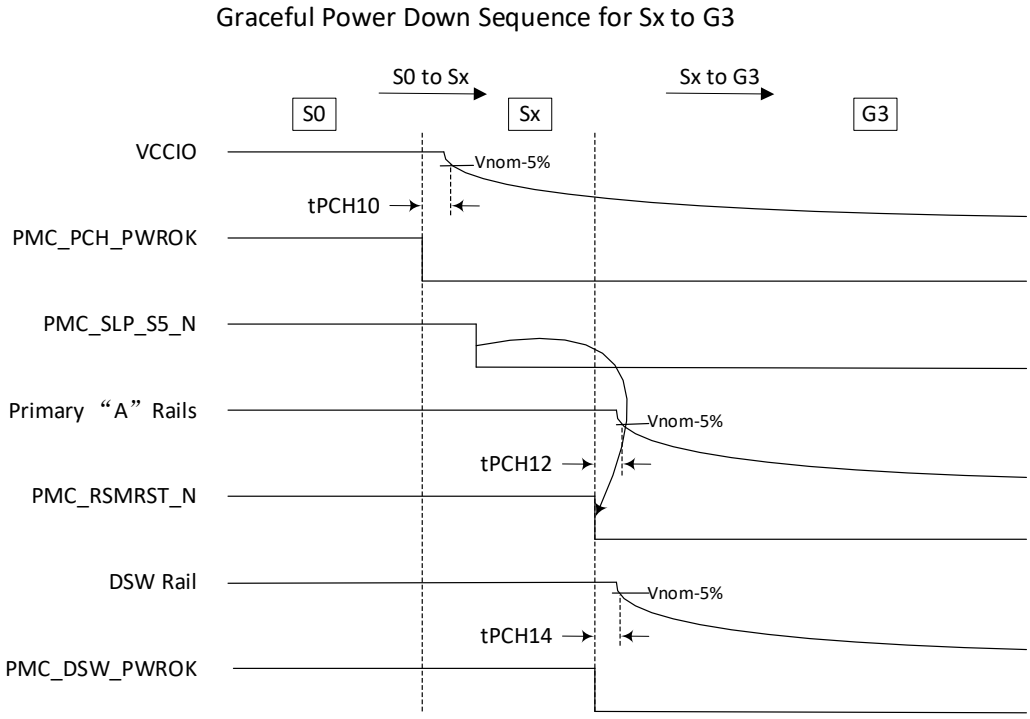
This implies that the platform should monitor the highest voltage available which is usually the main power supply like the battery voltage to determine when it has dropped too low and VR failure/shutdown is eminent. At that point, the PCH power good signals (PMC_PCH_PWROK, PMC_RSMRST_N, PMC_DSW_PWROK) should be driven Low before their associated rails turn off and droop below the defined tolerance.

Below power loss diagrams are from Elkhart Lake Platform Design Guide (PDG), other platforms maybe little different, please check the corresponding PDG.

Graceful Power Loss means the normal process, e.g., press Shut Down in Windows, or command in Linux. Emergency or Surprise Power Loss means unexpected power removal.

9.1 Graceful Power Loss Requirement

Figure 15. PMC_DSW_PWROK Requirement for Graceful Power Loss



For graceful shutdown from Sx to G3 each power OK goes low **before** its respective rails reach the lower limit of their tolerance band (-5% for rails ≥ 1.0V and -50mV for rail <1.0V).

Under these conditions the platform must meet all of tPCH10, tPCH12, and tPCH14. This is required to ensure the RTC well will be properly isolated. Failure to meet this requirement could result in RTC corruption and unexpected PCH behavior. Note that, Primary A rails commonly refer to V1P8A and V3P3A.

Notes:

1. The minimum timing between PMC_PCH_PWROK to PMC_SLP_S5_N is 60us. Then, the PMC_RSMRST_N should be driven low once PMC_SLP_S5_N is asserted.

2. It is recommended that the system should pull PMC_RSMRST_N and PMC_DSW_PWROK low at the same time when going to G3. Pulling PMC_RSMRST_N low before PMC_DSW_PWROK is permitted if VCC_3P3A_DSW remains powered & tPCH14 still is met.

3. Timing Parameters:

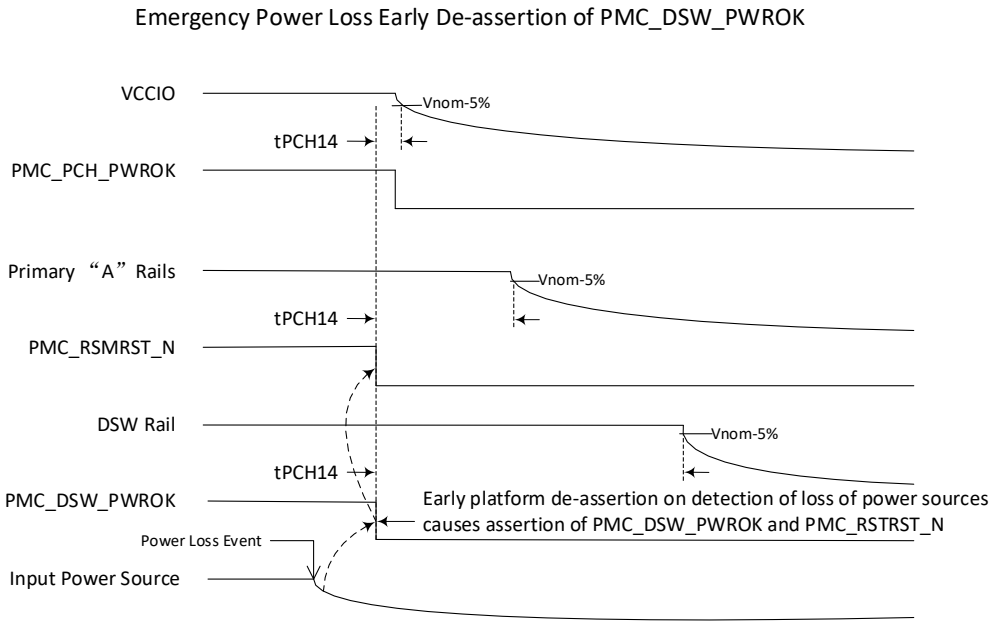
a) tPCH10 ≥ 1us

b) tPCH12 ≥ 100ns

c) tPCH14: ≥ 400ns

9.2 Emergency (Surprise) Power Loss Requirement

Figure 16. PMC_DSW_PWROK Requirement for Emergency Power Loss



For emergency power loss, if PMC_DSW_PWROK and PMC_RSMRST_N go low tPCH14 **before** any of the VCCIO, PCH Primary, or PCH DSW rails are below spec (-5%), the RTC well will be properly isolated, and tPCH10 and tPCH12 do not need to be met. PMC_RSMRST_N must go low with PMC_DSW_PWROK.

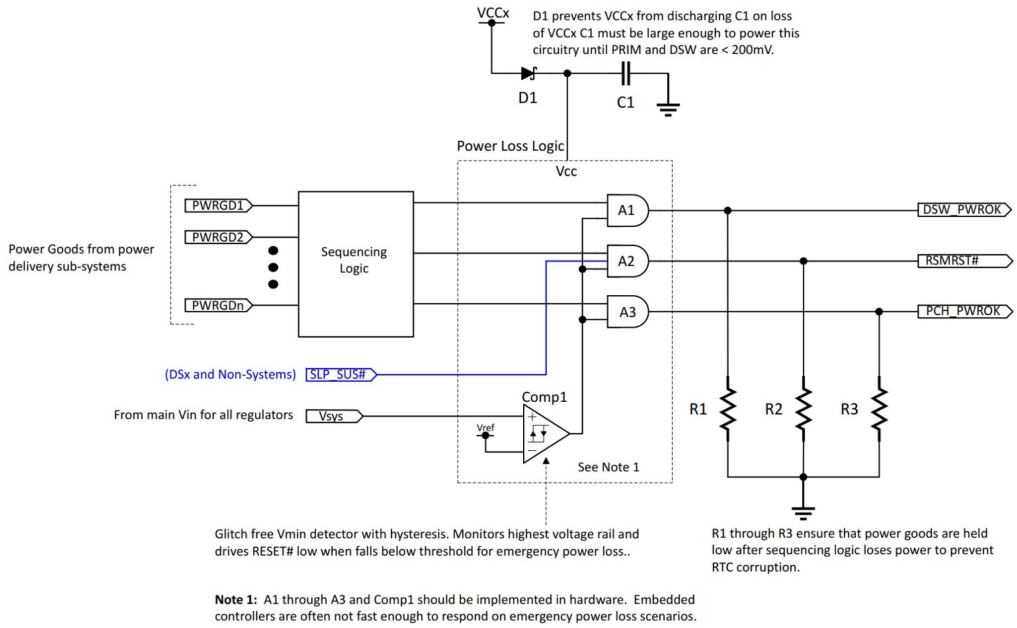
For this case tPCH14 is measured from PMC_DSW_PWROK low each of the following rails:
VCCIO @ -5%
Primary Rails @ -5%
DSW rails @ -5%

All must meet tPCH14 requirements.

9.3 Emergency (Surprise) Power Loss Implement Example

The figure below shows such possible examples of architectural implementation for ensuring that the PWROK go low and are locked out before the rails go out of spec on any emergency power loss. This figure is from ADL-N PDG.

Figure 17. Emergency Power Loss - PWROK Requirement



9.4 EoM (End of Manufacturing)

EoM (End of Manufacturing) is a MUST whether Intel® CSME features are in use or not.

9.4.1 EoM Importance

- It is crucial to understand that even if customers do NOT have any specific requirements for Intel® CSME, following the manufacturing flow and executing EoM must be done, so the system would not be exposed to various security threats.
- Intel® CSME supports a range of security configurations and technologies as: Intel® Platform Trust Technology (Intel® PTT), Boot Guard, Content Protection, Fuses, SPI Access and more.
- By following the Intel® CSME Manufacturing flow and executing the EoM command, these security configurations are locked, hence preventing potential Denial of Service (DoS) attacks on the system.

- Failing to follow the End of Manufacturing (EoM) flow exposes the system to various security vulnerabilities including DoS.

9.4.2 EoM Performs

EoM Flow will perform as the following:

- SPI Flash Region Lock: Even a one-bit change in the SPI descriptor or IFWI can prevent a system from booting. By locking the SPI region, user can prevent from Host SW from modifying flash content containing all the critical system firmware and prevent potential DoS.
- Move from Development to Production Mode: Development Mode allows issuing certain commands and enabling features which should be locked on production systems. Example, reading debug data which can disclose restricted information and may expose various system vulnerabilities. By moving the system to Production Mode, debug data is locked and can be exposed only in an authorized manner.
- Locking the Field Programmable Fuses (FPFs): FPFs are HW fuses which are one time programmable and are locked at EoM. Failing to set EoM can leave the fuses unlocked which can lead to a change in the un-programmed FPFs values. Example, FPFs can control the system boot source. Changing the boot source can lead the system to a no boot scenario. By locking the FPFs during the EoM flow, changes to the FPF values are not possible hence keeping the system more secured.

- SW/HW binding: During EoM when FPT -closemnf is issued, PCH is bounded with NVM.

9.4.3 EoM Flow

EoM is performed by one of the following options:

- Option 1: One time command via FPT command (FPT- closemnf)
- Option 2: Automatically after first boot (Dedicated pre-configuration in the IFWI)

Important Note:
Prior to executing the EoM command, customers should be familiar with the Intel® CSME manufacturing flow, the various security configurations set by CSME, and understand how it can impact their platform.

One time command to run the EoM flow
EOM flow will not be triggered during 1st boot, customer could control the platforms for production debug and manufacturing process.

§

10.0 Memory Reliability and Availability

Mission critical systems like Industrial controllers need higher Reliability and availability. DRAM and the interface are one of the major sources that could cause errors in those critical systems.

Sources of data errors:

- Data stored in DRAM is susceptible to corruption caused by cosmic rays from outer space and alpha particles from materials the computer system is constructed out of.
- Parts, circuits, and connectors can fail.
- Data corruption can occur during transmission on the bus.

10.1 Memory Reliability

10.1.1 Memory Reliability Introduction

Error correction codes protect against undetected data corruption and are used in computers where such corruption is unacceptable, examples being scientific and financial computing applications, or in database and file servers.

ECC can also reduce the number of crashes in multi-user server applications and maximum-availability systems. And ECC scheme also helps to correct single bit errors and detect double bit errors and machine check.

10.1.2 Memory Reliability Solution

For without additional ECC device, In-Band ECC also can provide ECC protection by using a portion of DRAM space is reserved to store ECC data.

Both ECC/In-Band ECC can be enabled by BIOS at boot time, In-Band ECC is available on select Elkhart Lake and Tiger Lake-UP3 SKUs and above.

ECC Enablement in Setup Menu:

- ECC: Boot system to BIOS, in ‘Intel advanced menu’ under ‘memory configuration, set “ECC” –> Enabled.
- In-Band ECC: Boot system to BIOS, in ‘Intel advanced menu’ under ‘memory configuration, set “In-Band ECC Support” –> Enabled.

Refer to the *In-Band ECC (IBECC) for the Intel Atom® x6000E series, and Intel® Pentium® and Celeron® N and J Series Processors for IoT Applications* and *11th Gen Intel® Core™ Processors for IoT Platforms In-Band ECC (IBECC)* for additional details on In-Band ECC.

10.2 Memory Availability

10.2.1 Memory Availability Introduction

"Memory Disable" allows fault handling in BIOS MRC (Memory Reference Code) to keep system available during memory Training.

10.2.2 Memory Availability Solution

Define a CMOS address which can be used to record Channel number need to be disabled: MRC_CHANNEL_DISABLE_CMOS_ADDR (0x4A), for example.

Figure 18. MRC CHANNEL DISABLE CMOS Defined Figure

```
#define MRC_CHANNEL_DISABLE_CMOS_ADDR (0x4A)
///< Memory channel disable, 0 = all enabled, 0xFF = all disabled.
///<  [Bit7:0] Mc1Ch3, Mc1Ch2, Mc1Ch1, Mc1Ch0, Mc0Ch3, Mc0Ch2, Mc0Ch1, Mc0Ch0
```

Once MRC training fails, record the failed MC number and Channel number to CMOS MRC_CHANNEL_DISABLE_CMOS_ADDR and reset system.

Figure 19. Record Failed MC/Channel to CMOS Figure

```
{
  UINT8         DisableChannel = 0;
  DisableChannel = MrcCall->MrcRtcCmos (MRC_CHANNEL_DISABLE_CMOS_ADDR);
  DisableChannel = DisableChannel | (Controller * MAX_CHANNEL + Channel);
  MrcCall->MrcRtcWriteCmos (DisableChannel, MRC_CHANNEL_DISABLE_CMOS_ADDR);
  (*PeiServices)->ResetSystem2 (EfiResetCold, EFI_SUCCESS, 0, NULL);
}
```

During system reboot, read CMOS value from MRC_CHANNEL_DISABLE_CMOS_ADDR and skip the related McxChx's MRC training.

Figure 20. MRC Read Disabled Channel from CMOS Figure

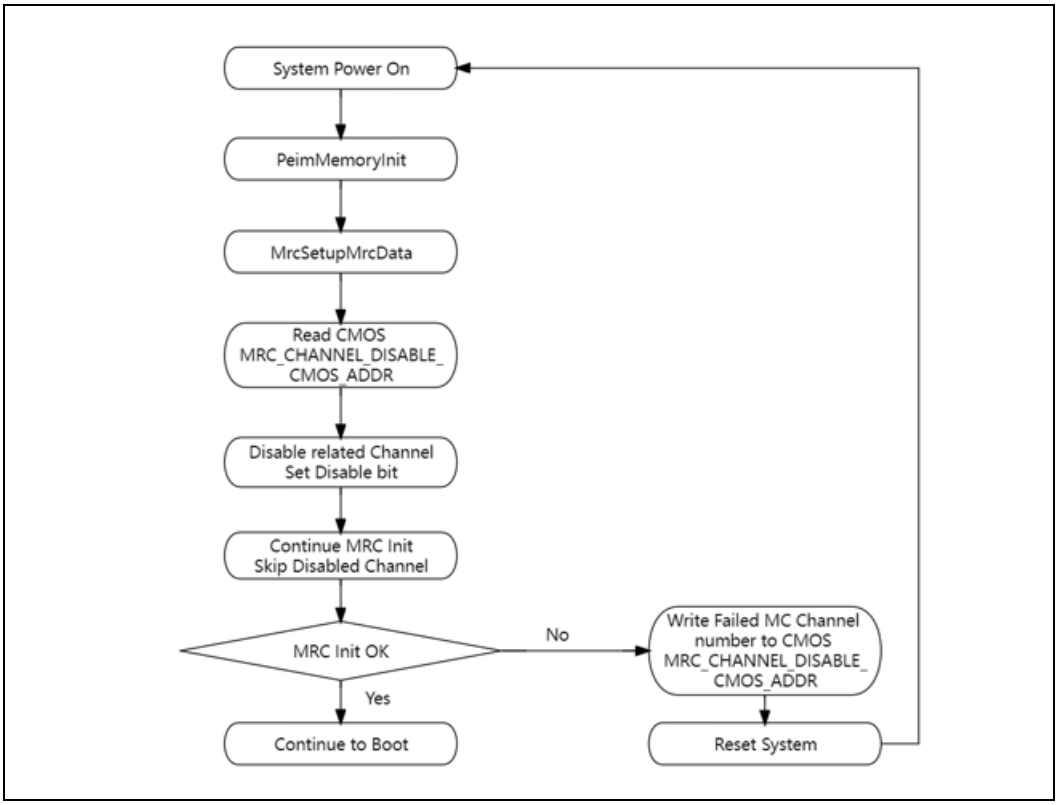
```
// Read DisableChannel from CMOS
*DisableChannel = MrcCall->MrcRtcCmos (MRC_CHANNEL_DISABLE_CMOS_ADDR);
```

Figure 21. MRC Skip the Channel Before MRC Training Figure

```
for (Controller = 0; Controller < MAX_CONTROLLER; Controller++) {
  ControllerIn = &Inputs->Controller[Controller];
  ControllerIn->ChannelCount = 0;
  for (Channel = 0; Channel < MAX_CHANNEL; Channel++) {
    ChannelIn = &ControllerIn->Channel[Channel];
    if ((DisableChannel >> (Controller * MAX_CHANNEL + Channel)) & 1) {
      ChannelIn->Dimm[0].Status = DIMM_DISABLED;
      ChannelIn->Dimm[1].Status = DIMM_DISABLED;
      ChannelIn->Status         = CHANNEL_DISABLED;
      ChannelIn->DimmCount      = 0;
    }
  }
}
```

10.2.3 Memory Availability Workflow

Figure 22. Memory Availability Workflow Figure



10.3 Conclusion

Memory training and testing fail are common issues encountered, ECC/In-Band ECC and Disable failed channel can help you out in these situations.

11.0 BIOS Recovery

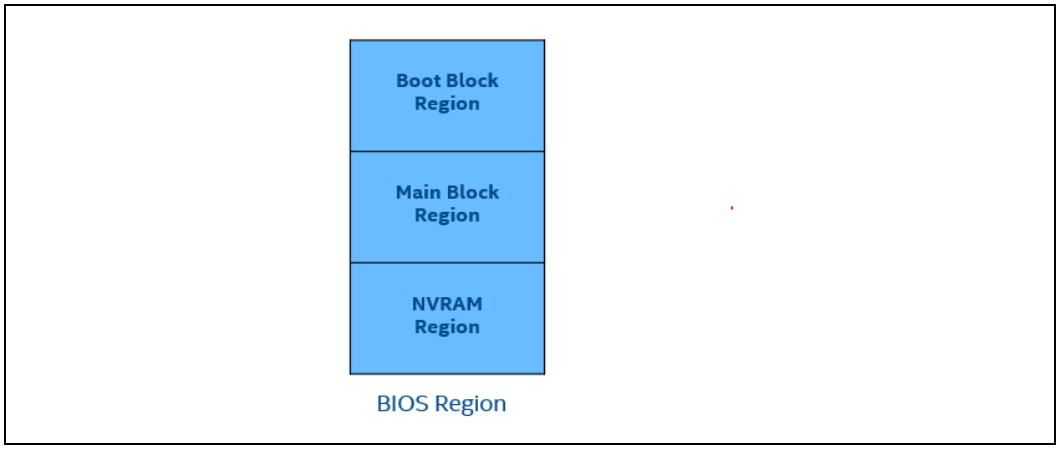
When BIOS region is corrupted, the system can be recovered automatically after BIOS Recovery. For more details and a total solution, you may contact your BIOS vendor (IBV).

11.1 BIOS Recovery Introduction

Recovery is a BIOS function that allows BIOS Recovery automatically when BIOS Main block region corrupted. The BIOS must have the Boot Block section of the BIOS in a non-corrupted state. This means that BIOS recovery will execute normally through the Boot Block phase of execution. If this is not possible, then the code used to perform a recovery may also be corrupted and therefore recovery is not possible.

11.2 BIOS Recovery Solution

Figure 23. BIOS Region Layout Figure



BIOS has “boot block", a portion of the BIOS which runs first and must be updated separately. This code verifies if the rest of the BIOS is intact before transferring control to it.

If the boot block detects any corruption in the main BIOS, it will typically warn the user that a recovery process must be initiated by booting from removable media (SSD/HDD, or USB flash drive) so the user can try flashing the BIOS again.

The Recovery software will detect any corruption in the main BIOS and set the Boot Mode to indicate that the Recovery option has been invoked and then the system attempts to find the recovery image.

Once recovery mode has been invoked, the system will attempt to find the BIOS update file on the different media types that are enabled during porting. Once the Bios Update file has been found, the system will load that image into memory and boot from the new recovery image.

BIOS Recovery Implementation Steps:

- BIOS Boot Block can boot normally.
- BIOS Boot Block detects any corruption in the main BIOS.
- If any corruption is detected, BIOS Recovery mode would be invoked, and System BIOS will be recovered automatically.

11.2.1 Hardware Architecture

None

11.2.2 Software

BIOS Boot Block detects any corruption in the main BIOS. If any corruption is detected, BIOS Recovery mode would be invoked, BIOS needs to implement several PEI Drivers to support to enumerate recovery and find recovery file.

11.2.2.1 BIOS Implementation

BIOS Recovery Implementation needs BIOS to provide PEI Drivers to detect USB/SSD/HDD devices and found FAT/NTFS/EXT file system.

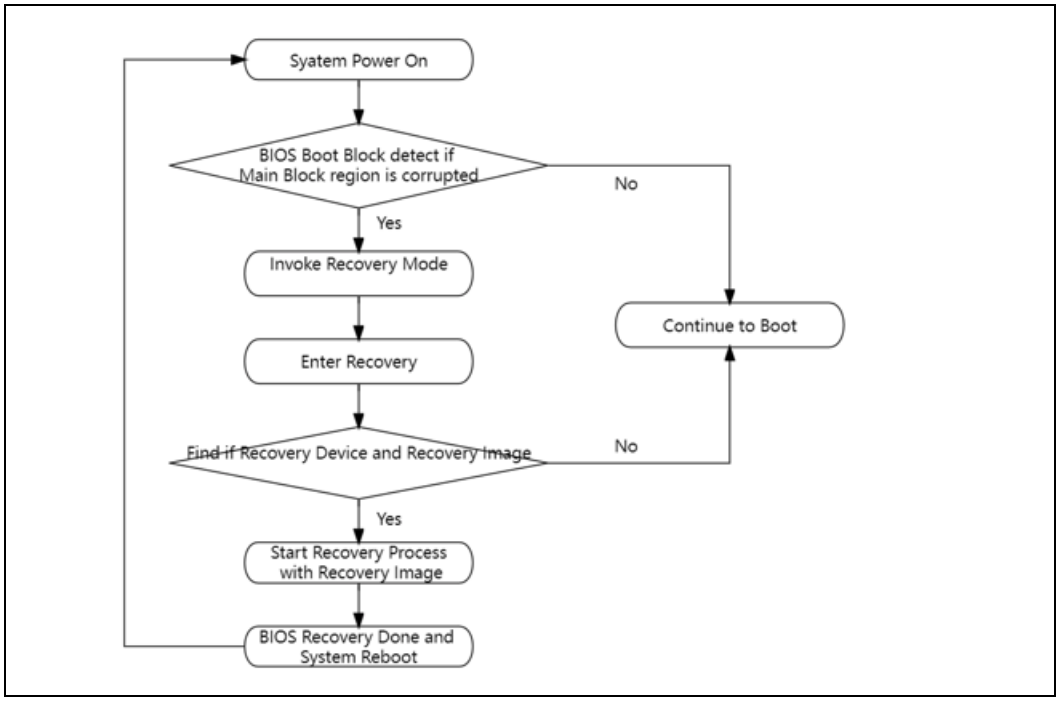
11.2.2.2 Device Support

Devices for BIOS Recovery Support:

SSD/HDD
USB Flash Drives

11.3 BIOS Recovery Workflow

Figure 24. BIOS Recovery Workflow Figure



11.4 Conclusion

BIOS Recovery allows System Recovery automatically when BIOS Main block region corrupted. It is easy and safe to restore System BIOS.

§

12.0 OS Recovery

System crashes and boot failure are common issues encountered; One Key OS Recovery can help you out in these situations. It is easy and safe to restore the operating system. When your computer fails to boot, you can restore it to a normal state easily by pressing the hot key during system startup. For more details and a total solution, you may contact your BIOS vendor (IBV).

12.1 OS Recovery Introduction

One Key OS Recovery is software preloaded, designed to back up and restore your computer. To utilize the features of the One Key Recovery system, the hard disk already includes a hidden partition from the factory to store the system recovery image file. The system recovers image file stored in a hidden partition to avoid any unwanted deletion or modification.

With it, you can restore the system to factory default in case of a system failure or take backup and create factory recovery partition for easy restoration as required. And the system provides users with a specific recovery key to boot your computer when it crashes, F11, for example.

12.2 OS Recovery Solution

OS Recovery is used to recover computer systems. When your computer operating system goes wrong, you can restore your system with OS Recovery. If you don't create any backup before, you can only choose to restore to its factory status. If you backup this system ever, you can choose to restore tore the backup status. Every coin has two sides, so does OS Recovery.

12.2.1 The Advantage of OS Recovery Solution

As just mentioned above, it can help common users to back up systems. When System OS crashes, users can use OS Recovery to restore the system by pressing One Key.

It is less complicated than reinstalling the system. Users don't have to prepare DVD/CD, USB, or some other software.

12.2.2 The Disadvantage of OS Recovery Solution

It will occupy the space of the system. There must be a recovery partition hidden in the computer, and it mainly contains the system image. When you start OS Recovery, the system image will work and the system that you backed up before will restore from hidden partition to drive C.

12.2.3 Hardware Architecture

None

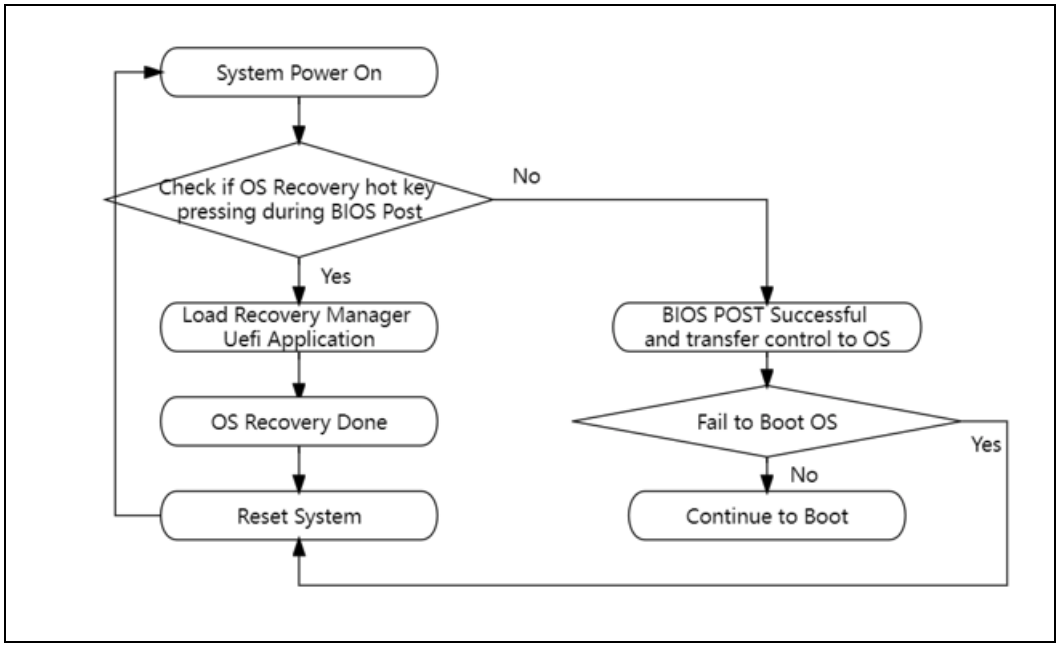
12.2.4 Software

BIOS code needs to modify for enable OS recovery:

- Enable hotkey for recovery manager, BIOS will detect if monitor hotkey is pressed during BIOS POST.
- BIOS is responsible for loading recovery manager.
- Recovery manager is a UEFI application which performs OS Recovery.

12.3 OS Recovery Workflow

Figure 25. OS Recovery Workflow Figure



§

13.0 USB Recovery

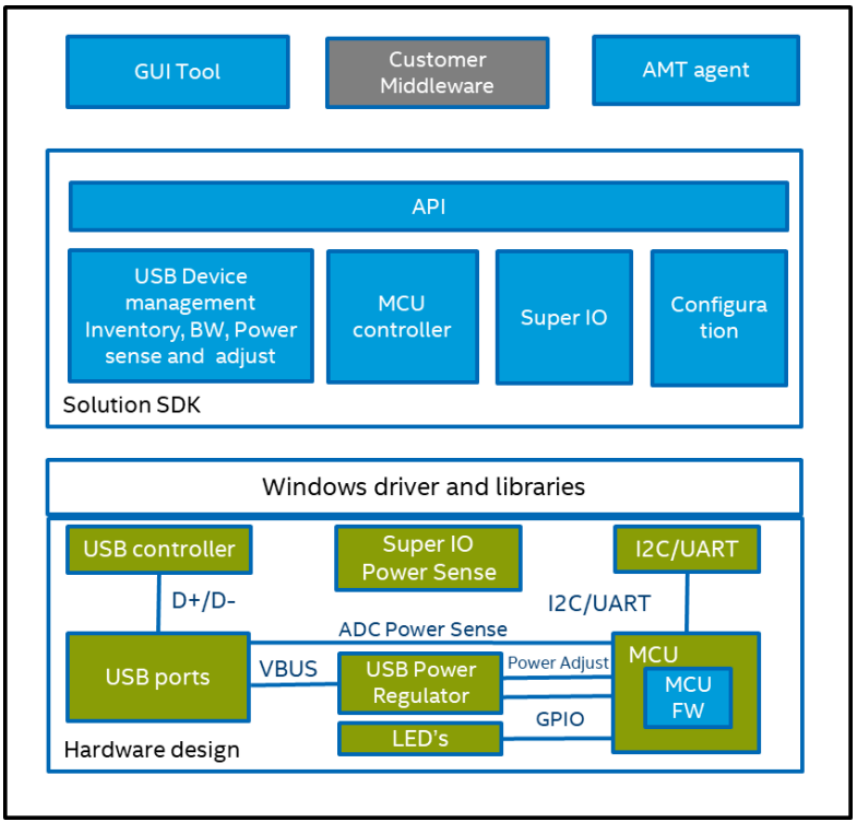
13.1 System Design Overview

USB interface is widely used on motherboard and USB peripheral devices misfunction (such as device missing, yellow mark and etc.) is encountered occasionally if the system runs for a while, a simple USB device unplug/plug activity which is performed on the site by user/maintenance/service technicians would easily resolve it.

To simulate the USB device, unplug/plug activity with add capabilities to manage (including monitor, alert, reset, adjust USB power supply, and etc.) USB ports will significantly improve system reliability by mitigating potential failures caused by USB peripheral devices.

Intel® has developed a hardware reference I/O board design to detect USB port/device status and perform power switch control to reset devices connected to specific ports. The reference solution includes both Software (SW) application and Hardware (HW) design implications as mentioned below in the concept overview.

Figure 26. Intel KPMU Concept Overview



13.2 Hardware Reference Design

Currently many board designs share the same USB power supply for several USB ports, which means that there is no way to control the USB power separately.

To manage a specific USB port/device, a specific design should be implemented by every single port/device to control the USB port power (Vbus). To achieve this, one port dedicated MCU (KPMU1.5) or PCH (KPMU2.0) is used to perform the control via many GPIOs, and a separate USB Vbus power regulator is designed for every port.

The following block diagram shows the reference design for customers' implementation reference. It covers different types of USB ports: native USB ports from the host, USB ports from a discrete USB hub, and USB ports from PCIe*-to-USB bridge.

The reference design is independent of the platform or types of USB ports (either native or bridge/hub).

Figure 27. KPMU1.5 HW Reference Design Block Diagram

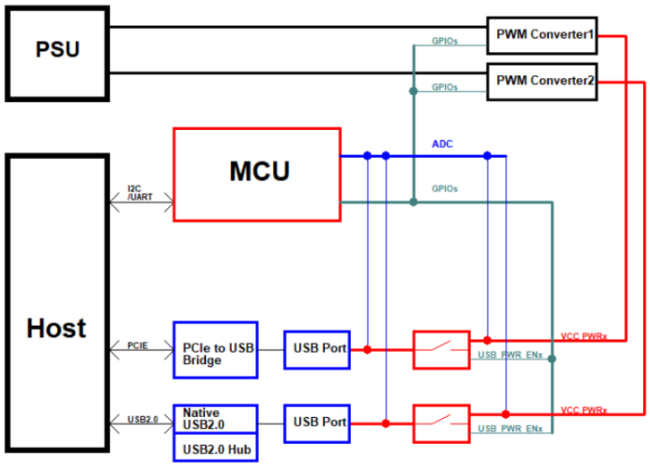
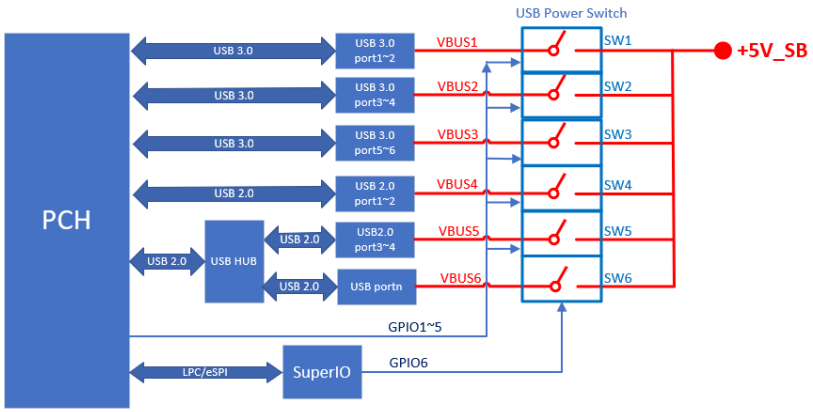


Figure 28. KPMU2.0 HW Reference Design Block Diagram



13.3 Software Design Architecture

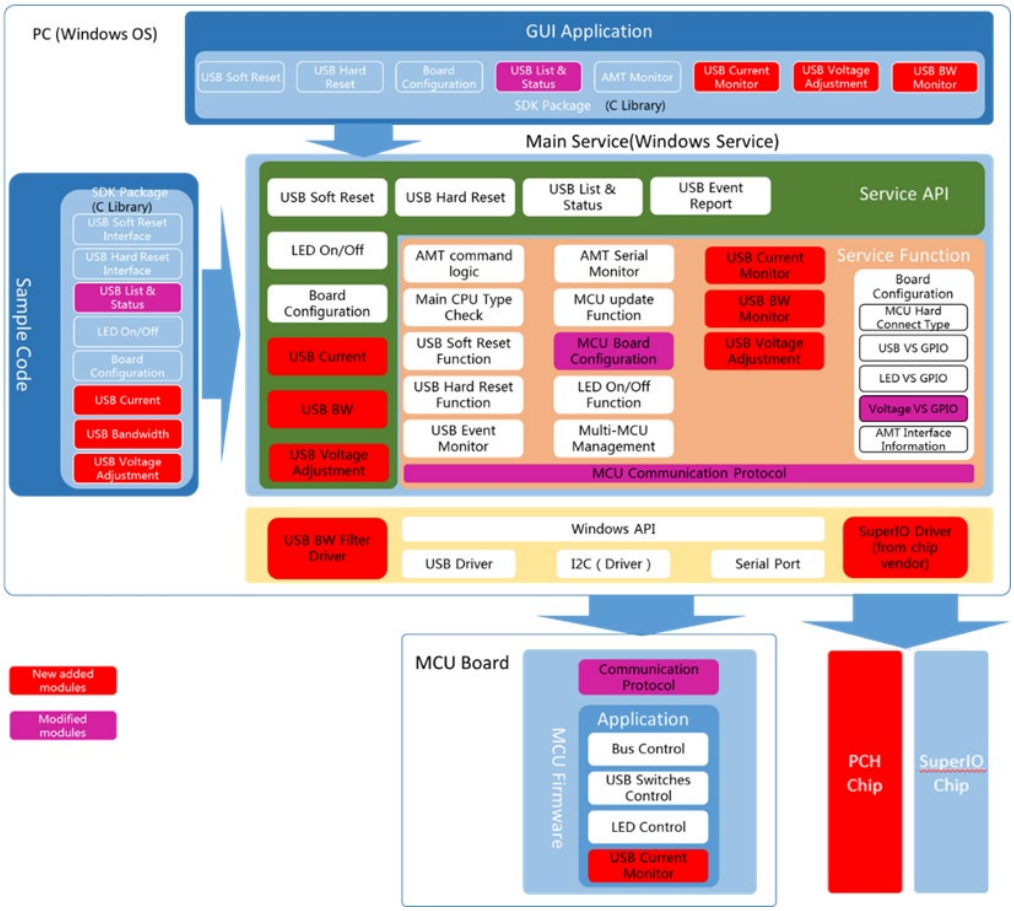
1. There are four layers for the software, from bottom to top they are: MCU firmware, communication HW driver with Windows API, Windows Services, Applications (GUI application, sample code application with library)

2. Serial port protocol and I2C protocol are supported between PC and MCU communication

3. Supported OS are Windows 7 and Windows 10

4. C++/C# library for all functions as development interface is provided

Figure 29. Intel KPMU SW Architecture



13.4 Technical Collaterals for Reference Design

Technical Collaterals for v1.5

- System Design Guide – Doc# 646176
- Build Instruction - Doc# 646262
- Software Design Guide – Doc# 646048
- Software Usage Guide – Doc# 646066
- Software Release Notes – Doc# 646058

Technical Collaterals for v2.0

- System Design Guide – Doc# 735952
- Build Instruction - Doc# 735963
- Software Design Guide – Doc# 735974
- Software Usage Guide – Doc# 735975
- Software Release Notes – Doc# 734807

Intel® KPM Utility SW Packages Download Link:

- https://registrationcenter.intel.com/en/forms/?productid=3422

§

14.0 Electromagnetic Compatibility

Electromagnetic Compatibility (EMC) is the ability of electrical equipment, devices, and systems to function properly and be compatible within their electromagnetic environment, and show no signs of generating, emitting or receiving electromagnetic energy causing electromagnetic interference (EMI) in other devices within the surrounding area. EMC can be grouped into two categories:

Immunity testing - measures how a device will react when exposed to electromagnetic noise and other disturbances. The purpose of these tests is to gain a reasonable assurance that the device will operate as intended when used within its expected operating environment.

Emissions testing - measures the amount of electromagnetic noise generated by a device during normal operation. The purpose of these tests is to ensure that any emission from the device is below the relevant limits defined for that type of device. This, in turn, provides a reasonable assurance that the device will not cause harmful interference to other devices operating within its expected operating environment.

Although a few exemptions exist, if your design, manufacture or import products with electronics inside, then it's almost definite that you're going to need to care about EMC with below facts:

1. Protection of the electromagnetic spectrum

   We only have a finite amount of electromagnetic spectrum that we can use for things like radio transmission, microwave communication, x-ray machines and a huge number of other products.

   Unfortunately, even electronic devices without transmitters emit electromagnetic radiation, just as a byproduct of switching currents and voltages inherent to electronic circuitry. Without limits to the amount of unintended electromagnetic radiation from electronic products, the electromagnetic spectrum could be adversely affected, and frequency bands reserved for radio transmission could become compromised.

   As the number of non-wireless and wireless electronic products continues to explode, the already packed electromagnetic spectrum is going to become even more crowded. Protection of this essential resource is critical to ensuring that devices continue to be able to function properly in the future.

2. Safety

   For many products and industries, EMC performance can mean the difference between life and death. Many medical, military, industrial, aerospace and automotive products (and others) have safety critical applications.

If the function of those products fails due to electromagnetic phenomena such as power supply surges, ESD or radiated electric fields, then lives can certainly be at risk. Imagine 300 cellphones all transmitting 7 Watts of power on an aircraft at 36,000 feet - it's rigorous EMC testing that ensures that the electrical systems can withstand those sorts of electromagnetic environments.

3. Product performance (Reliability)

   The function and performance an electronic product can easily be affected by external and internally generated EMC phenomena. As an example, if your internal power supply regulation is too noisy, that can adversely affect sensitive analog measurements (for sensor products) or lower the performance of a radio transmitter (for wireless products). Those are both examples of internal EMC problems.

   Externally, applied EMC phenomena can negatively affect products in a virtually unlimited number of ways, from data corruption to measurement accuracy to RF performance to frying ICs. EMC testing helps to ensure that your device will continue to function as expected in the presence of a typical EMC environment and (hopefully) reduce the amount of product returns to poor EMC performance.

As the complexity of these electronic products intensifies, constraining EM emissions within dense printed circuit boards (PCB), IC packages and even the IC itself requires careful engineering. With package pin counts more than 1000 and ever-smaller pitch spacing compressed into shrinking board space, the potential for electromagnetic interference is greatly increased.

Electromagnetic waves, conduction and inductive/capacitive coupling are all sources of EMI. Excessive emissions leading to EMC failure can be related to poor component shielding, enclosure design and/or cabling, which can couple energy from inside the system to the outside world. A harmonic signal from a seemingly harmless low--amplitude clock may be at the right frequency to excite a resonance within a module or housing, resulting in elevated currents that will radiate through an aperture (dimension dependent) or cable. System-level EMC design must therefore adequately model the chassis, any venting/seams and cabling in addition to the PCB.

In each platform design guide (for example, ADL-S PDG #619508), there is a dedicated chapter (chapter 8) to address the design consideration for Electromagnetic Compatibility. Highlight guidelines below for meeting high reliability design.

14.1 PCB Layout and Routing

1. It is recommended that the routing of High radiation signals (such as clock, high speed I/O) be embedded in inner layers and covered by solid ground. Due to routing limitations, full stripline routing may not be possible. Recommend < 38 mm

microstrip routing at breakout region and < 25 mm microstrip routing at connector region to reduce EMI/ RFI risk.

2. Avoid route signals over split reference planes (GND, Power Planes). This leads to unnecessary large current loops (as the current return cannot flow directly under/beside the forward current) and large current loops in general lead to high radiated emission values. Changing reference plane from GND to power plane, or from power plane A to power plane B, may significantly increase noise emission. It is recommended to have stitching capacitors (0.1 uF, 0402 or smaller) to bridge the two reference planes and provide current return path.

3. Decoupling is important! Always consider decoupling! Place ceramic capacitors (0.1 uF, 0402 or smaller) close to EVERY power supply pin of EVERY chip, as well as the power pins of all internal and external connectors to reduce power noise on your PCB design.

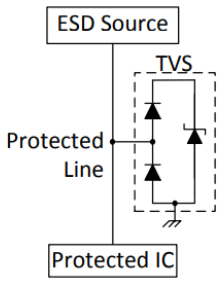
4. Connect circuit GND to chassis at IO area. This prevents radiation, as the GND shows a minimum voltage difference to the chassis (earth). And helps your IO-signal-filters on your PCB being most effective and keeps ESD pulses away from your circuit. Because incoming noise (burst, ESD) from the cable can directly flow back over chassis to earth.

14.2 ESD Protection Design

The key to the ESD design guidelines for protecting the devices on any external Input / Output (I / O) lines, is to prevent the voltage rising above a level that will damage the interface device. This may be achieved using a circuit that clamps the maximum voltages to just outside the maximum operating extremes. This is where the TVS becomes applicable.

A TVS is an array of diodes arranged to present a very high impedance to the voltages normally present in the circuit, but if voltages exceed the design, the TVS diodes will breakdown and shunt I_{ESD} to ground before it can damage the system being protected. The system designer is then challenged to lower the impedance for I_{ESD} from the ESD Source through the TVS to ground.

Figure 30. ESD Protection Concept



The impedance presented to I_{ESD} is a function of any impedance inherent with the TVS (in the diode array and the package of the TVS) and the PCB Layout between the ESD Source and the TVS ground. A TVS is generally designed to offer as low of an impedance to ground for I_{ESD} as its overall design constraints will allow. With the proper TVS selected, a critical phase of the design is to lower the impedance in the PCB Layout between the ESD Source and the TVS ground.

There are a few basic design guidelines for ensuring that any printed circuit board, PCB design is able to reduce problems from ESD to the minimum:

I. Protection parts (like TVS) should be placed near I/O connector as short as possible.

II. Reduce parasitic inductance around protection circuits: Many electronics circuits will incorporate ESD protection circuits. These can only be effective if the levels of parasitic inductance are low. Parasitic inductance arising from the PCB design can be reduced by keeping line lengths in this area particularly short, and also increasing the track width.

III. Avoid running sensitive tracks near the extremity of the PCB: As levels of pickup from static discharges are likely to be greater closer to the extremities of the board, it is wise to keep any sensitive lines away from these areas. Input and output lines will often need to reach the PCB edge at some stage, but they can be routed away from the edge as soon as possible where applicable.

§

15.0 Stack-up and PCB Consideration

15.1 PCB Stack-up Guidance

Different stack-ups can be implemented following the recommendation listed in PDG (for example: ADL-S PDG #619508), but 8 layer or above (1.6 mm thickness) is suggested for high reliability design.

All routing guidelines suggested in each PDG are defined based on these reference stack-ups that meet the Tline Spec electrical targets for Impedance (Z), Insertion Loss (A) and Crosstalk (K), inclusive of +/- 10% impedance HVM variation.

It is important to note that variations in the PCB stack-up, such as changes in the dielectric thickness, copper thickness, trace width, and spacing can impact the impedance, loss, and jitter characteristics of all the interfaces. Such changes may either be intentional, or the results of variations encountered during the PCB manufacturing process. In either case, they must be properly considered when designing the interconnects.

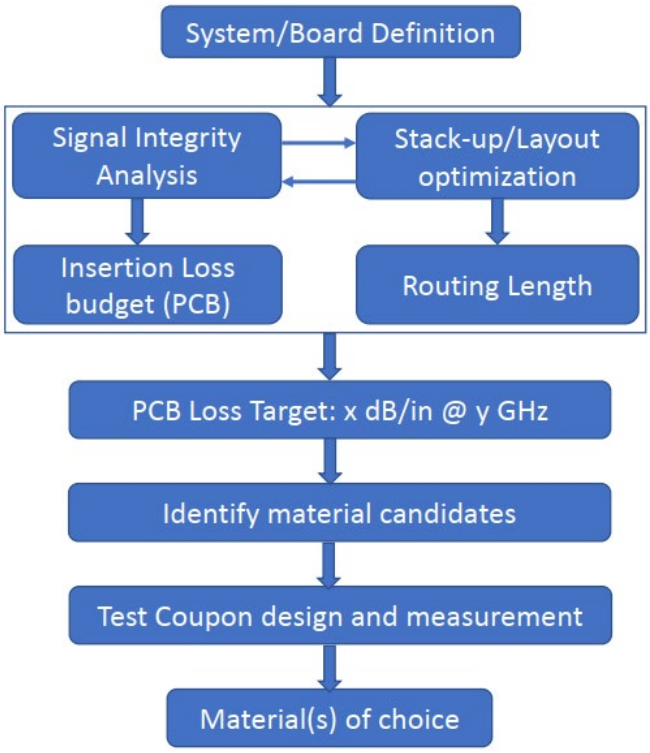
Customers should use Intel Platform Design Studio (# 647388) to run electrical analysis for PCB stack-ups that differ from the Intel reference stack-ups, ensure that electrical targets are met.

15.2 PCB Material Guidance

This chapter is intended to aid designers in engineering Intel Core and Atom Platform high reliability Printed Circuit Board (PCB) designs. The goal is to provide practical routing solutions with satisfactory signal integrity for PCBs of the topologies presented in the PDG, at reasonable costs.
Designs following these guidelines can leverage Intel's simulations heavily; designs which deviate significantly from these guidelines must be based on representative simulations to ensure that timing and voltage specifications are met.

For a typical board design, the following flow can be used to determine the PCB loss target, and then select the appropriate PCB material for optimal performance and cost.

Figure 31. PCB Materials Select Flow



16.0 Solder Joint Reliability

Solder joint reliability is often a pain point in the design of an electronic system. A wide variety of factors affect solder joint reliability and any one of them can drastically reduce joint lifetime. In order to achieve the highest solder joint strength & reliability, it is recommended that:

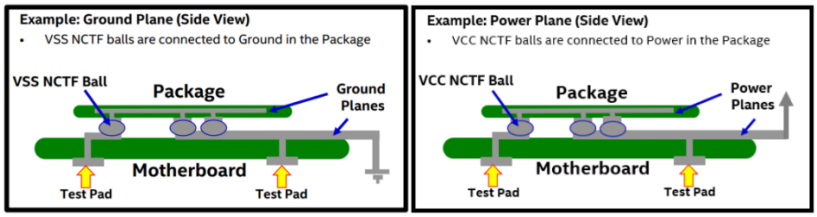
1. Customers follow the Intel reference Land Pattern design (Refer to #630369 for ADL-S) for CPU and PCH components. (Land pattern designs recommendations included pads, traces, trace angles and via-in-pads).

2. Intel add NCTF (none-critical to function) pin in package design and recommend including mother board test features to test the connectivity of corner NCTF Solder Joints (SJ) on processor and chipset packages. The corner NCTF solder joints experience the highest strain during board processing / handling and board flexure. It is useful to detect when those corner NCTFs fail, as fails at these locations can give an indication of marginal board assembly processing or designs.

Motherboard Design Implementation:

- Intel's BGA processors allow for corner NCTF SJ testing capability.
  - Some corner NCTF SJ's have pins connected to the package VSS/GROUND plane and/or VCC/POWER plane, which can be used to test SJ connectivity with ICT, using isolated test pads added to the customer's motherboard designs -> see figures below.

Figure 32. NCTF Solder Joint Connection Examples



- With motherboard test pads in place, ICT personnel can develop a continuity or resistance test to check connectivity from corner NCTF SJ's to their corresponding isolated test pads on the motherboard.

  Continuity / Resistance Test Threshold

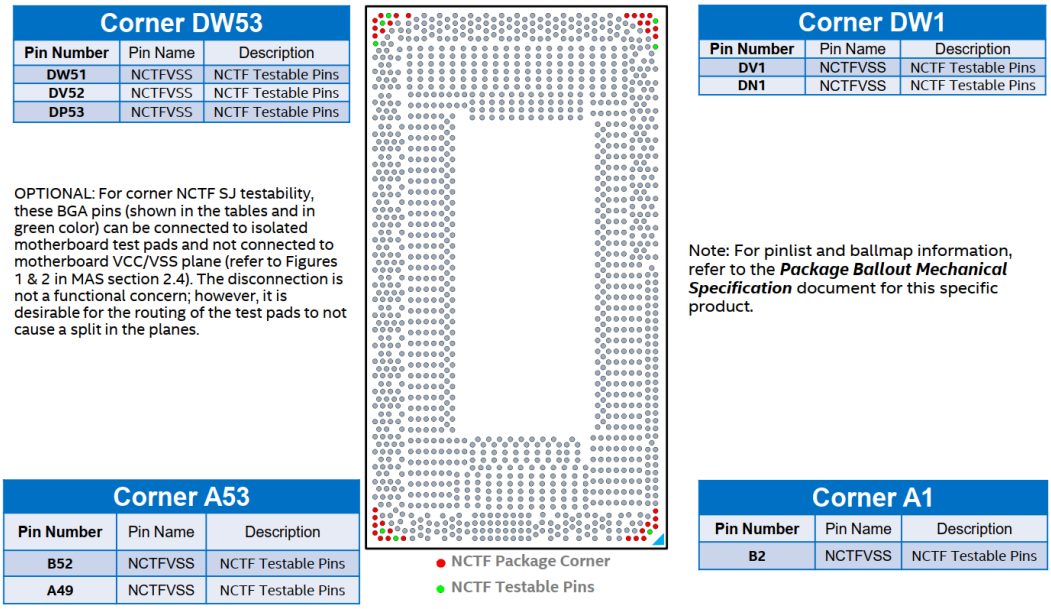
  - Continuity or resistance tests are developed using a pass/fail resistance threshold.

- The pass/fail threshold would be determined by the accuracy of the test equipment and measurement data obtained from boards with known good solder joints.
- For motherboards under test, a measurement below the pass/fail threshold may indicate a good package electrical solder joint (pass), and a measurement above the pass/fail threshold may indicate a bad package electrical solder joint (fail).

Note: This type of electrical resistance test can detect a completely open solder joint between the package and board but can be ineffective in detecting marginal solder joint connectivity (a SJ that may not be mechanically sound).

Here are the NCTF testable pins for TGL-UP3, these green corner NCTF balls have daisy chain connections routed inside the processor package. Customer should add isolated motherboard test pads to check corner NCTF SJ connectivity.

Figure 33. NCTF Pins for TGL-UP3



§