ELMG
power electronics digital control

PSMA

Industry Session #28: Reliability
Actions to Improve Software Quality in Digital Power Electronics using PSMA's SW Reliability Report

Presented By –
Hamish Laird, CEO
ELMG Digital Power, Inc
enquiries@ELMGDigitalPower.com

Thursday, March 19, 2020

OVERVIEW

- **PSMA SW Reliability Report structure**
- **Where to start**
- **First steps from Best Practice**
- **What comes next – how to get better**

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Report Outline – Best Practices

© 2019 PSMA All Rights Reserved

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

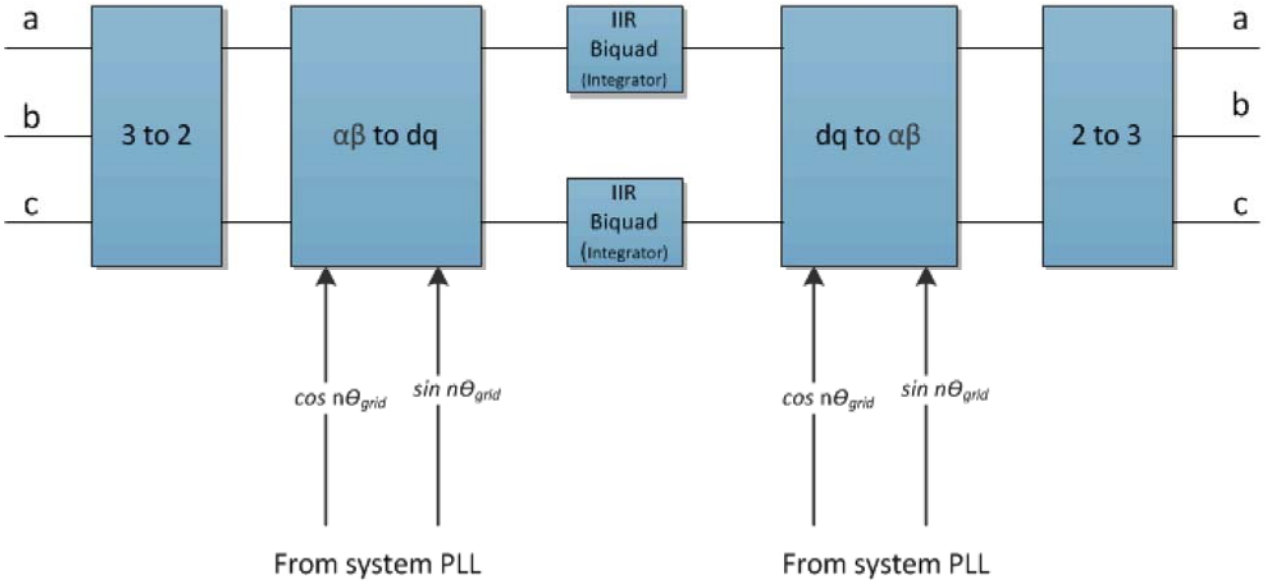
First Steps – from Best Practice

- **Assess where you are at**
- **Design partition**
- **Team Capability**
- **Code Standards**
- **Converter Design for control**
- **Version control**
- **Build Server**
- **Verification testing**
- **Code Inspections**
- **Release Process**

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Design partition

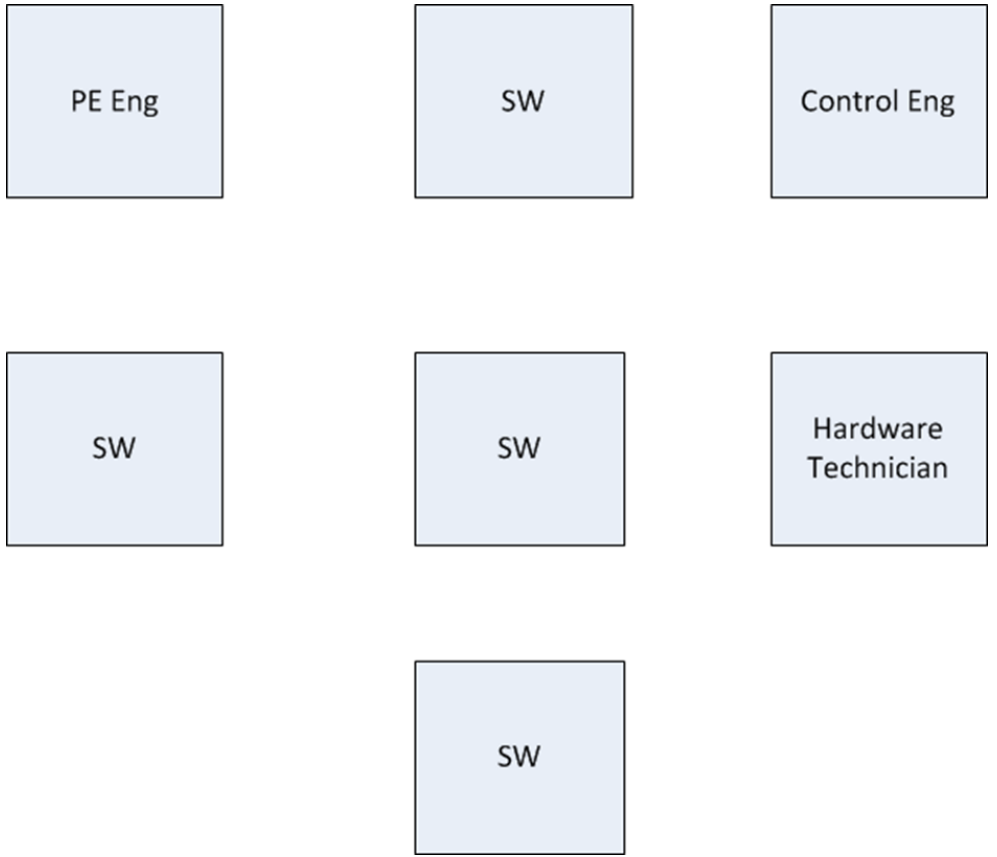
- **Divide the system into realizable and testable sub blocks**



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Team Capability

- **Typical team members in digital power team**



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Code Standards

Rule Summary

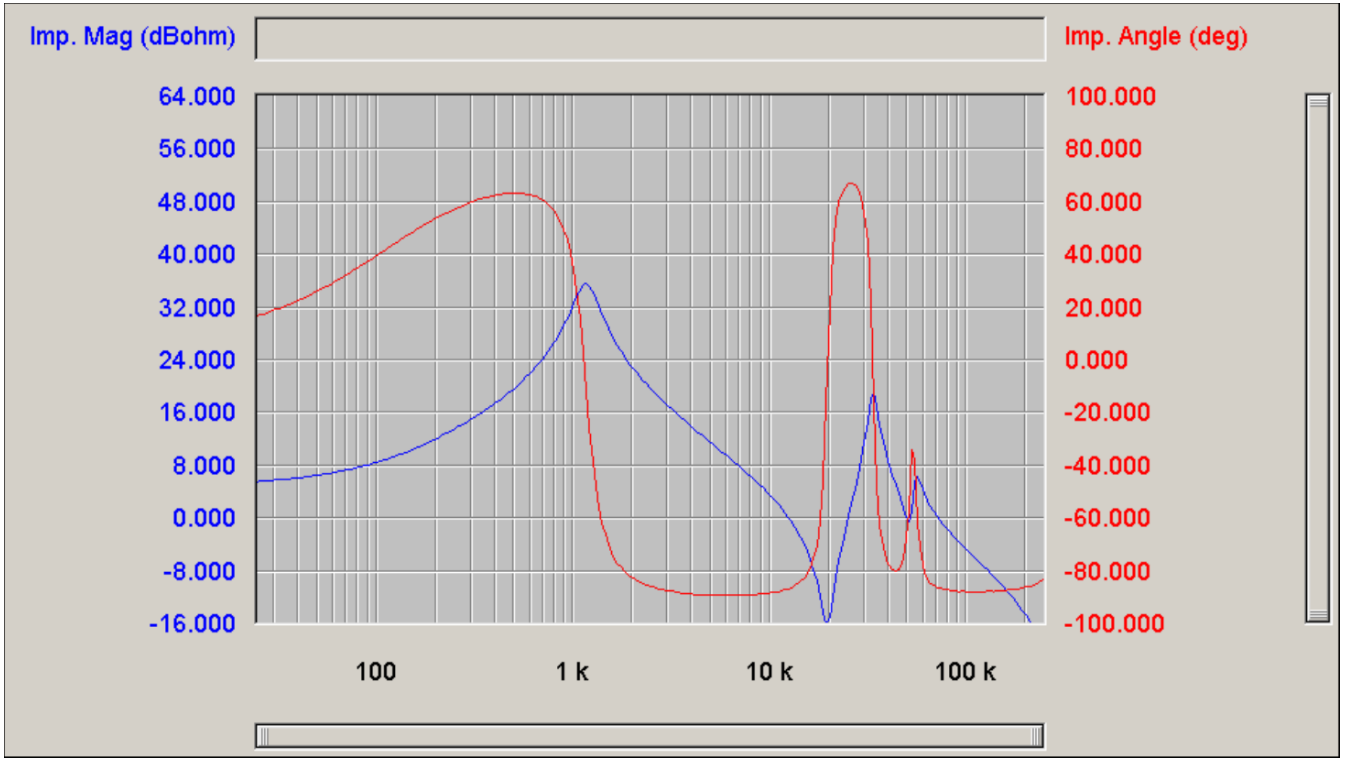
1 Language Compliance	
1	Do not stray outside the language definition.
2	Compile with all warnings enabled; use static source code analyzers.
2 Predictable Execution	
3	Use verifiable loop bounds for all loops meant to be terminating.
4	Do not use direct or indirect recursion.
5	Do not use dynamic memory allocation after task initialization.
*6	Use IPC messages for task communication.
7	Do not use task delays for task synchronization.
*8	Explicitly transfer write-permission (ownership) for shared data objects.
9	Place restrictions on the use of semaphores and locks.
10	Use memory protection, safety margins, barrier patterns.
11	Do not use goto, setjmp or longjmp.
12	Do not use selective value assignments to elements of an enum list.
3 Defensive Coding	
13	Declare data objects at smallest possible level of scope.
14	Check the return value of non-void functions, or explicitly cast to (void).
15	Check the validity of values passed to functions.
16	Use static and dynamic assertions as sanity checks.
*17	Use U32, I16, etc instead of predefined C data types such as int, short, etc.
18	Make the order of evaluation in compound expressions explicit.
19	Do not use expressions with side effects.

4 Code Clarity	
20	Make only very limited use of the C pre-processor.
21	Do not define macros within a function or a block.
22	Do not undefine or redefine macros.
23	Place #else, #elif, and #endif in the same file as the matching #if or #ifdef.
*24	Place no more than one statement or declaration per line of text.
*25	Use short functions with a limited number of parameters.
*26	Use no more than two levels of indirection per declaration.
*27	Use no more than two levels of dereferencing per object reference.
*28	Do not hide dereference operations inside macros or typedefs.
*29	Do not use non-constant function pointers.
30	Do not cast function pointers into other types.
31	Do not place code or declarations before an #include directive.
5 – MISRA *shall* compliance	
73	All MISRA *shall* rules not already covered at Levels 1-4.

APEC 2020

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

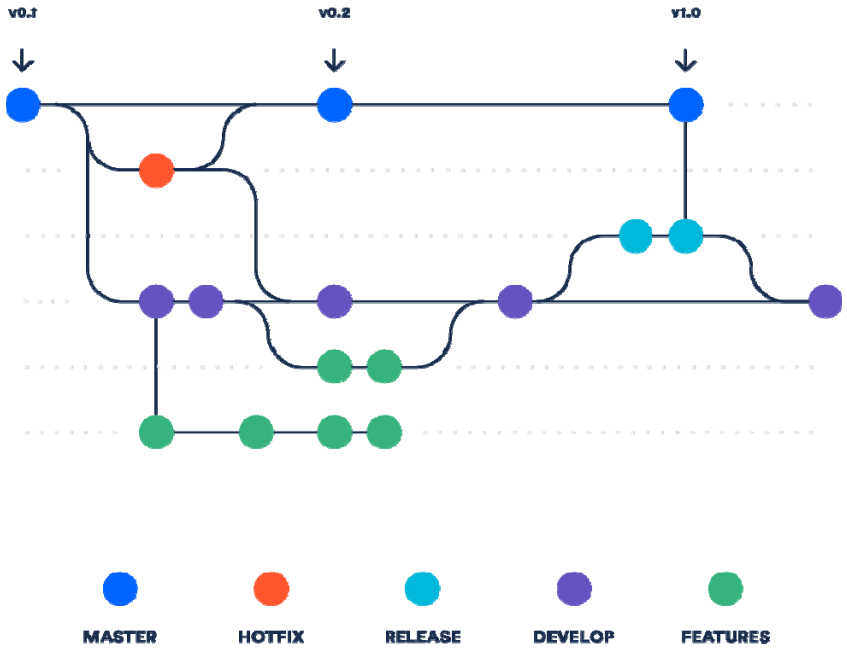
Converter Design for Control



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Version Control

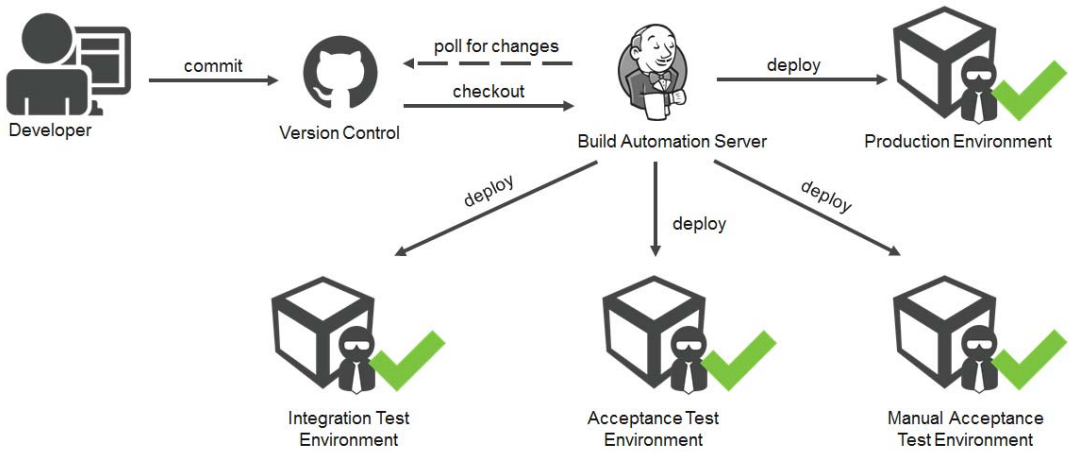
- **Use Git based version control**
- **Team works in development branch**
- **Additions in Features and hotfixes**
- **Choose which features got into release**



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Build server

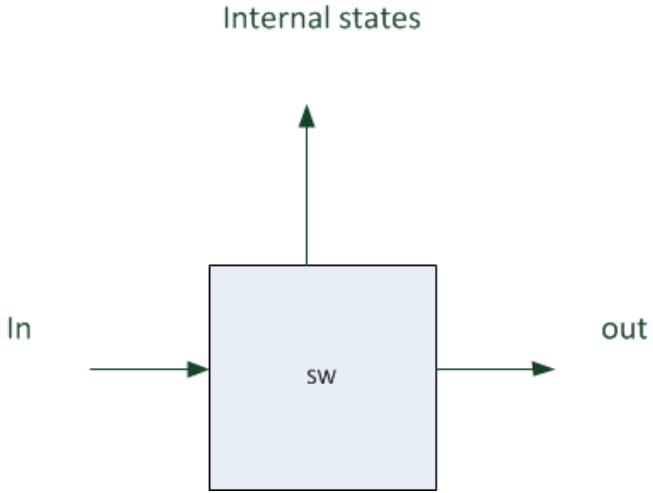
- **Central server**
- **Build code**
- **Automatically deploys to testing and inspection**



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Verification testing

- **Black box**
- **White box**
- **Need a verification plan for each block on partition**



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Code Inspections

- **Most effective tool for code quality improvement**
- **Do before testing**
- A review meeting should be scheduled for no longer than one hour with the intention of inspecting less than 200 lines of code.
- The author should prepare by proposing the code to be inspected.
- The meeting leader / moderator should arrange the meeting room and decide on the questioner and the recorder.

For one hour, the four review members work through the (less than) 200 lines of code, inspecting the code against the design documentation and the coding standard.

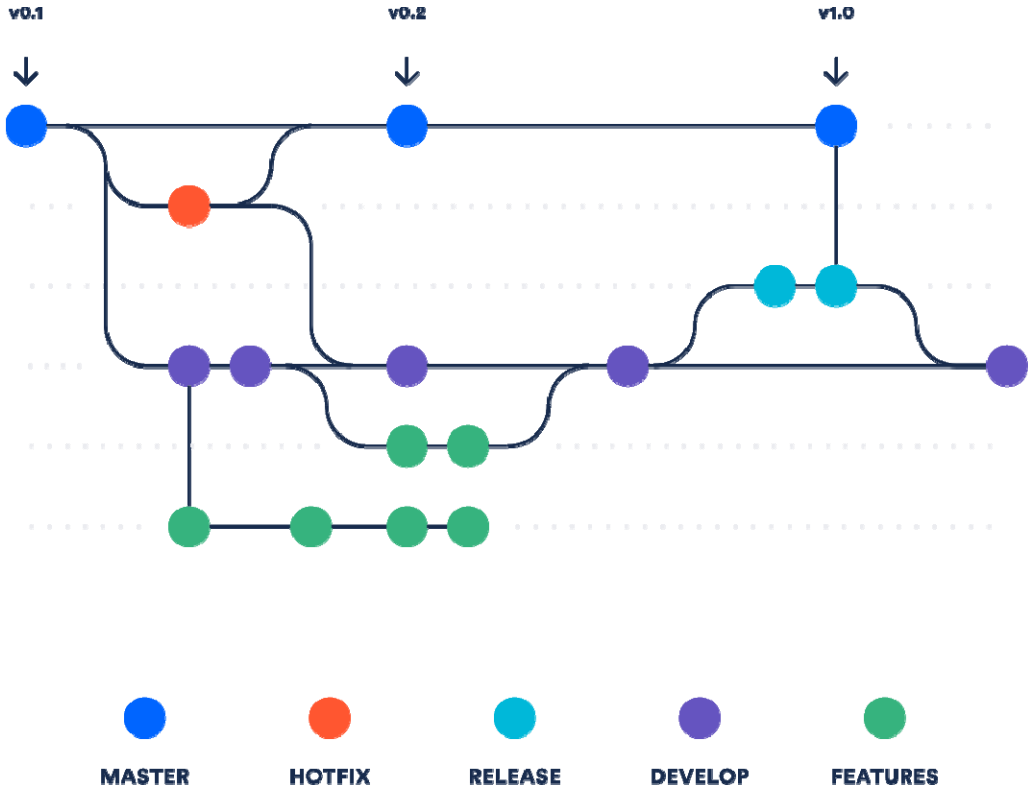
After the inspection, the recorder forwards all the meeting actions to the moderator who ensures that the author makes the changes. The moderator then decides if the inspection needs to be repeated or if the code can be accepted without further inspection.

APEC 2020

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Release Process

- **Automate this**
- **Integrate with build server**
- **Continuous release is best**



APEC 2020

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

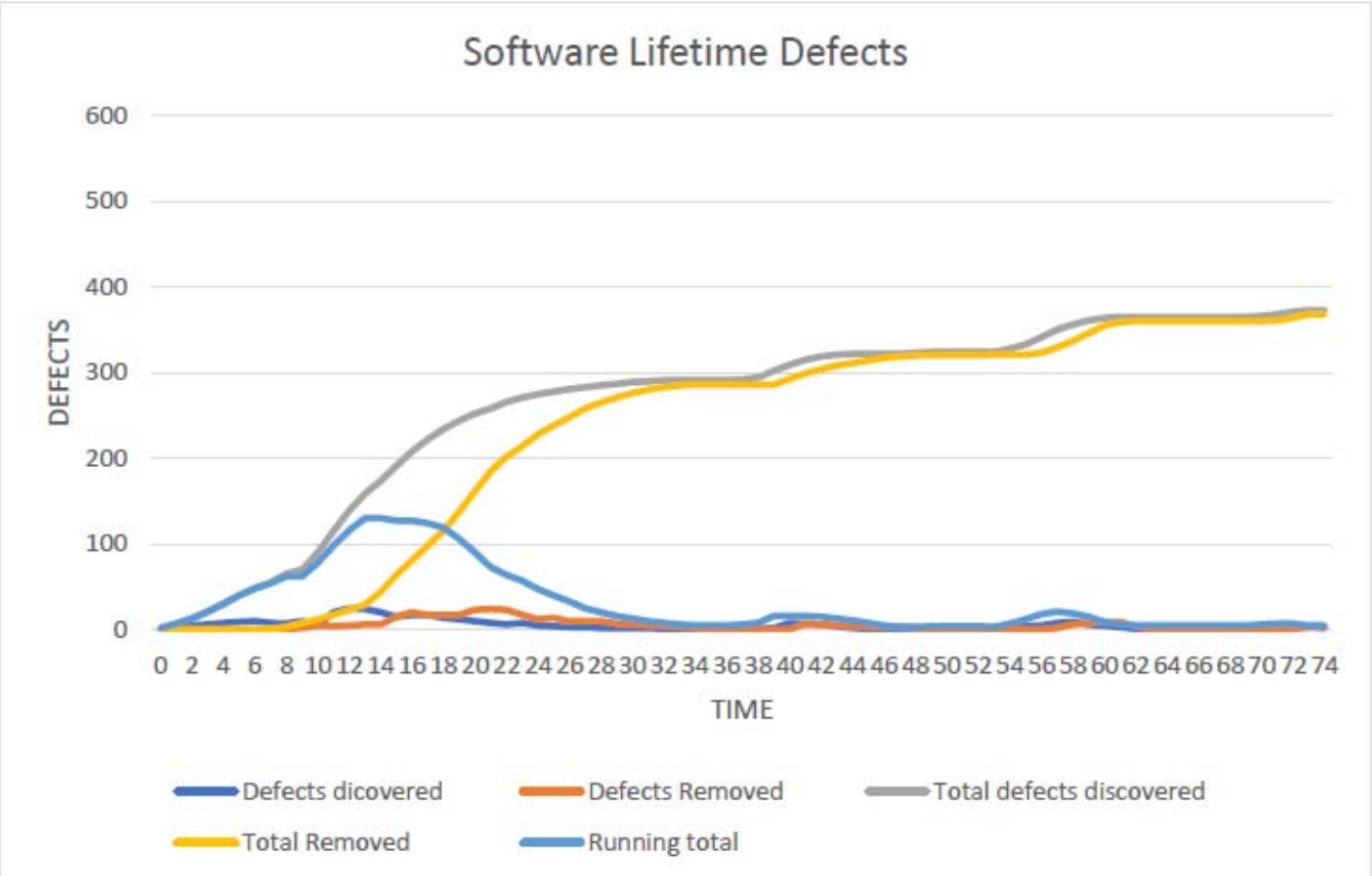
What next

- **SW/Firmware Reliability Report sections cover each of these steps in some depth**
- **Aim to get better**
- **It takes time**
- **Openness is best**
- **Expect customer code and process audits**

APEC 2020

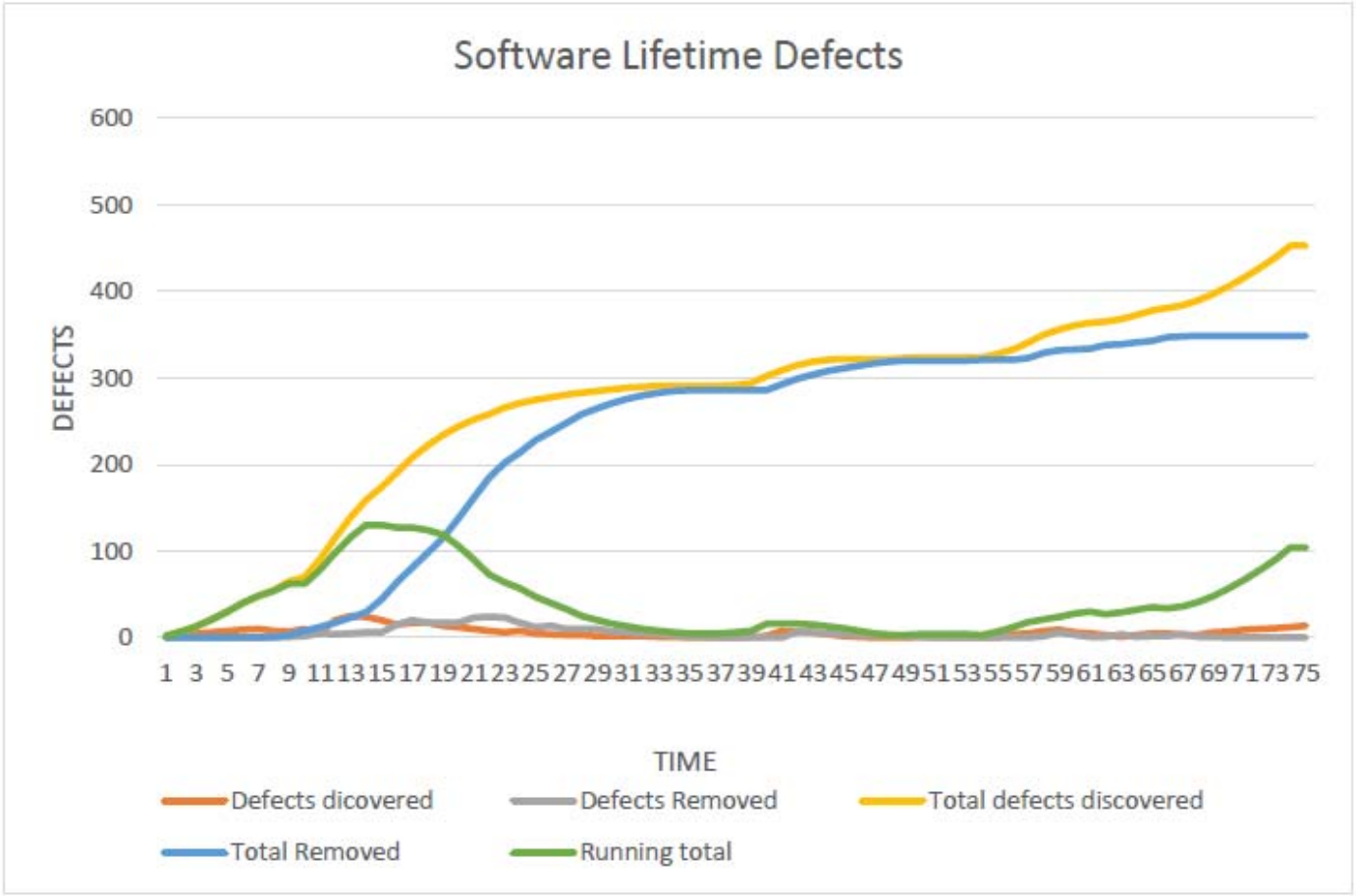
ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Track defects to see how good you are



ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Software End of Life indication



Conclusions

- **PSMA SW/Firmware Reliability Report has best practice steps – start at the beginning**
- **Explanation of how to do each step in report**
- **Start with a partition**
- **Add version control**
- **Build capability**
- **Track defects to see how you are doing**

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

Q & A

Thanks a lot for your time and attention!

Any questions and/or comments?

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.

References

- PSMA Power Supply Software Firmware Reliability Improvement Report 2019 - PSMA

ALL INFORMATION SHALL BE CONSIDERED SPEAKER PROPERTY UNLESS OTHERWISE SUPERSEDED BY ANOTHER DOCUMENT.