An empirical study of the practical application of EN50128 to software engineering

Dr. Andrew Hussey
Maria Hill
Martin Hughes
Lionel van den Berg

HITACHI
Inspire the Next

18 October 2023

Introduction

EN50128 commonly applied to railways Software Engineering.

EN50128 provides a framework for the Software process, based on the SIL of the Safety Functions implemented by that Software.

Implicitly, the application of EN50128 should lead to more robust Software with fewer faults.

Despite this, there are few empirical studies of the application of EN50128.

Software Best Practice

5 major commonalities between EN50128 and software best practice

1. Emphasis on requirements – deriving them early (well before coding begins) and verifying and validating them.

2. Emphasis on testing – at all levels: component, subsystem, system, and on the need for robust test planning and test reporting.

3. Emphasis on traceability at all levels:
   - Requirements to project scope/contract;
   - Requirements to tests;
   - Tests to test status and defects.

4. Emphasis on good application data processes.

5. Emphasis on maintenance activities for software.

Overall: the need for good documentation for all aspects

KPIs for Measuring Software Quality

HITACHI
Inspire the Next

Total number of open defects over time

Speed with which the total number of open defects rises or falls.

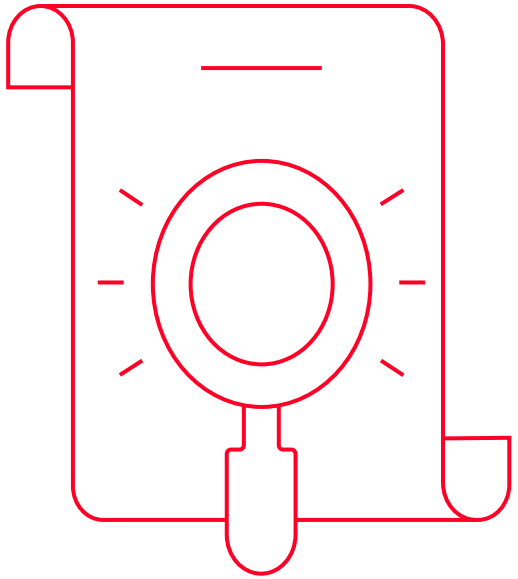
Defect density

Number of defects per thousand lines of code.

Number of baseline changes

Number of build releases for the individual components that make up the greater system.

A large number of components being changed at a fast and/or sporadic rate indicates an amount of churn and thrash.



Case Study – TCS Functions

HITACHI
Inspire the Next

RioTinto

AutoHaul® TCS is the control centre-based system used to monitor and control the RTIO railway and provides the GUI to the Train Control staff to:

- Set routes for trains;
- Track the movement of trains through the RTIO network;
- Monitor the status of, and receive alarms from, field equipment such as signals, track circuits, points, and asset protection devices;
- Receive indications and status from the RTIO network signalling infrastructure and Asset Protection devices;
- Setup the Automated and Driver Assisted missions for the train; and
- Perform maintenance monitoring and remedial action that was previously undertaken by the Driver for AutoHaul® Trains.

TCS has significantly been modified and upgraded and is now a complex software system made up of 41 separate subsystems.

Method

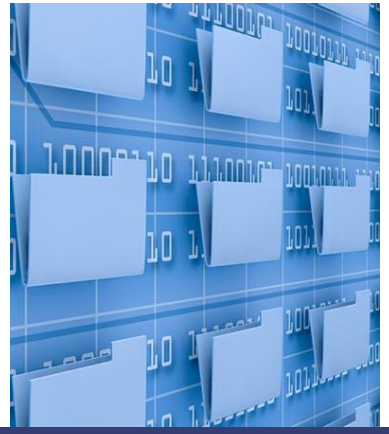
GBMS V&V Governance

GBMS requires software changes to be made following basic integrity.

RAMS R&Ms requires governance of V&V

Pseudo Assessment:

- Assessment Plan using applicable EN50128 clauses
- Assessment Report



Assessment Activities:

- Collaborative audit sessions
- Multiple reviews of documents
- Additional clarification meetings
- Previous assessments

3.3 Assessment of Software Validation

Clause 6.3.1.1 of EN50128 [12] defines the scope of software validation as:

"*… to demonstrate that the processes and their outputs are such that the software is of the defined software safety integrity level, fulfils the software requirements and is fit for its intended application*".

For the TCS software assessment of the TCS software validation the following activities will be performed:

Input Document	Assessment Objective(s)	Clause(s)
Software Validation Plan	To assess if an appropriate Software Validation Plan has been produced, including whether an appropriate set of techniques from EN50128 [12] Annex A –Table A.5, A.6, A.7, and A.8 suitable for SIL-0 has been selected and applied.	6.3.4.3 to 6.3.4.6
Software Validation Report	To assess if an appropriate Software Validation Report has been produced.	6.3.4.7 to 6.3.4.11
Software Validation Verification Report	To assess if an appropriate Software Validation Verification Report has been produced.	6.3.4.12 to 6.2.4.14

Table 3: Assessment of Software Validation

Positive Outcomes

A framework for deciding what activities to perform/ not perform for a SW release (best practice #5)

A language for communication within the team, management and with the client regarding activities and timeframes (best practice #1 and #2),

More focus for regression testing that was was more targeted, including application data (best practice #2 and #4)

Re-examination of the traceability of requirements – a challenge because the SW was already existing and in operation (best practice #3)

The benefit of considering the existing processes and documentation when tracing to and showing compliance with the EN50128 clauses, particularly concerning the verification reports (best practice #1 and #5).

Challenges

Software originally developed to EN50128:2001, but not formally assessed therefore assessment against the updated EN50128:2011 was a challenge, highlighting the importance of the assessment activity.

An understanding of EN50128, particularly terminology, was an obstacle at the start of the assessment activity and created inefficiencies. The standard is complex and training and familiarisation with EN50128 was identified as a need for all software personnel.

Important to start by understanding and documenting the existing process before trying to trace to or show compliance with EN50128, to derive the full benefit of what is already being done and to highlight the gaps that need to be addressed.

Assessment Outcomes

Collaborative "assessment“ worked well and benefited the TCS team and resulted in on-the-job training. If a higher SIL is required, a collaborative "assessment" could still benefit to prepare for the formal independent assessment.

Standard is complex and unless the team has experience and training, full compliance is unlikely without additional inspection and assistance.

Standard appears extremely onerous, intimidating, and intractable for an inexperienced software team, which obstructs the application of the standard, so the collaborative assessment approach helps to overcome those barriers.

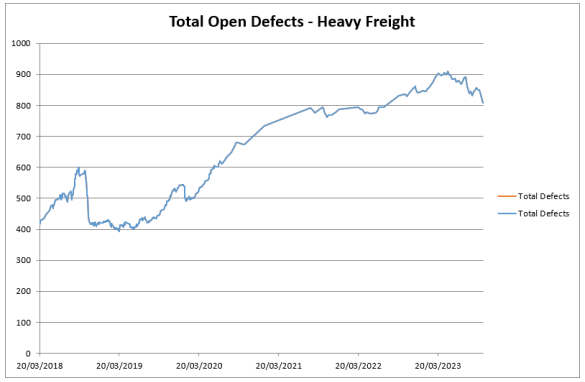
KPI Measurement Outcomes

HITACHI
Inspire the Next

Total number of open defects

Improved process compliance has the line flatten over time, indicating that:

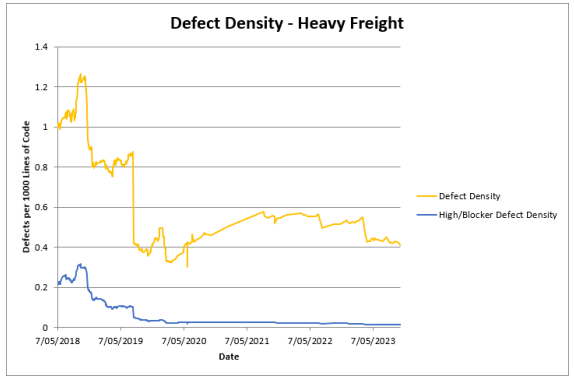
- **Defects cleared at the speed at which new code is being developed;**
- Planning and scheduling of software development may have become more controlled;
- Code quality may have increased;
- Defect clearing may have become more organised.



Defect density

Dropped over the lifetime and even though the size of the software code base is continually increasing, the defect density is not, indicating:

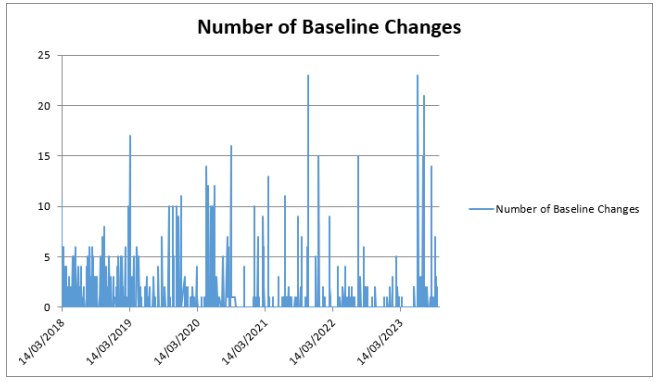
- Quality of new code has increased;
- **Rate at which new defects are being raised may have slowed.**



Number of baseline changes

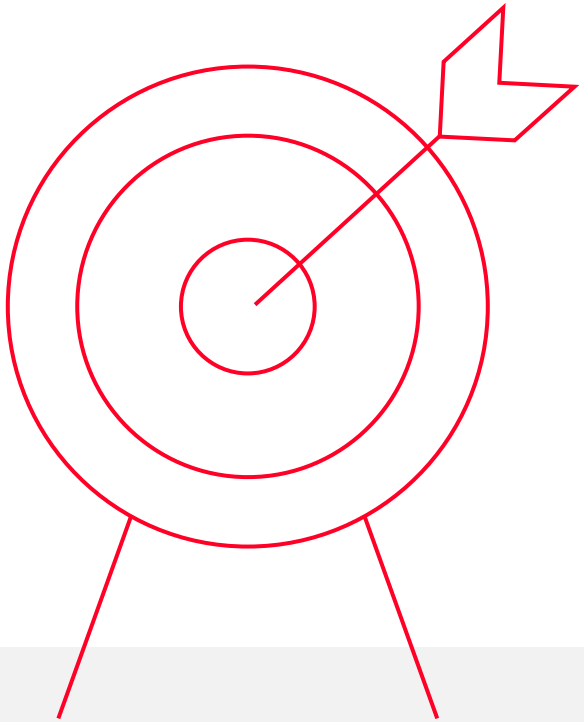
Lessened over the lifetime and started to occur at regular intervals, indicating:

- Software releases are now more planned;
- **There is less thrash and churn in the development process;**
- The code quality has improved (as there are fewer unplanned releases to fix critical defects).



Conclusions

EN50128 can be used to develop Software that meets commonly accepted principles for Best Practice, as well as to reduce the occurrence of faults



1. Comparison of EN50128 to commonly accepted Software Best Practices shows commonalities and overlaps

2. Case Study shows that the assessment activities were themselves beneficial, particularly when done collaboratively

3. Aspects of EN50128 seen as most useful to improve the quality of the Software:

- Assessment process driving the software team toward best practice
- Giving a framework for training the team, highlighting competencies for software development, verification and validation, not just EN50128


HITACHI
Inspire the Next