Using MIL-STD-882 as a WHS Compliance Tool for Acquisition

Or what is This Due Diligence thing anyway?

Matthew Squair

Jacobs Australia

28-29 May 2015

Acknowledgement

I'd like to acknowledge the assistance of Kate Thomson and John Davies in casting their legal eyes over this presentation.

Disclaimer

The comments and opinions of this presentation are mine and do not represent the opinion of Jacobs Australia or the Australian Defence Organisation.

Where to find this

You can find this presentation and the associated paper at www.criticaluncertanties.com

License

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

Mark Twain

"It is better to be vaguely right than exactly wrong"

Carveth Read

A bit about me...

Who I work for

Pertinent experience

Interests

What is the Australian Defence Organisation about?

What is the Australian Defence Organisation about?

Capability...

Operationally it's the use of capability by the operational arms

Sustainment, it's about supporting

Acquisition, it's about obtaining the materiel for new or replacement capabilities

Acquisition and sustainment of materiel are traditionally handled by the Defence Materiel Organisation (DMO)

The law and the engineer

"If you want to know about nature's laws ask a scientist"

"If you want to know about man's laws ask a lawyer"

"But if you want to know about the intersection of man and nature's laws ask an engineer"

The WHS model act 2011 in a nutshell

The legislation is very pragmatic:

- Rejects risk acceptance...because risk is so problematic
- Negligence driven, e.g reasonable (1863) & practicable (1947)
- Due diligence is admitted as a defence (stockbrokers defence)
- Borrows hierarchy of controls from existing safety standards
- Deliberately establishes non-transferable responsibilities
- Establishes supply chain responsibilities
- Eye watering criminal penalties for duty holders...

What is this due diligence of which you speak?

Due diligence INCLUDES:

1. Acquire and keep up-to-date knowledge
2. Understand operations and their hazards and risks
3. Appropriate resources and processes to eliminate/minimise risks
4. Processes for receiving and responding to safety information
5. Processes for complying with any duty or obligation, and
6. Verifying the provision and use of the resources and processes referred to in paragraphs (3) to (5)

The WHS act and the supply chain

WHS act imposes *specific* responsibilities upon designers, manufacturers, importer's and suppliers

However the end customer still retains overall responsibility

Customer can rely upon advice (evidence) from suppliers

But what is the standard of persuasion? How much evidence is required and of what probative value? What may we presume?

Advice from legal counsel - When the courts can apply severe penalties, look for strict compliance

Project background

Project was a major capability upgrade to an in service aircraft by the OEM

Project was required to demonstrate compliance to the WHS Act (2011) to obtain Special Flight Permit. But demonstration of compliance *was not* required of the supplier explicitly

Compliance finding is part of the technical airworthiness framework

Degree of compliance finding (& evidence) needed is driven by program complexity, size and supplier maturity

Supports design acceptance and type certification

Compliance finding process is oriented towards design standards, not legislation... So what to do?

Compliance finding and the WHS

Compliance finding process oriented towards design standards

These tend to generate an evidential tail of design artefacts (evidence)

Not so for legislation...

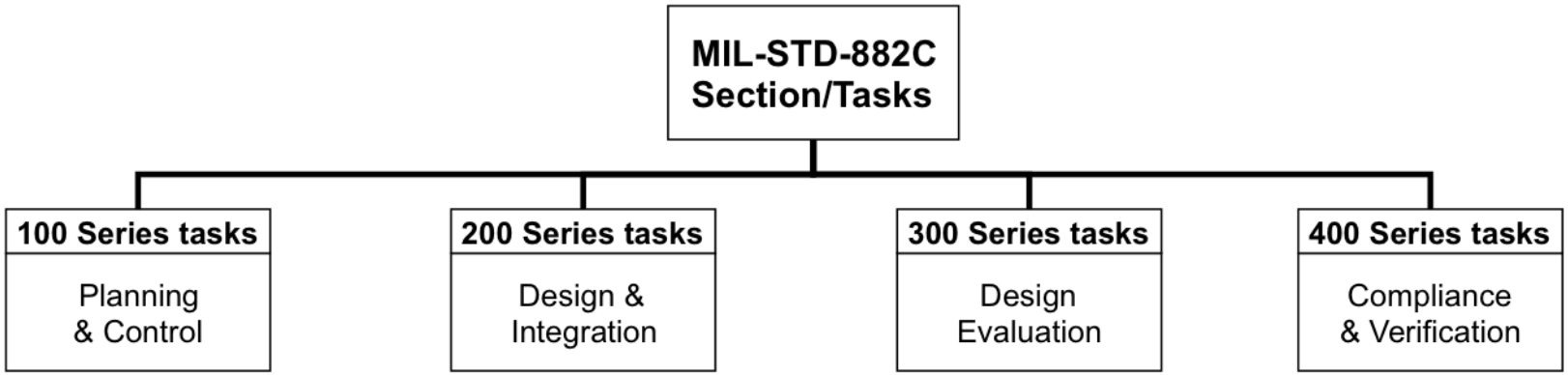
Solution, use the contracted system safety standard (MIL-STD-882C)

Tracing the WHS Act to the standard allows us to translate subjective high level objectives to specific tasks and accomplishments

MIL-STD-882 is task/ data deliverables oriented, gives us evidence

Deliverables already in scope of contract, original build was done to MIL-STD-882C (with tailoring)

MIL-STD-882C System safety standard tasks



1. System Safety Program
2. Safety Program Plan
3. Integration Management
4. Program Reviews & Audits
5. SSG/SSWG Support
6. Hazard Tracking
7. Progress Summary

1. Preliminary Hazard List
2. Preliminary Hazard Analysis
3. Safety Requirements Analysis
4. Subsystem Hazard Analysis
5. System Hazard Analysis
6. Operating & Support Hazard Analysis
7. Health Hazard Assessment

1. Safety Assessment
2. T&E Safety
3. Safety Reviews of ECPs

1. Safety Verification
2. Safety Compliance Assess.
3. Explosives Hazard Class.
4. EOD Data

A bit more on evidence

Evidence and it's quality is a key aspect of compliance finding:

- Relevance*
- Clarity
- Unambiguity
- Parsimony
- Authenticity

The first part of the compliance finding task was therefore to establish the relevance of each deliverable to WHS Act compliance

How well does the standard satisfy the WHS Act?

- Competence and compliance - Yes
- Reasonable forseeability of hazards - Yes
- Hierarchy of controls - Yes
- Use of design standards in lieu of risk analysis - Yes
- Reasonable practicability - No (Customer must decide)

MIL-STD-882 myth: The standard is risk centric

MIL-STD-882C is not risk acceptance centric, instead it requires the upfront elimination/reduction of hazards much like the WHS Act

Practical implementation

Having confirmed adequate coverage the compliance finding team moved into assessing the evidence provided by the OEM

For more complex deliverables the finding included an analysis of the deliverables quality and a summary of the conclusions was included in the compliance finding

An Independent Safety Assessors report provided additional backing evidence for the compliance finding

The exercise highlighted the necessity for compliance findings to be performed by competent persons. In the case of specialist safety analyses (e.g. fault trees) this competence may not exist within the usual project office

Software hazards and reasonable practicability

The aircrafts software was also modified, these modifications were assigned specific integrity levels on the basis of functional risk

Problem, risk acceptance based standards, such as DEF STAN 00-55/56 or IEC 61508, violate reasonably practicable

In fact they can establish a case for recklessness

How do we establish that what was done was all that was reasonably practicable?

Software hazards and reasonable practicability (Cont'd)

We ignored the SIL assignment and looked outside the project for an 'industry standard', we selected DO-178

We cross compared assigned integrity levels to FAA guidance (AC23.1309E) on DO-178 DALs for commercial aircraft classes

Non-trivial task to correlate SIL targets against DALs by function and failure mode

Resultant comparison was used to establish whether what had been done reflected an industry standard for assurance efforts

Results

Results

The project was able to demonstrate to the Design Acceptance Representative that the project was compliant to the WHS Act

This did require a separate consideration of whether all ‘reasonably practicable’ measured had been implemented by the customer

Conclusions

Risk acceptance based standards and the WHS Act don't mix

Yes you can use MIL-STD-882C as a tool to demonstrate compliance, with some caveats

... much better if you do it upfront in the project

Risk driven software standards are extremely problematic under the act, SIL or DAL assignment 'magic' does not satisfy what's reasonably practicable

In order to satisfy the duty holders due diligence obligations we seem to have gone full circle back to task/deliverable contracting

The full effects of the WHS Act on the regulatory landscape have not yet evinced themselves...so watch this space

Future work

Express the WHS Act/MIL-STD-882CC compliance argument utilising a formal notation such as Goal Structured Notation (GSN)

Identify how the tasks and deliverables of MIL-STD-882C can be better used to minimise project office compliance finding burden

Develop ‘advise to contractors’ guidance and model text for the ASDEFCON contract templates.