Duane J. Truitt - A Practitioner's Response to "Occidental Engineering"

Commentary On
Occidental Engineering

The Occidental Engineering case study, authored by Michael S. McFarland, S.J. and published on the Online Ethics Center, involved a discovery of a software coding bug affecting the life-safety performance of a new air traffic control and monitoring system to be delivered by Occidental Engineering to its client, the Federal Aviation Administration. The bug was fixable, but not within the contracted schedule. The chief designer who discovered the bug brought it to the attention of his project manager and requested additional resources (time and labor) to fix the bug prior to delivery to the client for their subsequent review and testing. The project manager argued that any such delay would result in irreparable harm to the company and its employees due to expected draconian punishment from the client, and that the bug would get fixed eventually anyway in a subsequent revision of the software following client review. The project manager also argued that the company could not disclose the error to the client, even though contractually the company was required to certify there were no known bugs. The software designer allowed himself to be talked out of reporting the bug to the client by the project manager, and then he subsequently retired. The bug was eventually fixed before the new system went live.

The author of the case study undertook an extensive review of fundamental ethics theory, and made occasional references back to the specifics of the Occidental Engineering case study. At the end, the author attempted what I believe is an unjustified excusal of the two principal parties (the software designer and the project manager) of their ethical malfeasance by blaming the affair on the shortcomings of the institutions involved, mostly Occidental Engineering (for underbidding the job and forcing the work to be done without sufficient resources of man-hours and schedule, and thereby putting the project manager and project staff in an untenable position), and perhaps to some degree assessed some blame to the client organization, the FAA (for using such draconian punishments for failing to meet a production schedule). Mr. McFarland lets the two principals off the hook essentially

by concluding that the institutions otherwise put too heavy a burden on them personally in requiring them to cover up for the company’s malfeasance in bidding the work.

I disagree with this conclusion and approach by the author, for the following reasons:

1) The company and the project team – particularly the project manager - failed to properly plan the work and provide sufficient resources to complete the work to the required work and product standards. That is a fundamental responsibility of both the company and the PM. Proper planning, including risk management planning and dealing with defects in designing new code, is integral to the business of designing new software. There should never be “last minute” surprises in a well-managed engineering design project.

2) Dishonesty, as practiced deliberately by the PM in this case study, violates the ethical standards of the project management profession, as documented in the Project Management Institute (PMI), which certifies project management professionals. The PMI Code of Ethics and Professional Conduct, Chapter 5 Honesty, as follows:

> **CHAPTER 5. HONESTY**
>
> **5.1 Description of Honesty**
>
> Honesty is our duty to understand the truth and act in a truthful manner both in our communications and in our conduct.
>
> **5.2 Honesty: Aspirational Standards**
>
> As practitioners in the global project management community:
>
> 5.2.1 We earnestly seek to understand the truth.
>
> 5.2.2 We are truthful in our communications and in our conduct.
>
> 5.2.3 We provide accurate information in a timely manner.
>
> 5.2.4 We make commitments and promises, implied or explicit, in good faith.

5.2.5 We strive to create an environment in which others feel safe to tell the truth.

5.3 Honesty: Mandatory Standards

As practitioners in the global project management community, we require the following of ourselves and our fellow practitioners:

5.3.1 We do not engage in or condone behavior that is designed to deceive others, including but not limited to, making misleading or false statements, stating half-truths, providing information out of context or withholding information that, if known, would render our statements as misleading or incomplete.

5.3.2 We do not engage in dishonest behavior with the intention of personal gain or at the expense of another.

Most State engineering laws and practice rules also prohibit licensed Professional Engineers from communicating untruthfully to the public, and to their employers, and to their clients.

3) It is true that the project manager owed a fiduciary duty to her employer, Occidental Engineering, and the employees who depended upon this contract for their jobs. However, inasmuch as the hidden bug involved a function that is life-safety critical – failure of which could kill innocent crew and passengers (potentially many hundreds who might die in a mid-air collision involving multiple airliners) of aircraft being monitored and controlled by the system – the interests of the client and of the users of the air traffic control system greatly outweigh any such fiduciary duty owed to the company by the PM. The fact that the software bug did not actually kill anyone is immaterial – it very easily could have. Replicated multiple times it is actually fairly certain that eventually such a “killer bug” would make it through the system undetected by the client and actually kill innocents, as in the Morton Thiokol Challenger accident that the case study author made reference to in his concluding sections.

4) The author could have productively spent less time and words on describing the multiple theories of ethical behavior. Instead, a more useful analysis would focus on how to achieve potentially satisfactory outcomes for the project manager, the software designer, the company, and the client (and their aviation end users) that

would not have involved tolerating such a potentially tragic flaw in the work product, and which would have allowed the ethical responsibilities of all parties involved to be adequately discharged.

- For example, after the bug was identified by the designer, the PM should have discussed the case with senior management in Occidental Engineering, in order to provide senior managers an opportunity to weigh in and make a proper decision. The consequences of the contractor hiding the bug could not only kill innocent people, but, as a result of a post-mortem review of such a failure, revelations of the cover-up could easily result in levying the “death penalty” (a ban on future contracts) against the company as a Federal contractor, destroying its reputation, perhaps even destroying the entire company. The PM had no right to make such a decision on her sole volition; her actions indeed it make it appear that perhaps her principal concern was not for the company or her co-workers, but in escaping criticism from senior management for her performance as a project manager. It may well be that the company managers would make the right decision and properly disclose the bug to the client, but either way it relieves both the PM and her project team of a responsibility that rightly belonged higher up the chain of command.
- Another example: the company should have disclosed the defect to the client when delivering the software, and in doing so made specific commitments to correct the bug in the next release of the code. The client might not have been ecstatic to learn that the software has known bugs in the beta release, but anyone at all familiar with computer software knows that there is no such thing as bug-free software, particularly in an initial “beta” release issued for client testing. I believe that a reasonable client would accept such notification of that defect as evidence of a professional supplier with adequate concern for quality and commitment to honesty. As a client I would never trust any software developer that tells me their initial release was “bug free”. While it is possible that the client might downgrade the supplier for delivering beta software including such bugs, it is highly unlikely that the “death penalty” (contract termination) would be the result. Virtually all engineering design firms (and their errors and omissions liability insurance carriers) strive to write service contracts with clauses that specifically address defects and their correction. Such clauses provide for specific timeframes in which known or identified defects can be corrected without major penalties or contract termination. Full disclosure of all known defects to the client also flags the issue

for the attention of the client to ensure that the bug is actually fixed.

Certainly the FAA retains some responsibility for their contracting and procurement processes and standards if they do not provide for reasonable selection methods and adequate compensation of contractors. Likewise effective contract documents also provide for adequate means and schedules for correcting identified defects in work products, especially those defects that involve or affect life-safety performance. “Low ball” bids – and the procurement processes that produce such bids - are or should be avoided, or at least viewed with extreme skepticism by the client’s source selection team. It is imperative for the buyer to ensure that the winning design proposals are actually reasonably priced, and that the design contractor is actually fully prepared to deliver as promised for the proposed price. Source selection for life-safety or other mission-critical engineering systems design should never be made on the basis of “low bid”. Indeed several of the major engineering professional societies discourage, and many State public agency engineering procurement laws prohibit, the bidding of engineering design services by government buyers.

As the bottom line in this discussion, and writing here as both an experienced engineering contractor and an experienced purchaser of engineering services, I can say that these kinds of situations are unfortunately extremely common, yet effectively manageable. If contract procurement and management are handled openly and honestly by all parties, with reasonable expectations in a spirit of cooperation and dedication to providing the “best value” to the client’s sponsors (in this case, the taxpayers, and for private entities, the owners or stockholders), the desired contract performance in most cases is not difficult to deliver. It is wise and useful to understand that no project of any nature ever executes perfectly, and that no engineering work product, especially not an initial or “beta” release of a software product, is ever going to be defect-free. So our challenge lies in anticipating, avoiding, correcting, and in some cases mitigating the risks of product defects.

It is very important to determine that the testing and review regime per the contract documents is adequate to identify all of the life safety-affecting bugs and other errors or defects, so that same can be corrected in a reasonable timeframe. Contract procurement and management regimes that are based upon an assumption of rigid perfection, with concurrent draconian punishments meted out for any imperfections, are destined to produce failures, often of the most spectacular kind. Open and honest communication, combined with trust and reasonable consequences for less-

than-perfect performance, are the most likely means to produce the desired final results. The financial costs of correcting any identified defects, of course, must by borne in accordance with the terms of the contract documents via such mechanisms as warranty clauses, bonding, and/or performance-based contract compensation. The absolute worst outcome is when defects are not properly identified, tested and evaluated, or even disclosed once known, out of fear of excessive punitive reactions by the client, or by the employer of the project team. In the case of life-safety engineering systems, what we don’t know can kill us. Honesty and trust by all parties involved are not just “nice to have” – they are both essential to a successful outcome.

This text is a critique of the Occidental Engineering case study. You may also read Michael McFarland's Response to Practitioner on "Occidental Engineering."