More and more energy suppliers and manufacturers are being hit by the most spectacular and far-reaching software failures. This is reflected in a recently-conducted survey by SQS Software Quality Systems AG for 2013. At the end of every year, the company asks its consultants to name the top 10 software failures from the last twelve months, and here are its top ten from 2013:

1. Launch of ‘Obamacare’: software swallows a third of insurance applications
The politically controversial ‘Obamacare’ health insurance programme in the USA made fresh headlines when it was launched.

In the autumn, the healthcare portal responsible for handling the insurance was exposed to fierce criticism of its software from many quarters. The most serious defect was that around a third of the insurance applications could not be processed at all to begin with. Because of software errors, the application forms filled in on the portal were stuck there and did not reach the insurers concerned.

One reason was a system routine which prevented the social security number from being entered. The people affected then risked receiving no insurance cover even though their applications were correct. Along with this major fault, many users also complained about the poor usability of the software and errors in the forms. Around 35,000 users also had difficulties logging in for more than a week, although the system was in fact designed to support around 800,000 users. Those responsible for the healthcare portal therefore advised applicants to contact the insurers directly to check whether they had received their applications as indicated.

2. Near-blackout of the national grid in Austria
A simple meter reading query brought the Austrian national grid to the brink of total collapse in May last year, also jeopardising electricity networks in other European countries.

A command had been misdirected into the control system for the European electricity networks during the commissioning of a new natural gas control system in southern Germany, almost bringing the whole grid down. The automated function then acted like a ‘distributed denial of service’ (DDoS) attack, where hackers bring a server to its knees with a deluge of queries. When the system failure was publicised, a representative of the electricity regulatory authority told Austrian Radio (ÖRF) that security levels in the energy providers’ IT systems needed to be improved.

3. Private data on six million members of a social network made public
The software failure that produced the most headlines in 2013 was down to one of the world’s leading social networks.

This caused the private contact details of around six million of its members to be made public. Their e-mail addresses and telephone numbers were visible to outsiders for about a year. The cause of this was a software error in a system on the network that generated recommendations for new ‘friending’ requests. On average, it seems the contact details were shared once or twice without permission. All the users concerned were informed of the failure by e-mail.

4. German university ‘dissmisses’ 48,000 students and staff
“In twelve days your login will be blocked. This is because you have left the university, your employment contract has ended or your guest login has expired.”

This e-mail went out to 37,000 students and 11,000 employees of a major German university one Sunday morning last year. A software error in the university’s data centre was responsible for the misinformation. Problems in reconciling staff and student data then caused the e-mail to be circulated. A spokesperson for the
university tried to see the funny side of the supposed mass dismissal, “I presume the Rector got the message as well,” she said.

**5. Preparation for SEPA: banks transfer sums of money twice**
A regional banking group in Germany transferred sums of money for thousands of customers twice by error.

The fault, which affected its standing orders, also failed to execute many transfers on the specified processing date. The cause was a software error in a new program to convert the accounts to the new SEPA (Single Euro Payments Area) standard. In the course of this conversion, the new SEPA-compliant standing orders were set up successfully in the new system, but the old ones were not deleted. This caused duplicate transactions. The customers concerned had the incorrectly transferred sums refunded immediately, with interest.

**6. Trading on the US Nasdaq exchange crippled for three hours**
For about three hours, trading in shares and options on New York’s Nasdaq exchange ground to a halt.

Software errors brought about this total failure two and a half hours after the start of trading one day last August. The source of the problems was the ‘Securities Information Processor’, which swaps share prices with other exchanges. During the shutdown, the exchange operator temporarily froze all prices and listings. Almost 30% of all shares on US exchanges are traded on the Nasdaq, including Apple, Facebook, Google and Microsoft. This meant that the blackout also affected the pricing behind other major US indices like the Dow Jones and the S&P 500. The failure was not the first of this kind to hit US exchanges. The year before, for example, a trading platform had to call off its own IPO because of a software error in the trading system.

**7. New high-speed train hits the tracks two years late**
A major European rail operator had to wait two years longer than originally agreed with the manufacturer for 16 new high-speed trains.

One reason for the delay to the high-tech trains was that a software error held up the scheduled acceptance testing by the authorities. The error in the train control system caused the brakes to be applied with a second’s delay. Other problems with the brakes, and also with the air-conditioning system, had already blown the scheduled delivery date. The delayed delivery led to significant bottlenecks for the railway company concerned. Train delays and cancellations were the result. In compensation, the manufacturer of the new trains is offering to supply the operator with an extra train worth EUR 30 million.

**8. Hundreds of flights cancelled or delayed by telephone crash**
When a software error crippled the internal phone system of a major European air traffic control centre, both passengers and airlines were faced with huge delays.

Hundreds of flights were cancelled altogether. Some 1,300 flights, or 8% of European air traffic, suffered delays of up to several hours. The telephone crash, which lasted for 12 hours, meant that the authority could only process the day’s flights after a delay, if at all. The fault arose when the systems were switched from nighttime to daytime operation in the early morning. The affected system was not just a simple telephone exchange. It was used by air traffic controllers to communicate with their colleagues in other national and international control centres.

**9. Millions of customers without phone and text services**
Six to seven million customers of a national network provider had to get by without mobile calls and text messages for four or five hours one day in October last year.

Because of a software error, the relays in the telephone network were temporarily flooded with network signals. This caused the relays themselves to shut down and restart, in turn causing the whole network for phone calls
and text messages to collapse, especially as the relays took longer to reactivate. Data services were not affected by the system failure.

**10. New logistics software stops spare parts for cars**
Last year, the workshop customers of a major German carmaker had to wait for over a week to receive the spare parts that they needed.

The reason was a software change in the firm’s central logistics system. In the days and weeks after the change, a backlog of up to 200,000 parts built up. Some 5,000 dealers and branches around the world were affected. Curiously enough, customers in the immediate vicinity of the central warehouse suffered especially long waiting times, as this supplies them directly. To limit the damage to customer satisfaction, the carmaker ordered its staff in the central stores to work extra shifts at the weekend and overnight.

“At financial service providers, telecommunications companies and public authorities, important services have been dependent on IT systems ever since the 1990s. That is why they have also dominated the annual top 10 for a long time,” Jochen Brunnstein, Principal Consultant at SQS Software Quality Systems, says of this year’s list. “Manufacturers and utility companies, on the other hand, are relatively new to the list. Their core business is only now being really revolutionised by software. Examples of this are the great advances in automotive electronics, and smart metering from energy suppliers.”

This year’s list also shows that serious software failures rarely cause just a loss of image. “Let’s take the example of Obamacare: the jerky start caused by poor software also left substantial political flood damage in its wake,” adds Brunnstein. For private companies, on the other hand, major software failures almost always bring significant financial losses. As Brunnstein says, “In these cases, the financial damage is always many times more than the necessary preventive and systematic software quality assurance would have cost.”
The Expeditionary Combat Support System (ECSS) was a failed enterprise resource planning software project undertaken by the United States Air Force (USAF) between 2005 and 2012. The goal of the project was to automate and streamline the USAF's logistics operations by, in part, consolidating and replacing over 200 separate legacy systems. Development of the system was originally contracted to the Oracle Corporation in 2005, and was later supervised by Computer Sciences Corporation.

After spending $1.1 billion on its development, the USAF concluded in 2012 that the system, "has not yielded any significant military capability" and estimated that, "it would require an additional $1.1B for about a quarter of the original scope to continue and fielding would not be until 2020." Based on that conclusion, the USAF canceled the program in November 2012.

**FLOOR REMARKS BY SENATOR JOHN MCCAIN ON THE AIR FORCE’S ECSS PROGRAM**

**Jul 07 2014**


Washington, D.C. – U.S. Senator John McCain (R-AZ) today delivered the following statement on the Air Force’s Expeditionary Combat Support System (ECSS) program that squandered over $1 billion in taxpayer funds on ECSS over eight years:

"Mr. President, at a time when vital defense programs are threatened due to lack of funding, the federal government has wasted billions of dollars attempting to procure new large information technology (I.T.) systems – consistently disregarding lessons-learned from past failures and well-established acquisition ‘best practices.’ Even with a current annual budget of $80 billion dollars for information technology projects, the federal government struggles to make those systems work. The American people can still remember the embarrassing failure of Healthcare.gov, the Obama Administration’s most recent information technology fiasco. But, what they may not realize is that the Health & Human Services’ Healthcare.gov mess is not unique and is – in a very important sense – merely business-as-usual in how the government (particularly the Department of Defense) acquires large I.T. systems.

"Indeed, the Pentagon is responsible for many of the most egregious cases of wasted taxpayer dollars when it comes to government I.T. programs. Lack of planning for these acquisitions within the armed forces has made the adoption of new information technology systems an expensive and risky endeavor. The Air Force’s Expeditionary Combat Support System, or E.C.S.S., is a prime example of how a system designed to save money can actually waste billions of taxpayer dollars without producing any usable capability.

"Today, the Permanent Subcommittee on Investigations issued a bipartisan report on the failed acquisition of E.C.S.S., a program that was supposed to decrease costs and increase efficiencies by consolidating the Air Force’s hundreds of legacy logistics systems into a single new system. It is important to recognize that what happened with E.C.S.S. is not an isolated case of incompetence. Unfortunately, it is one of many examples that show how billions of dollars can be wasted if the intended acquisition is not started-off right – with a detailed plan that includes clear, stable requirements and achievable milestones, supported by realistic original cost estimates and reliable assessments of risk.

"The Subcommittee’s report notes that the Air Force started the E.C.S.S. acquisition in 2004 with the goal of obtaining a single, quote ‘transformational,’ unified logistics and supply-chain management system that would allow the Air Force to track all of its physical assets worldwide, from airplanes to fuel to spare parts. These types of computer platforms, that is, large business systems that companies use to make their businesses operate more efficiently, are known as ‘enterprise resource planning’ systems, or E.R.P.’s. So, basically, E.C.S.S. was supposed to be an E.R.P. that would have combined all of the Air Force’s global logistics and its associated supply-chain management activities under one streamlined management I.T. system.
“As the Department of Defense’s overall strategy to become fully auditable hinges on how successfully it procures and integrates those E.R.P. systems into its business enterprises, failures like E.C.S.S. are not only costly to the taxpayer but also disastrous to the Department’s larger financial improvement efforts.

“To keep costs down, the Air Force intended to build its new E.R.P. system using already available commercial software instead of a software system designed from scratch. That type of commercial software, however, works best when the organization using it follows efficient business processes. So, in order to take advantage of the commercial software that supported E.C.S.S, the Air Force needed to dramatically change long-standing internal business processes that supported how it managed global logistics and its associated supply-chain.

“That never happened. Unfortunately, the culture of resistance to change in the Air Force made it difficult to make those changes. The Air Force needed strong leaders who could communicate not only the goals of E.C.S.S. to end-users and get their buy-in but also develop sound program management strategies to overcome resistance to change among those lower-level personnel. Ultimately, the leaders of the E.C.S.S. program did not effectively communicate with the end-users. Without their buy-in, E.C.S.S. was doomed to fail before it even really started.

“Because the Air Force had not adequately planned what needed to be done to procure E.C.S.S. effectively, it was easier for program managers to just order changes in configuration that in effect customized the commercial software on the fly, rather than alter the Air Force’s own culture. That caused costs to skyrocket and delivery schedules to slip.

“The Air Force’s eagerness for expensive customization was especially troubling given that, as early as 2004, the Air Force identified the need to avoid customizing the commercial software lest costs explode. But, in the end, it failed to heed its own advice. The Subcommittee report finds that the Air Force’s customization of the commercial software was a major root cause of E.C.S.S.’s failure.

“Such customization could have been avoided had the Air Force fully and timely implemented a congressionally-mandated procedure for improving its operations called ‘business process reengineering,’ or B.P.R. B.P.R, which is a proven private-sector management approach, offers a structured way to introduce major new changes into an organization to help it run more efficiently, and ensures that careful planning goes into every stage. Not infrequently, Fortune 500 companies use B.P.R. to, for example, restructure existing business units to work more efficiently – passing resulting savings on to consumers – and to absorb effectively new business units from companies that they’ve acquired or merged with to maintain overall competitiveness in the marketplace.

“Had the Air Force actually used B.P.R. in connection with E.C.S.S., that is, redesigned those business processes that needed to be changed for the Air Force to have absorbed its commercial off-the-shelf software effectively, the risk identified in 2004 would have been consciously addressed at each stage of the procurement, not essentially disregarded for eight years.

“In its 2004 risk assessment, the Air Force also identified a lack of stable program requirements as a risk to the program. That risk, too, was not accounted for. From the beginning of the E.C.S.S. procurement, the Air Force failed to properly define and stabilize the program’s requirements – what the system would do and how it would do it. Even those who were going to use E.C.S.S. felt like they were in the dark. In 2008, a technician stated, quote, ‘My [number one] complaint is that E.C.S.S. has yet to identify … any timeline [for when] we can expect to receive detailed information [or] requirements about what E.C.S.S. will provide.’ This user’s complaint reflects the lack of planning that went into the Air Force’s attempt to procure E.C.S.S.

“To date, the Air Force still does not know how many legacy systems it actually has on hand, let alone the number that E.C.S.S. was to replace. The Air Force’s lack of knowledge about its current information technology systems led to confusion when it tried to construct a replacement. That is why I successfully offered
an amendment to the National Defense Authorization Act for Fiscal Year 2015 that would require program personnel to have a proper understanding of existing legacy systems and clear goals in connection with its efforts to procure new information technology systems.

“But more has to be done. As the Subcommittee’s report recommends, the Department of Defense should also start assessing how much B.P.R. would need to be done (and how feasibly it can be done) earlier in the acquisition lifecycle of these E.R.P.’s. Also, ‘investment review boards,’ which are critically important governance tools used in connection with the Department’s efforts to procure E.R.P.’s, should be integrated into the budgeting process when these programs begin. That would help make sure that not only is B.P.R. being implemented early and effectively but also that the large information technology system being procured lines-up with the Department of Defense’s broader efforts to modernize its business systems. Collectively, these initiatives would help these programs start-off right, and allow both the Department of Defense and Congress to conduct better oversight and hold leadership accountable for future failures.

“In this case, however, no one within the Air Force and the Department of Defense has been held accountable for E.C.S.S.’s appalling mismanagement. No one has been fired. And, not a single government employee has been held responsible for wasting over $1 billion dollars in taxpayer funds. With six program managers and five program executive officers over eight years having transitioned in and out of the program, the Air Force has had trouble determining who should be held responsible. On scores of other failed programs, this, of course, is a story we are well familiar with.

“This chronic lack of accountability is why I support efforts in the National Defense Authorization Act for Fiscal Year 2015 to align the tenure of program managers with key decision points in the acquisition process. That provision, if enacted, would allow us to not only hold accountable those responsible for blunders like E.C.S.S. but also to reward those involved with successful acquisition strategies.

“The Subcommittee’s report details many leadership failures within the Air Force and the Department of Defense in the E.C.S.S. program that should serve as a warning for current and future major information technology acquisitions. Since 1995, the Government Accountability Office has placed the Department of Defense business systems modernization efforts (that is, its efforts to replace its existing information technology systems to improve how the Department of Defense is managed) on its high-risk list every year. And, it has been on that list for many of the same reasons that E.C.S.S. failed, including inadequate management controls to oversee how it acquires these large systems.

“According to the Government Accountability Office, the Department of Defense, quote, ‘has not fully defined and established business systems modernization management controls.’ It further noted that those management controls are, quote, ‘vital to ensuring that [DOD] can effectively and efficiently manage an undertaking with the size, complexity, and significance of its business systems modernization and minimize the associated risks.’ I challenge the new Deputy Secretary of Defense, who acts as the Chief Management Officer, to work with the Government Accountability Office to get the Department of Defense’s business systems modernization efforts off the high-risk list, and I look forward to a plan from him on how he intends to do that.

“Such a plan is clearly necessary, given the current difficulties the Department of Defense is facing in procuring major information technology programs. The Army, for example, has spent roughly $1.8 billion dollars on its Logistics Modernization Program (L.M.P.). Yet, just recently, in May of this year, the DOD Inspector General reported that the Army will most likely miss the congressionally mandated auditability deadline in September 2017, because it failed to properly implement B.P.R.

“Additionally, the Defense Enterprise Accounting and Management System, or DEAMS, a current Air Force acquisition effort that has received roughly $425 million in funding and is scheduled to receive billions more. DEAMS has faced similar issues to those witnessed in the failed E.C.S.S. procurement program. For instance, similar to E.C.S.S., the Air Force has been frustrated by its inability to get the buy-in it needs from DEAMS’s
intended end-users for them to change their business processes and allow for DEAMS’s integration into the Air Force.

“According to a December 2013 DOD internal report, end-users at McConnell Air Force Base indicated that the training for DEAMS, quote, ‘did not provide them with a real understanding of the system and its application to their day-to-day work process.’ Sound familiar? In the case of DEAMS, the Air Force and the Department of Defense is again failing to properly procure and implement an E.R.P. program that is crucial to its business operations and to the Air Force’s becoming fully auditable by 2017.

“The Navy has also struggled with the procurement of large information technology, as a program called Navy E.R.P. illustrates. According to the Department of Defense’s Deputy Chief Management Officer, B.P.R. guidelines demand that program offices for information technology acquisitions effectively map-out current legacy systems and business processes that need to be changed or retired and then lay-out a new plan that would improve and transform the shortcomings of the old systems. These ‘as-is’ and ‘to-be’ process maps help guide the DOD components and agencies in how they procure large information technology systems.

“But, when the Department of Defense Inspector General asked the program office for Navy E.R.P.’s process maps, disturbingly, the Navy said that no such plan existed. This is particularly unsettling because the Under Secretary of the Navy at the time, who is now the Deputy Secretary of Defense, certified that those plans were actually completed.

“In addition to the lack of process maps, the Department of Defense Inspector General found that Navy E.R.P. could not be used to track and account for the Navy’s $416 billion dollars in military equipment assets. That means Navy E.R.P. would not even allow the Navy to become fully auditable as required by Congress, raising questions about why the Navy would spend $870 million dollars on a program that wouldn’t even fulfill congressional mandates.

“This lapse in oversight is unacceptable, which is why the Subcommittee’s bipartisan report recommends that the Department of Defense review its internal policies to make sure that I.T. systems that receive B.P.R. certifications on paper are actually implementing B.P.R. in reality.

“These certifications are required for a reason: they help decision-makers in the Department of Defense and Congress make informed decisions on whether a given program is ready to go further in the acquisition process and whether taxpayer funds should be authorized and appropriated for that purpose.

“As I mentioned earlier, information technology procurement is not only a Department of Defense problem. In November of last year, in response to the disastrous Healthcare.gov rollout, President Obama himself said that quote, ‘One of the things [the federal government] does not do well is information technology procurement. This is kind of a systematic problem that we have across the board.’ While I wish the President would have kept that concern in mind before committing over one billion dollars to Healthcare.gov, I agree with him that information technology procurement in the federal government is in desperate need of reform. The White House’s Office of Management and Budget has expressed significant concerns about 42 federal information technology investments, totaling $2 billion dollars. According to the Government Accountability Office, quote, ‘despite spending hundreds of billions on I.T. since 2000, the federal government has experienced failed I.T. projects and has achieved little of the productivity improvements that private industry has realized from I.T.’

“The Department of Homeland Security’s Secure Border Initiative program, or S.B.I.net, was another notable major I.T. procurement failure. You might remember S.B.I.net as the high-tech surveillance program that, when it began in 2006, promised a single, quote ‘transformational,’ integrated security system for hundreds of miles of border protection. Well, I remember S.B.I.net as a system that, according to the Government Accountability Office, cost $1.2 billion dollars and was on a path to spend 564 percent more than its initial cost estimates when it was cancelled in 2010. Once again, ever-changing requirements; a lack of internal management controls; and
not really understanding what we were trying to procure, how hard it would actually be, and planning effectively for those difficulties, led to the federal government’s squandering over $1 billion with nothing to show for it.

“The federal government’s incessant inability to procure major information technology systems is especially concerning since, in the coming months, the Department of Defense will be selecting a contractor to develop a centralized military healthcare information technology system. That program is supposed to provide seamless sharing of health data among the Department of Defense, Veterans Affairs, and private sector providers. In light of the recent tragic consequences stemming from mismanagement at the Phoenix VA Healthcare System and VA hospitals around the country, we can’t afford to further jeopardize veterans’ healthcare because of information technology failures. And yet, any serious effort to reform how care is delivered to our veterans will largely turn on the effective delivery and integration of this system. I am putting the Department of Defense and the Department of Veterans Affairs on notice that we will monitor this program carefully throughout its acquisition.

“In closing, Mr. President, there is still much to be done at the Department of Defense and throughout the federal government to ensure the acquisition of large information technology programs is improved. If we don’t want to repeat past failures, the Department of Defense’s attempts to procure large business I.T. systems must be supported by the right leadership, proper planning and a workforce that is open to changing ‘business as usual’ in order to help make sure the Department operates more efficiently, effectively and transparently.

“Thank you, Mr. President.”

BB

CSc 233 Spring 2015