Legacy Telecommunication Systems

Theme Editors Introduction

Matt Tett
Enex TestLab

Abstract: The subject of legacy telecommunication systems is often overlooked in the pursuit of technological advancement, yet somehow the result is often less than graceful with end users left walking a tightrope between technology they are familiar with, and the evolving replacement systems.

Introduction

Legacy Systems are all around us, whether we like it or not. If those futurists amongst us are correct then we are going to see an ever increasing prevalence in the coming few years with connected technology supplanting many legacy devices in our day-to-day lives through the "Internet of Things (IoT)".

Almost every aspect of our business and personal lives touch legacy devices, from financial through to traffic systems.

Human nature is most comfortable with familiarity; therefore change is often resisted. Organisations logically take a risk averse approach when deploying new technologies. Whether from a disaster recovery perspective, "let's just leave the old system running until the new one is bedded in and proven." To issues with migration, "the new system does 90% of the work the system it is replacing, so let's just leave the old one handling the 10%."

Legacy systems ironically are often here to stay, and the longer they are left the less people know about them – developers, system admins, even technicians are long gone. I recall a client who was in the wholesale supply of petroleum products, a middle-man as it were, they had their core server system which handled all their day to day transactional processing which was over ten years old. Their CIO once said to me during an audit, don't breath, or go near that box it handles over $2m a day and we don't know how it works, if it goes down, we're stuffed (I wonder what their governance team thinks of that?). Similar stories are

http://doi.org/10.18080/ajtde.v3n2.X

heard the world over. We all know custom software owners who have no access to their code and the original developers are likewise long gone, they have no path to change or even remediate security issues should they arise, so their solution generally is to try and plug the gaps with other technologies glued together, making an existing problem even worse.

Critical infrastructure has been a victim of legacy services for a long time, with the advent of the Internet and lower cost public communications networks people often find a quick "fix" is to put systems online that were never intended to

Financial services are also critical; many core-banking systems are long overdue for replacement or updating. However the standby claim is that "the system is too BIG." Therefore bolt-ons and stopgap fixes abound. This doesn't necessarily make them any less secure or functional, but it is not very efficient.

Another client, a very large retailer, still ran a mainframe system nationally, and their comfort came by the fact that their multinational vendor continued to provide annual support contract, albeit at a significant premium, but more importantly supplied replacement parts, so while the base software system was in the dark ages, the hardware could still be maintained and therefore keep their shaky system up. Inevitably the vendor finally pulled the plug and said they no longer could manufacture replacement parts. Most businesses would have seen the writing on the wall years before and planned a replacement, but no, this client following in the footsteps of our other client, decided it was better to pay for continual environmental monitoring of the equipment with alerts going off should the, temperature, humidity etc change. In the vein hope that any variation would indicate a prospective issue coming.

The greatest ones we have heard of though come when a supplier is seeking to change a fundamental piece of the jigsaw puzzle. We operate a network connected device interoperability test laboratory that enables technology vendors to come in and test their existing products on nbn services. The original premise under the former government was that as the copper network was replaced by fibre networks certain legacy technologies needed to be tested to ensure that they continued to operate. This is particularly critical in systems such as remote/tele health care and monitoring and alarm systems, such as medical, intrusion etc. There are also a plethora of other legacy systems connected to the PSTN/POTS network which boggles the mind, traffic control systems, vending machines, accessibility devices. With the new government the move to multi technology mix means that the interoperability lab is even more relevant as vendors need to ensure that their existing products remain compatible and that future changes and emerging products interoperate across all the network delivery technologies.

http://doi.org/10.18080/ajtde.v3n1.X

What added further complexity is the number of Retail Service Providers (RSP), each with their own configuration. So the vendors don't just test against a National Broadband Network service, they also test against the services offered by each of the RSPs.

With the coming of the IoT this is going to be increasingly more relevant. Likewise mobile networks, and particularly where vendor technologies rely on an "always" on, or "always" up network connectivity. Since the demise of dedicated copper services, critical legacy systems, such as healthcare, ATM/EFTPOS, wagering/lotteries and alarm monitoring systems providers are having quite a time seeking the backup route back to their bases. Often moving from two terrestrial/cabled services to a mobile service. These in themselves can prove problematic due to interoperability/compatibility issues with the technologies as carriers may have differing configurations. A prime example is mobile and satellite communications networks where the network traffic these days has a variety of systems in place which seek to optimise packets and prioritise various traffic classes.

Conclusion

Bottom line is that legacy systems are here to stay, and while our communications networks are becoming ubiquitous and advancing in technological leaps and bounds, the providers and vendors, on both sides of the table, need to be aware of the impact that change can bring and ensure that their customers and ultimately the end-users continue to be the beneficiary of the technology delivered in the first-instance.

http://doi.org/10.18080/ajtde.v3n1.X