Information Security Now – 41

John Mitchell

The standard definition for a safety-critical system (SCS) ’is a system whose failure or malfunction may result in death or serious injury to people and/or loss or severe damage to equipment/property’. Although the word ‘directly’ does not come into the definition the implication is that the system’s failure will have a direct impact on life, or critical equipment. Looking at today’s inter-connected world I am minded to expand this definition to include those systems which could indirectly impact on those aspects. For example, a melt-down of our financial systems could lead to civil unrest with people dying, or critical infrastructure being destroyed, as a result.

I first became interested in safety critical systems when working for British Gas back in the early nineteen eighties. Getting the gas from the North Sea to the consumer required some fancy engineering work and involved complex computerised control systems. There were plenty of manual overrides and although the exposure window for an incident was relatively short it was long enough for either the back-up system to kick in, or the human to intervene. In those days, many safety critical systems related to energy supply and the Critical National Infrastructure (CNI) was mainly centred on energy and transport. Since those early days the CNI has expanded and is now heavily dependent on computers to control every service on which the nation relies. So today, when we think of the CNI we tend to include SCS as part of the equation

Two of the main SCS components are resilience and recovery, so it stands to reason that any SCS design has to consider the threats and associated counter-measures to those components. Based on this, we may not have done some of the things that we have done in the past, where economic considerations took priority over the risk. An example is the electrification of our railway services. Prior to electrification each locomotive had its own individual power source which could operate independently from the others. The non-availability of one service did not have a significant impact on the other locomotives. With electrification, all locomotives became dependent on power being constantly and consistently available. In the event of an outage all units are affected. Back-up power supplies are redundant if the transmission method is destroyed, so we have situations where the power may be available, but we do not have the ability to deliver it to where it is required. So although on the surface we have good resilience via the back-up power, in practice the weakest point is the delivery mechanism; the wires. A single point of failure which negates the entire end-to-end delivery system. When it comes to recovery we may have to replace gantries and wires over several miles, or in the event of major destruction we may not be in the position to replace the lines for several months. In such a case getting a train service up and running again may well depend on having a reserve of independently powered diesel-electric locomotives. A case of old technology coming to the rescue of the new.

You may think that this is rather tangential when discussing SCS in the sense of them being computer based (this is after all an IT magazine), but the computers are only there to support the entire system. It is therefore essential for an SCS that we examine the total system and not just the IT component. This means that the requirements specification and subsequent design should examine the totally of the service being provided. The Americans may have used triple-redundant computers on their space shuttles, but still managed to lose two of them. And it's not just the design of the logic, but also the integrity of the data being processed. The loss of Air France 447, which crashed into the Atlantic on the 1st June 2009 killing all 288 people on board, was caused by the absence of data when ice crystals blocked the plane's pitot tubes, which are part of a system used to determine air-speed. The autopilot disconnected and the pilots were left without adequate information to correct the situation. In this case the SCS acted correctly in disconnecting the autopilot because it had insufficient data to fly the aircraft, but the long-stop of human intervention failed because they had not been adequately trained to deal with such a situation. So, the SCS should not only consider the system's logic, but also the quality, or absence of the data being processed and the likely effectiveness of any human intervention. Anyone who has been involved in risk analysis will recognise the absence of data from the pilot tubes as being a key risk indicator (KRI). The underlying principle of a KRI is that once it is triggered immediate action is required. That is why the preparation of a risk register should be a requirement for any SCS.

The main sections of the register for a SCS are the same as for any computerised system: confidentiality, integrity, availability and compliance of each component. Each of these elements can be modelled and tested during the design phase, with the design being modified accordingly. There may well be several thousand identified risks for a complex SCS, but this is no reason not to prepare and maintain a risk register throughout the life of the system. In fact, it is all the more reason to do so, as we would not want to miss a significant risk, or chain of risks. We know from experience that it is often several small things in a chain which results in the final catastrophic failure; such as the Air France disaster. The register not only provides a basis for action, but also for independent review. Is it comprehensive? Have the inherent risks been correctly scored? Is the action decision (tolerate, treat, terminate, transfer) reasonable? Will the defined controls mitigate the inherent risk to an acceptable residual level? Are management aware of their risk appetite and tolerance?

The UK has a Safety-Critical Systems Club (SCSC) which has some 1,400 members and which celebrates its 25th anniversary this year (http://scsc.org.uk/). Considering that our financial services rely on computer systems and that any interruption to these can have a significant adverse impact on our economy, then I am disappointed that only a handful of financial services organisation are members. After all, having the economy grind to a halt could have very serious consequences to lives and property.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council, it's Audit & Risk Committee and Chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638