Mission-critical operations: When failure is *not* an option

By Steve Mustard, CAP

The term "mission critical" applies to any activity, system, or equipment whose failure can result in the failure of an organization's operations. Depending on the organization, the consequences of failure can be very wide ranging.

At one extreme, the failure of an online vendor's website can result in a loss of sales. Although this could be disastrous to the business concerned, the impact is limited in scope, and recovery may not be difficult. Most of us, for instance, have experienced problems accessing Amazon, Facebook, Twitter, and so on. These outages may make the news and can result in a significant financial impact for the business concerned, but operations are usually returned promptly, and there are few, if any, lasting consequences.

In the industrial space, reports indicate a tenfold increase in the number of successful cyberattacks on infrastructure control systems since 2000.

At the other extreme, the failure of control systems in a petrochemical operation could result in injury and loss of life to personnel and the public, as well as harm to the environment from which recovery may be extremely time consuming, expensive, and difficult. Consider, for example, the Deepwater Horizon accident in 2010, which caused the largest oil spill ever in U.S. waters. Eleven people lost their lives the day of the accident. The harm to the environment is still being experienced in the Gulf region of the U.S. and will be for many years to come. Currently, the costs arising from the accident, including financial settlements and fines, exceeds $42 billion.

A wide variety of factors can affect mission-critical operations:

- hardware or software failures
- network communications problems
- accidental damage or disruption
- natural disasters
- deliberate damage, such as cyberattacks

Cyberattacks on the rise

One factor making the news regularly is cyberattack. High-profile incidents have affected household names, such as Sony, Target, eBay, P.F. Changs, and Domino's Pizza. In these cases, confidential information was stolen, resulting in the need for major disaster-recovery activities. On 25 December 2014, a group known as Lizard Squad successfully brought down the Xbox Live and PlayStation networks. Approximately 48 million Xbox Live subscribers and 110 million PlayStation users were unable to access their respective networks, causing major disruption on one of the biggest access demand days in the year.

In the industrial space, reports indicate a tenfold increase in the number of successful cyberattacks on infrastructure control systems since 2000. This is partly a consequence of advances in control systems, enabling them to be integrated into the business environment. Although this has proven to be a huge benefit for businesses, allowing better visibility of process information in near real time, the increased connectivity has exposed new vulnerabilities that attackers can target. The connection between industrial (or operational technology) and information technology (IT) systems has created problems for both types of systems. For instance, the Target incident was originated through the HVAC control system. In Germany in December 2014, a steel mill was attacked, and the blast furnace suffered major damage. The origin of the attack was the business network; the attackers navigated through the business network to the control system network and disrupted the emergency shutdown systems that are designed to prevent major damage to the plant.

There are many potential cyberattackers: hackers seeking to prove their capabilities, criminals seeking financial gain, and state-funded operations attempting to damage another state's operations. As a result, mission-critical systems must be designed and operated to cope with accidental and deliberate incidents. In addition, the management of such systems requires an enhanced level of diligence, as the nature and source of threats is always changing.

A cultural change

There is a need for mission-critical operations specialists. These specialists understand the threats, risks, and consequences of failure. They may focus on specific areas, such as robust IT network design, control system security, control room operations, and alarm handling, but they will normally have a broad understanding of all key aspects of mission-critical systems.

There is an acute shortage of suitably qualified and experienced individuals to work in mission-critical systems design and operation. If we are to keep our businesses and our critical national infrastructure safe, we will need a new generation of specialists who understand the importance of the phrase "failure is not an option."

About the Author

Steve Mustard, CAP, has been in the software development business for more than 25 years, including developing embedded software and hardware for military applications and developing products for industrial automation and control systems. Much of his current work involves assessing the cybersecurity readiness of critical infrastructure organizations. Mustard is a U.K.-registered Chartered Engineer, a Fellow of the Institution of Engineering & Technology, a European-registered Eur Ing, and a member of the Automation Federation's Government Relations Committee and the ISA99 committee.

More Workforce Development

Preparing for the future: the human equation

Bah humbug!

Who owns your career?

Control system migration is a major learning opportunity

It's a team effort

Want appropriately trained employees? Partner with your local community college

Mission-critical operations

Creating Twenty-First Century Learning Systems

See all Workforce Development Articles

Reader Feedback

We want to hear from you! Please send us your comments and questions about this topic to InTechmagazine@isa.org.