INDUSTRIAL INTERNET OF THINGS:

TWO SIDES OF THE SAME COIN

Gerard Ward, Cyber & Technology Loss Adjuster at Integra Technical Services, sets out the challenges presented for the insurance markets by the era of Industry 4.0, also known as the Industrial Internet of Things (IIoT). This is particularly relevant because, from January 2020, Lloyd's and many other insurers have stated there first-party property damage policies will confirm whether they provide coverage for cyber risks or not.

THE ERA OF IIOT

Traditionally cyber security for ***Information Technology*** (IT) and ***Operational Technology*** (OT) have been two distinct specialities. While both aim to maintain robust and resilient systems, their priorities are often different: IT computer programs operate predominantly on information, whereas OT controller programs operate on the basis of physics in support of mechanical motion.

Data security for IT systems is measured against the CIA triad (Figure 1), with confidentiality at the apex, followed by data integrity and availability. But this CIA triad is inverted for OT systems which underpin process industries and critical infrastructure, and where system failure risks human injury or loss of life. Consequently OT systems prioritise availability and integrity before confidentiality.

OT security has historically relied on air-gapped networks separated from the Internet to provide availability. Yet increasingly enterprises are implementing IIoT solutions that fuse IT and OT and using the Internet support automated control decisions that optimise asset performance and business value. However, the more system connection points, the greater the complexity; and the risk that the networked surface could suffer security and quality failings.

IIoT use cases are extensive: they range from Australian miners using autonomous trucks to haul extracted material from pits (and autonomous trains to transport it to ports); to firms such as Ocado and Amazon using IIoT robotics in warehouses to pick and pack goods. As 5G is rolled out the increase in data speed, bandwidth, and reduction in data latency will spur further IIoT uptake.

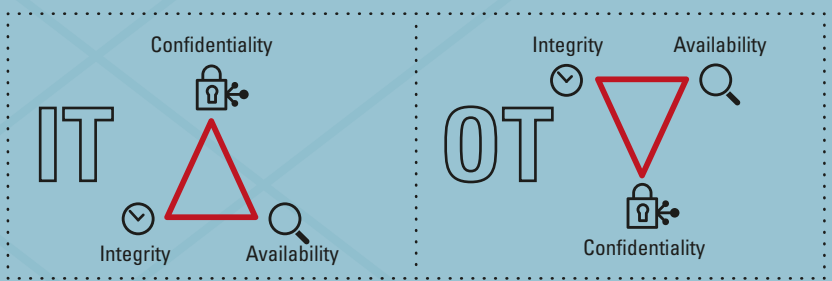

Figure 1: IT Security Triad supporting OT

In August 2019 Cisco released a report estimating the projected uptake of IIoT type technologies will by 2022 account for approximately 7 billion of the 14.6 billion IoT connected devices.

The influential US based National Institute of Standards and Technology (NIST) has developed a conceptual utility architecture which illustrates the role of IIoT systems in managing distributed energy resources (Figure 2). In this implementation IIoT optimises performance of the distribution grid via a connection between an industrial facility microgrid and a utility-managed distributed energy resource (DER) system.

SP Group forecasts a 12.4% compounded annual growth in demand for DER technologies, which are expected to reach US$169 billion in value by 2025.

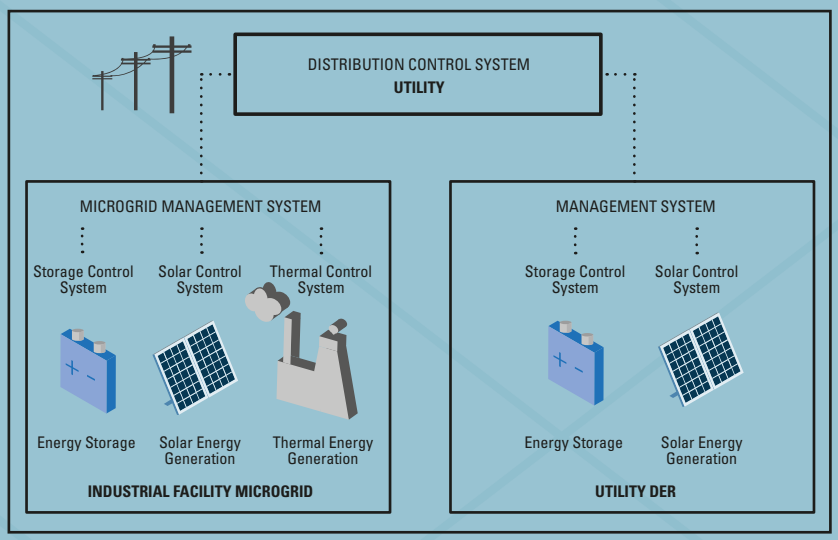

Figure 2: Example DER Infrastructure (source: NIST)

THE INSURANCE CONUNDRUM

As a way of limiting exposure to physical damage caused by data risk, some first-party property damage policies rely on exclusions such as CL380 and NMA2915. Other insurers confirm affirmative cyber through their property and casualty policy wordings. To remove ambiguity and ensure absolute clarity for insureds, from January 2020 Lloyd's first-party property damage policies will need to explicitly state whether or not data-related damage is included, a trend being adopted by many (if not all) other insurers.

This represents a significant change for insurers who are considering confirming cyber coverage. The sheer ambition and scale of the industrial use cases, and their expanded reliance on data – coinciding with the growing extent of IIoT implementation – increase risk.

Autonomous systems may encounter situational outliers that were never envisaged by the machine learning (ML) tools or artificial intelligence (AI) smarts. In these situations data failings resulting from a breach or error can be amplified. With OT components relying on AI, failings in AI-determined safety systems can have severe consequences.

While risk managers and underwriters have many frameworks and standards against which to measure organisational IT and OT risk, the standards available for IIoT are, at best, limited. The source for figure 2 above was released by NIST in August 2019 as a discussion paper. This paper calls for industry participants to develop scenarios which can inform reference design and support a best practice guide for improving IIoT data security in DERs.

The scenarios described are complex, with analysis and visualisation capabilities comprising security information and event management (SIEM), workflows, graph analytics, dashboards, predictive analytics, machine learning and other technology layers. And further demonstrating that IIoT standards need to catch up with implementations, the international standards organization ISO – authors of the IT security 27000 series widely favoured by business - currently have under development their IIoT security standard 30166.

In a modern manufacturing plant the controllers for steam, chilled water, electrical and fuel efficiency are managed by OT systems. But the energy management system determining the optimal operating strategy will be a networked and interconnected IIoT implementation. The challenge for insurance risk pricing is that while the core OT and IT components are mature technologies, the integration and interconnection elements are not.

When IIoT incidents occur, the right claims management solution can rapidly and accurately pinpoint root cause to either IT or OT components within the IIoT implementation. But it needs the support of specialist skills and a clear organisational structure. Integra Technical Services has assembled experts who can collectively investigate the relevant people, procedures, operations, information systems and environment, to accurately determine cause and consider a policy response. Identifying the prospects for recovery and betterment forms a key part of this root cause analysis.