RESILIENCE IN WATER AND WASTEWATER TELEMETRY AND CONTROL SYSTEMS

Lester Abbey, Managing Director, Abbey Systems Ltd

The author has 40 years experience in this field.

ABSTRACT

Resilience is a key requirement of any mission-critical process such as Water Supply and Sewage Disposal. Resilience means that the functionality of the system can remain largely intact irrespective of plant failure, natural events, planned outages, overloads, human error and other common causes of system failure.

This paper will examine the elements of control and telemetry systems and the consequences of failure of various components of these systems. There will be a focus on isolating failures so that the rest of the system functions correctly, and maintaining a level of functionality system-wide in cases of major breakdowns.

This paper will present a number of real-world situations such as earthquakes, power failures, plant breakdown and human error where a resilient system mitigated the potential damage to the process over which it had control. It will also present a number of illustrative instances where the lack of resilience compounded the difficulties of the initial problem.

In Control and Telemetry Systems, resilience is particularly required in communications, power supply and control philosophies. The paper will present a number of practical examples of how this can be achieved, with an emphasis on simple and robust solutions. There are also examples where over-engineering, such as multiple backups, can actually reduce resilience.

KEYWORDS

Resilience, Control systems, Telemetry systems, Communications systems, Plant Control, Disaster management

1 INTRODUCTION

1.1 RESILIENCE

Resilience as defined in the Oxford Dictionary is "the ability of a substance or object to spring back into shape; elasticity; the capacity to recover quickly from difficulties; toughness. Or, to put it simply – snap back into shape.

Its meaning in this paper is that the systems will keep going even when the wheels start to fall off. By "keep going", I mean that the Control and Telemetry will continue to be useful for its primary purpose of controlling and monitoring the supply of Water and the removal and treatment of Wastewater.

This paper is generally based on the field experience of Abbey Systems and other parties involved in these types of system. The emphasis is on practical examples of situations which normally occur during operation, and extraordinary events such as earthquakes, tsunamis and widespread power outages.

This paper stresses that Control and Telemetry systems are tools for Councils and Water Authorities to do their jobs in the Water industry and not an end in themselves. Hence all focus on resilience is to ensure that the Telemetry and Control systems support their function as tools, when under pressure.

1.2 TWO SITUATIONS REQUIRING RESILIENCE

Day to day operation, where temporary problems arise; human error, localized outages of power, communications etc are the norm.

Civil emergencies such as earthquakes, tsunamis, widespread power outages.

The two situations have differing requirements, the importance of which may vary from council to council.

1.3 SCOPE OF PAPER

Telemetry and Control Systems offer a wide scope for discussion of resilience. As such there are many possibilities and techniques. As such there are no clear answers to the many questions posed in this paper – rather information is presented so that councils and water authorities can make decisions based on their needs, imperatives and budgets.

2 WHAT IS THE CORE FUNCTION?

In order to determine where resilience is required to ensure that the tool of telemetry and control still functions under duress we need to identify the core functions of these types of system. They fall into four categories:

2.1 ALARMS

Most systems started off primarily as alarm systems and that capability is still the most used of the core functions. These systems monitor a wide number of functions over a large area and if something has gone wrong the system has the capability to inform someone who can act to remedy the situation.

2.2 CONTROL

These types of system are capable of co-ordinating the control of plant over a wide area: typically linking pump stations with reservoirs, but also controlling a line of sewage pump stations to maximize well storage or balance flow into a treatment plant. The RTUs may also act as independent controllers for pump stations or other plant.

2.3 SYSTEM OVERSIGHT

Another initial function of these systems is to provide oversight of plant scattered over a large geographical area. While less important than Control and Alarming, this provides a useful tool for managing the system in real time.

2.4 REPORTS

Reports are becoming a more significant output from these systems. Regulatory authorities are requiring accurate and complete data on things like turbidity, flow, water usage and alarm response. It is also used for targeting maintenance and determining patterns for future growth prospects. The key resilience issue with reporting is that even if the reporting system is unable to be used the data must still be collected and accurate.

3 WHAT TYPICALLY GOES WRONG

3.1 DAY TO DAY

3.1.1 COMMS FAILS

This is the most common problem and can manifest in several ways irrespective of the communications methodology.

* *Intermittent failure for one or two points*, often due to marginal coverage or weather conditions.

* *Intermittent failure system-wide,* generally due to Base station comms equipment or repeater sites problems.

* *Short complete breaks* - network or service issues.

* *Prolonged outages* – major network problems or repeater outage.

3.1.2 POWER FAILURE

Power outages can occur for short periods of time at any time of the year. The average outage is for 63 minutes with a frequency of 1.86 times a year. These are generally localized, affecting only a portion of the sites involved in a telemetry and control system.

3.1.3 COMPUTER FAILURE

This happens more often than it needs to, for any number of reasons, and must be taken into account because there can be serious consequences should the failure occur at an inopportune time.

3.1.4 INSTRUMENTATION FAILURE

Instrumentation does regularly fail as well and can very much affect the operation of telemetry and control systems.

3.2 MAJOR EMERGENCY

Major emergencies are events such as earthquake, tsunami, hurricane, volcanic eruption, warfare, or other conditions that affect major parts of the network and plant that it is controlling and monitoring. This is the sort of thing one can expect during a major emergency:

3.2.1 POWER DOWN

There will be widespread power outages and these outages may last for days, even weeks. Most Water and Wastewater networks rely on power being available in order to perform their core purpose – yet a functioning Telemetry and control system allows backup strategies that wouldn't be possible without Telemetry.

3.2.2 CELLULAR NETWORKS DOWN

These networks can recover more quickly than power; in fact their initial failure is often due to a lack of power after the batteries go flat. Gensets and reserve batteries can often resume service once the cell tower site is attended to. Still, outages can occur for several days with intermittent service for a long time after.

3.1.3 INTERNET DOWN

The local internet connections and ISPs will be affected by both power outages and communications losses. The internet is often used for remote system overview and alarms. Some systems use the internet for connection to RTUs via Wifi. This facility can be lost for a number of days.

4 SITUATIONS WHERE RESILIENCE WAS OF IMPORTANCE

4.1 CHRISTCHURCH EARTHQUAKE; WHAT WORKED AND WHAT DIDN'T

4.1.1 COMMENTS FROM LES COLLINS, ENGINEER CHCC

When the earthquake first occurred, none of our systems let us down . All telemetry carried on normally although it became busier for a while. There was, though a concern that telemetry info may be unreliable or lacking, and a large team was mobilised to validate telemetry reports and also assess damage.

Our greatest exposure was a weakness in the battery backup at sites and repeaters. Irrespective of whose gear, all sites were effected by mains failures for differing periods and eventually went mute until either power or a new battery set arrived. This made the SCADA Base quieter due to lack of traffic

Yokogawa sites may have stalled a little early as they are more power hungry that simpler RTUs, but it made little difference.

Repeater sites were similarly affected.

We turned off our paging system to control the number of alarms entering the SMS system and also because not all cell towers were operating. As sites were checked, we cautiously restored alarms, but most sites were actually checked regularly by humans to make sure SCADA was representing actual, and reliable information.

Councils servers and UPSs went down very quickly so there was no remote access to see the SCADA Base. However, the shift controllers "double team shifted" for a few days so there were at least two men in shift control for 24 hours a day. One dealt with SCADA issues, the other dealt with the flood of phone calls .

The city wastewater treatment plant became an operations base and dispatch point for marshalled contractors and technicians. Information sent to the field was a combination of validated and trusted telemetry, site confirmations (PTT radios), cellular and line information as it came to hand.

The reticulation network was severely damaged all over and some controlling assets were shut down so as not to make the situation worse.

4.1.2 SUMMARY OF KEY FACTORS

Power - The power was off for up to 4 days, longer in isolated areas. This was longer than the battery storage in many key sites such as repeaters and cell towers. The increased SCADA traffic and cellular traffic after the quake exacerbated the power drain on these sites.

Radio Communications - All repeater sites were owned and maintained by the council. There were two separate networks – an older voice radio network used by the Datran RTUs and a new high speed data radio network for the new Yokogawa DCS RTUs. Both sites were similarly engineered as to access, battery storage and physical characteristics such as repeater hut, mast etc. Repeater sites held up for 2 to 3 days without needing attention. The data radio sites tended to go down sooner because of a heavier demand for power during this emergency. Radio communications could be restored by fresh batteries, restoration of mains power or gensets.

Cellular network - The cellular network functioned fairly well just after the earthquake but the batteries in the cell towers went flat before the mains could be restored. The network was also overloaded because of all the emergency telephone traffic and the presence of missing links and chokepoints.

Internet Communications - The internet was used for remote overview and alarming.

4.2 SURVIVING A TSUNAMI – CRESCENT CITY, CALIFORNIA

Crescent City was inundated by a tsunami that wiped out most of the city and its infrastructure including treatment plants and all of its pumping stations. Among the few things to survive were two repeater sites and a large reservoir on the hill behind. The repeater sites proved to be vital to civil defence and voice communications as well as keeping the makeshift control center informed of reservoir depth.

Had the repeater stations not been equipped with adequate battery backup the situation would have been much worse.

4.3 COMMS OUTAGE CAUSES DATA LOSS – SALT LAKE CITY, UTAH

Granger-Hunter Water District in Utah invested heavily in a high speed data radio network so that they could recover and store data at a higher rate than their older, slower voice radio network. When the network was working properly the performance met requirements. When there was communications loss however, there were large gaps in the data recorded at the base station.

Initially this was rectified by placing dataloggers at the affected outstations. As more and more outstations would experience communications failures, more dataloggers were installed. Eventually the expense of dataloggers, site visits to retrieve data and time needed to integrate the datalogger information with the SCADA information became too much. Granger-Hunter moved away from PLC-based RTUs and adopted RTUs that could store data during comms outages. Where the control processes were complex PLCs were retained but the RTU was responsible for data retrieval and communication.

4.4 COMMUNICATIONS FAILURE CAUSES PUMP TO BURN OUT

In a pump station, the wrong setpoints were used and an expensive pump needlessly burnt out. Designed-in resilience could have avoided this.

A very remote site was controlled by an RTU for sewage pumping from a large pond. The communications was precarious but generally workable. The Pump station operated to setpoints determined during commissioning. After some time new setpoints were entered at the master unit and downloaded to the RTU. There was a comms outage of some hours (repeater maintenance) and coincidentally the RTU was reset. The RTU attempted to retrieve its setpoints from the Master, found out that it couldn't communicate and reverted to the default ones determined during commissioning. Much had changed since then, including new instrumentation and level sensing, and these old setpoints caused the pump to run continually, even when dry. When communication to the Master resumed the RTU did not attempt to update its setpoints and kept the pump running. Eventually the pump had a thermal overload alarm – which was transmitted successfully to the Master - and after another hour burned out completely.

So even though some resilience was built in (restoration of setpoints after restart) it could have been done better. An operator should have been alerted to the fact that the master and the RTU had different setpoints – the system didn't cater for this. Automatic update of setpoints would have helped. The operator probably should have responded to the thermal overload alarm, but it was a two hour drive to get to site. Most importantly – for some reason the thermal overload contact was not set to automatically turn the pump off when active.

4.5 SEWAGE STORAGE DURING A WIDESPREAD POWER FAILURE

An interesting example of system resilience is a fallback plan in the event of a widespread power outage. Many would argue 'what is the point of SCADA and control when the plant is inoperative because of lack of power?'. Battery backup at the RTUs enable them to keep functioning and if the connected instrumentation is wired correctly it still works as well. If a power outage occurs the residual volume in wetwells can be used to store wastewater until the power is restored. The Scada and telemetry, which can operate in the absence of mains

power, can determine the wells most likely to overflow in the near future, allowing council teams to get generator sets onsite to empty the wells. A strategy can thus be formed to selectively pump to wells that have more unused capacity.

5 RESILIENCE FACTORS IN SYSTEM DESIGN AND USAGE

5.1 DISCUSSION OF OWNERSHIP OF ALL PARTS OF THE SYSTEM

In a complex system that involves SCADA, telemetry and control, significant parts of the system can be under the control or ownership of other parties. This means the options for designing in resilience are reliant on the other parties' strategies, which may be at odds with the council's or water authority's requirements.

The parts of a system that are affected by outside ownership are typically Power Supply, Communications, Computing and Alarming.

5.1.1 COMMUNICATIONS NETWORK

As Telemetry and control systems were adopted by councils over their older manual systems the communications used to be either Post Office or Council-owned radio networks. There was some debate as to whether the council should be involved in the ownership and operation of a radio network, the imperative was for council control over all aspects of its system.

As technology improved higher data rates were required and more expertise was needed to maintain more complex networks. There has been a migration to third party providers, in particular cellular, trunked radio, wifi/internet, satellite. Because these networks are professionally set up and have diversity of paths and equipment they are often more reliable than a council-owned radio network.

Cellular Networks - These provide a reasonable data rate, very little capital expenditure, have fairly good coverage and for day to day operation prove more resilient than a standard council-operated radio network. There is a running cost which can exceed the cost of running a council-owned network. During civil emergencies the availability can become very poor to nonexistent.

Wifi / Internet - This provides high data rates and little capital expenditure with fairly reasonable running costs. There are problems with coverage and reliability of the 'last mile' (e.g.WiFi link) of communications. The internet is inherently resilient but even the most resilient system can be crushed by overload.

Satellite - Satellites provide excellent coverage and reasonable data rates. Best of all they are unaffected by earthquakes, tsunamis, forest fires, riots, power outages or other civil emergencies. The connection is expensive as are the running costs.

5.1.2 MAINS POWER

There was a day when the local council owned the MED. Now we have a free market. Council has gensets, power authorities have CAIDI targets. In normal operation outages of 1 to 2 hours can be expected every year with longer outages in storm conditions. There is more of a problem in major emergencies when sufficient battery backup (12 hours at RTU sites, 48 hours at repeater sites) and portable gensets that can be taken to problem areas in emergencies are needed.

5.1.3 COMPUTING - INTERNET

Most councils own their own SCADA computer, sometimes the IT department arranges for it and takes responsibility. Parts of the computing can now be outsourced – entire alarm systems can be hosted, the alarm delivery most often requires an external agent e.g. Vodafone, Spark, internet.

5.1.4 LEASED SYSTEM

This is not yet prevalent in New Zealand but is becoming more popular in the United States. A telemetry provider owns and operates the Telemetry and control system and delivers alarms, reports, system overview and sometimes control loops. This type of system is chosen by smaller authorities who lack the support staff and don't want to engage in any capital expenditure. They don't work well in times of civil emergency.

5.2 RESILIENCE FACTORS FOR DELIVERING SYSTEM OUTCOMES

Day to day - In everyday operation there will be problems which will affect system operation. There are considerations in system design and implementation which can ensure operation even if there are minor failures of parts of the system The types sorts of problems that typically occur are:

- Intermittent communications failures,
- Hard communications failures
- Short duration power failure
- Instrumentation failure or drift
- Computer failures

All these are expected and can be dealt with. The expectation is that if the fault is 'hard' it will be repaired within 24 hours and if it is intermittent it can be survived with little or no loss of function.

What we are trying to achieve - This paper discusses resilience in Control and telemetry Systems but it must be remembered that these systems are ***tools*** to assist the core functions of the delivery of water and removal and treatment of wastewater. The resilience discussed here is effectively the resilience needed to keep the system functioning so that the core function is supported, not the correct operation of the telemetry system as a whole.

5.2.1 ALARMS

There must be multiple paths for annunciation, including a robust backup. Systems that rely on the internet or cellular network can be affected by disruption of service. Similarly the unavailability of the Master Station due to power outages, comms failures or system crashes will disable most alarm systems. Some councils keep the pre-telemetry alarms going – a flashing light atop a pump station and a message as to who to call if flashing. Another approach is to normally use the cellular network or internet but have an audible alarm in the control room or an autodialler that uses the PSTN network.

5.2.2 CONTROL

Control methodologies can be affected by communications outages, power outages and master computer failure. Localising the control algorithms is a good start, retention of manual systems is also worth doing. Also simple backup control systems such as a float switch at high level alarm could also turn all pumps on for a set period of time. If the control methodology involves multiple sites such as pump station/reservoir pairs, a good backup strategy would be direct communication between the sites if a repeater or master station fails.

5.2.3 SYSTEM OVERSIGHT

Diversity of location and/or equipment for display of system e.g. webserver/ tablet, is a technique to ensure that an overview is available under most circumstances. Most web-based systems will also have an attached PC at the communications hub for backup purposes.

5.2.4 REPORTING

Reporting function is the only one that doesn't need to be available at all times – reports can wait. However, the data that goes into the reports must be collected and there should be no gaps and inaccuracies. To ensure this there should be a facility at the collection point – typically an RTU to store and time-tag the data. This constitutes a method of collecting and storing data that doesn't depend on mains power, computer availability or communications integrity.

5.3 KEY FACTORS IN ACHIEVING RESILIENCE

5.3.1 FOCUS ON THE JOB THAT SCADA IS MEANT TO DO

It is a tool to facilitate delivery of water and removal of wastewater. *It is not an end in itself.* Focus should be on ensuring its usefulness as a tool for this function rather than keeping the entire system intact at all costs. Fancy 'extras' such as surveillance cameras and touch panels should not receive the same attention as components providing the core outputs.

5.3.2 POWER

Power is a fundamental requirement for all aspects of the system. Backup measures such as batteries and gensets should be apportioned according to need and expected outages.

5.3.3 DIVERSITY

Putting all one's eggs in one basket for a SCADA Master gives a single point of failure. Many councils are investing in Disaster Masters at different locations with full Master station capability including communications to RTUs.

Diversity of communication channels is also being used but often the complexity and expense mitigate against this.

5.3.4 SIMPLICITY

A complex system is much more difficult to make resilient than a simple one. There is pressure for more complexity given reporting requirements, council amalgamation, new technologies becoming available and rapacious vendors seducing engineers with ever more features and gadgets. Simplicity can be very hard to achieve. As famously said by Albert Einstein "Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius - and a lot of courage - to move in the opposite direction."

An approach that we are trialling is to build complex systems out of simple, self-sustaining subsystems.

5.4 SPECIFIC SOLUTIONS

To ensure resilience over these day to day occurrences here are some techniques in use:

5.4.1 COMMUNICATIONS PROBLEMS

Techniques for overcoming communication problems fall into two camps – operate as well as possible until comms resumes or attempt to keep comms availability as high as possible.

Data storage at remote sites ensure that no data is lost during a comms outage.

Local control strategies that kick in when comms in unavailable.

Techniques for keeping comms going under pressure:

Dual path communications – This is expensive and can make things worse. Both paths must be exercised frequently to ensure that problems haven't developed. Similarly the changeover mechanism must be exercised.

Self-healing mesh network – A network that has multiple paths and automatic re-routing if a path is blocked or unavailable. This is the panacea being offered to ensure 100% connectivity. It works well for a small number of nodes but can grind to a halt as the number of nodes increase.

5.4.2 POWER FAILURE

Battery backup at the RTU is essential. It should back up attached instrumentation as well. Loop power transducers are an example of how this can be accomplished.

Strategy for operation – A strategy for continuing operations should be devised should the power fail. Gravity is useful in water supply and doesn't require power -, Battery backed up telemetry identifies full reservoirs and *ones that will be empty shortly.*

Gen Sets for critical problems – If an outage will continue longer than what battery or storage facilities can cater for portable generator sets can be transported and attached to critical sites.

Uninterrupted Power Supply (UPS) at Master. The Master Unit should be able to function for 24 hours without mains power – perhaps more at a Disaster master site. It should be tested and a watchful eye should be kept on what is connected to the UPS as it can grow to a point where the UPS is no longer able to support the load. Batteries must be kept renewed, as they deteriorate with age.

5.4.3 INSTRUMENTATION FAILURE

The best way to surmount this is to start with good quality instrumentation. To detect problems the telemetry system can detect whether the instruments are providing sensible information within expected bandwidths, and alarm when these are exceeded.

The calibration of many instruments can drift – this needs to be checked on and regular re-calibration could be required.

Sometimes a backup check is useful; often we use a float switch set at a certain known well depth and check what the level sensor reads when this float switch is activated.

5.4.4 COMPUTER FAILURE

A backup computer that takes over as soon as the Master does not seem to be in action. Typically a third simple device should choose who is in charge as there have been cases where a Backup fails in such a way that it seizes control from a working Master.

The backup should be synchronized with the Master as regards alarms, processes and stored data, and when the Master is restored it should get an update from the backup of all that went on during its down time.

Master Station design should ensure that setpoints, metering pulses, data collected by RTUs and alarms are not lost after restart.

RTUs should know when to go into local mode when they are no longer in contact with the Master.

5.5 EXAMPLE CONSIDERATIONS

What follows are some examples of resilience techniques applied to components of telemetry and control systems.

5.5.1 SWAMPFOX

In designing the Swampfox, resilience was a key factor. Here are some design decisions that were made to further the resilience of this product and its usage as a tool for water and wastewater authorities. The primary focus was simplicity i.e. all in one box – it either works or not and the entire box can be replaced easily if it isn't working.

For Communications resilience we chose radios designed to work in marginal areas giving good coverage and protocols that ensured that there was no lost or duplicated messages. In addition, the protocol supports the ability to transmit datalog files to the Master and for the Master to transmit configuration files to the RTU.

Battery monitoring; most RTU's have battery backup, but more often than not the battery is not maintained or replaced when old. The first indication of trouble comes when there is a mains fail and the battery holds up 20 minutes rather than the planned 12 hours. The Swampfox monitors battery health and warns when the battery needs replacing; sometimes the battery is actually replaced after the warning.

5.5.2 SELF HEALING NETWORK

The concepts behind an IP-based self-healing network are compelling and attractive. The general idea is that the network consists of a number of nodes that can communicate with each other. Should one node or path fail the network will find another path to relay any message traffic. This is a proven and readily available technology.

There are some serious issues with these types of networks that need to be considered when using them for a widescale telemetry network. Firstly, the speed of links between nodes can be as low as 4800 bits per second; a typical IP network can accept data at a rate of 10 million bits per second. So a situation exists where data can go in at 10 Mbits/sec, come out at 10 Mbits/sec and in the middle can slow down to .0048 Mbits/sec. As the number of entry points to this system increases, the possibility of chokepoints increases. Also, by increasing the number of nodes one increases the number of possible paths back to the master; this seems like a good idea in the first instance but the reality shows that the bandwidth decreases by a factor of $1/(2^{n-1})$ with n being the number of hops available to the ratio network.

When too many nodes are added and too much traffic is introduced the network can grind to a halt very quickly and be difficult to unsnarl.

This concept works very well for a high speed network with a limited number of nodes; in Wellington it is used over the Telemetry IP Backbone which links all 21 repeater sites with high-speed high-reliability microwave radios. There is one alternative path in this ring network. The network will work reliably if any node is lost and has a diversity of links from the Master to the backbone.

5.5.3 DUPLICATION OF EQUIPMENT/ FAILOVER

Duplication of key equipment and failover techniques are common techniques used in achieving a resilient system. There are pitfalls however, as discovered in the Christchurch earthquake.

There is a failover server and Yokogawa router that needs to be turned on (and the other turned off) - somebody turned it on and it locked because both were then running. Note though that the Yokogawa router can slow traffic and become a nuisance at that time.

There is scope for the wrong equipment to take over or require some action to make it work which is forgotten in the haste of an emergency.

5.5.4 RETENTION OF MANUAL SYSTEMS

Telemetry and Control Systems weren’t always available for Water and Wastewater. They were introduced to save time, trouble and travel. When for whatever reason the system breaks down there should be a facility for driving up and turning the valve on, shutting the pump down, resorting to float switch operation or whatever used to work in the old days.

6 CONCLUSIONS

Telemetry and Control systems are complex systems with a need for resilience in a number of key components. They are also tools for the core functions of the delivery of water and removal of wastewater to the constituent community. Resilience should be focused on that requirement.

There are two situations where resilience is examined – day to day operation and times of civil emergency.

6.1 CORE FUNCTION

The core function of these types of systems is to assist the council in its water and wastewater functions. To this end there are four primary functions:

- Alarms
- Control
- System Oversight
- Reporting

To achieve these functions., techniques, equipment and systems can be put into place to ensure that functionality is retained during comms outages, power failure, computer failure and other mishaps likely to occur.

6.2 TYPICAL PROBLEMS

Problems encountered in Telemetry and Control systems of this nature are largely centered around power failure and communication failure. Computer and instrumentation failure play a lesser but still important part.

The problems manifest differently in a major civil emergency as opposed to day to day operation. For example a communications system that performs well under the common problems of day to day operation may well perform less effectively than other systems during times of civil emergency.

6.3 SITUATIONS WHERE RESILIENCE IS OF CRITICAL IMPORTANCE

The use of Telemetry and Control during major emergencies such as earthquakes and tsunamis was beneficial in maintaining rudimentary service even though there was widescale damage to plant. Resilience can also limit damage and maloperation of connected plant during comms outages and power outages that occur in localised areas during day to day operation.

6.4 RESILIENCE FACTORS

Ownership of system allows the operator to determine the level and type of resilience; however, this might not be practical for financial or operational reasons. Most of the key factors centre around keeping the communications going or coping with its loss and the loss of mains power.

Simplicity is emphasised and the duplication of equipment and communications also provides some resilience; however, that approach can conflict with the goal of simplicity. There are no easy answers – the factors outlined must be taken into account along with operational requirements, budgetary constraints and individual council needs.

REFERENCES

Interview with Steve Champ, CEO QTech Data Systems

Interview with Leslie Collins, WW Asset Manager Christchurch CC

Interview with Ken Mitchell, Network Engineer Scanpower

Interview with Eric Wier, Crescent City, California

Paper presented at the Water NZ Annual Conference 2015 “Integrating the regions control systems – the story so far” - James Murphy, Telemetry Engineer

The Myth of Mesh - John Yaldwin Chief Design Engineer 4RF

“Capacity of Ad Hoc Wireless Networks” J. Li Blake, D.S.J.D Couto, H.I. Lee and R Morris