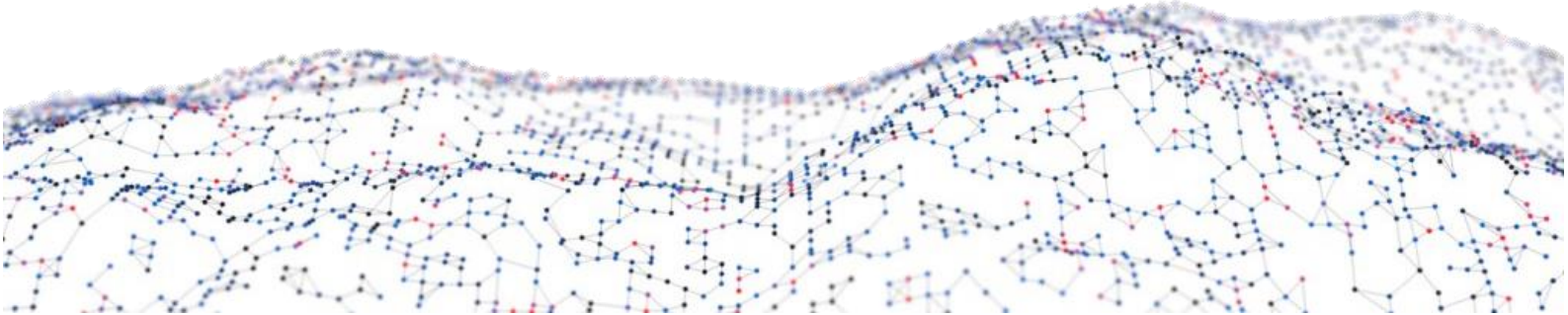
Torque IP

INDEPENDENT TECHNOLOGY ADVISORS

Duress alarm systems in healthcare environments

Whitepaper

6 January 2025



CONTENTS

Works Cited

Alliance, A. H. (2018, 09 18). *AHFG - Part C - Design for Access, Mobility, Safety and Security*. Retrieved from AusHFG: https://aushfg-prod-com-au.s3.amazonaws.com/Part%20C%2018%20Sept_4_Nov%202021%20Reference%20Edit.pdf

AusHFG. (n.d.). *standard-components*. Retrieved from Health Facility Guidelines: https://healthfacilityguidelines.com.au/

Health New Zealand - Hauora Aotearoa. (2022). *Procurement considerations for Mobile Duress Alarm Systems.* Health New Zealand.

Health, N. M. (2022, March 10). *Protecting People and Property*. Retrieved from NSW Health: https://www.health.nsw.gov.au/policies/manuals/Pages/protecting-people-property.aspx

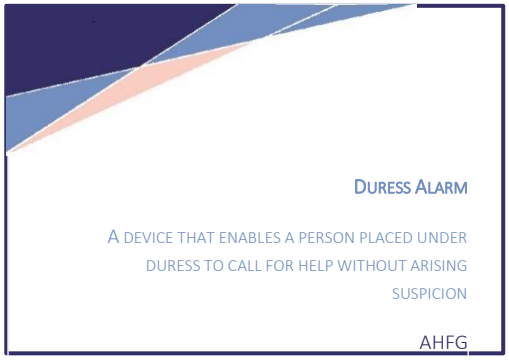
Longmore, M. (2023, June 19). *Mental health nursing "beyond crisis"*. Retrieved from Kaitiaki Nursing New Zealand: https://kaitiaki.org.nz/article/mental-health-nursing-beyond-crisis/

Saxena, N. (2019, 10 09). *St-08 Security ICT standard*. Retrieved from healthhub.act.gov.au/technology: https://www.act.gov.au/__data/assets/pdf_file/0007/2412547/St-08-Security-ICT-Standard-2019.2.0.pdf

Executive Summary

Every business or undertaking has a responsibility under the Health and Safety at Work Act 2015 (HSWA) to ensure, as far as reasonably practicable, the health and safety of staff and any others who could be put at risk in the conduct of its business operation.

While all businesses have their own challenges and risk profiles, there are specific challenges in the provision of healthcare services where staff are subject to threats and assaults from service users, family members, or associates.



Although Health NZ has not publicly released statistics on violence there are many reports in the media citing an increase in assaults and violence within healthcare facilities (Longmore, 2023).

Many steps have been taken to address these threats with hospitals implementing a range of service-specific initiatives, particularly in areas of greatest need such as Emergency Departments, Acute Inpatient Mental Health Units, Adult Inpatient areas, and Outpatient Mental Health facilities. These steps include greater use of integrated technology systems such as CCTV, Electronic Access Control, and importantly recognising risk by including both fixed and mobile duress alarm systems.

This whitepaper reviews the requirements for system specification, performance, design, integration, installation, deployment, and maintenance of duress alarm systems within healthcare facilities and makes suggestions on the need for recognising the differing requirements of staff in various facilities and locations.

Terms and abbreviations

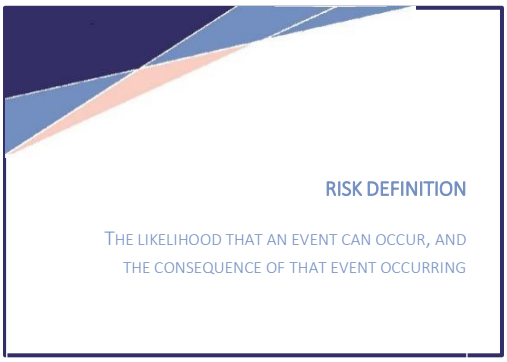
The following term and abbreviations are used in this whitepaper.

Terms and abbreviations	
AHFG	Australasian Health Facility Guidelines
BLE	Bluetooth Low Energy, reduced power version of Bluetooth
CCTV	Closed Circuit Television
EACS	Electronic Access Control System
GHz	Gigahertz, unit of frequency
Headend	A central master facility for processing and distribution of data
ISM	Part of the RF spectrum reserved for Industrial/Scientific/Medical purposes
LAN	Local Area Network
LQI	Link Quality Indicator
Mesh	Communication network comprised of radio nodes in an interconnected configuration.
MHz	Megahertz, unit of frequency
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTLS	Real-Time Location Services

Terms and abbreviations	
SNR	Signal to Noise Ratio
Triangulation	Method of determining location by forming triangles to a point from known point locations
WAP	Wireless Access Point
Wi-Fi	Wireless Fidelity, the wireless LAN network
UPS	Uninterruptible Power Supply
Zigbee	IEEE 802.15 WLAN specification, low power wireless mesh network

Requirements of a Duress system

Assessment of risk



Healthcare facilities recognise that risks exist and the nature and triggers of them are many and varied. The risk profile varies between facilities, wards, departments, locations, and the design and structure of these places and their operational policies. The assessment of risk and the requirement for duress alarms can only be determined through consultation with all stakeholders including clinical and security staff, operational management personnel, and with the teams that support the installed solution including the Facilities team, and the Data and Digital team. (Health, 2022).

In a healthcare setting, it is essential that the duress alarm activation is part of a planned and coordinated operational clinical and security response management plan and be alerted to multiple responders and locations. In the same way that the staff member under duress is mobile, the responders are also mobile and not located in a central monitoring location. The reference standards require responders to be advised of the location of the event within a minimum of five seconds.

Current Health New Zealand design expectations include wide use of duress systems based on the need identified in the facility or unit-specific risk assessment. Although a standard expectation for acute mental health facilities, both fixed and mobile duress systems are increasingly being installed in other areas of a hospital or facility to provide staff and visitors with an increased sense of safety and security and to meet the needs of the facility health and safety requirements.

To be effective, the duress system must be considered as an integral part of the facility safety and security system and be easily integrated into other security and patient care systems in the facility. The ability to transfer information between disparate systems including the Electronic Access Control, the CCTV, and Nurse Call systems is often essential and critical and must be fully reviewed during the risk assessment.

System performance

Duress alarms are considered a life-safety system and the primary requirement for a properly performing duress system is that it is always available. While some downtime may be inevitable, the impact of component or system downtime must be considered in product selection and design and mitigation strategies including component and system, redundancy, backup systems, and fault tolerant design whereby some components can be offline without substantially degrading performance.

- Fault tolerant design examples include the design of systems using Mesh or multi-path transmission systems.
- The building materials and structure of healthcare facilities may provide challenges to effective RF transmission Similarly, when required to operate outside of a building, systems based on Wi-Fi may perform poorly particularly in adverse weather conditions. Transmission frequencies in the 900MHz ISM band will provide better performance in some areas than those dependent on Wi-Fi, particularly those requiring longer range transmission, external and open spaces, or areas where the building construction materials and facility equipment including concrete, steel, and glass may attenuate the Wi-Fi 2.4Ghz and 5Ghz frequencies to a greater degree.

Most duress system vendors will provide Mean-Time-Between-Failure figures for their devices however these can be misleading as they do not consider the impact of system failures in supporting infrastructure such as facility power supply, and server or supporting systems failure. The service availability analysis must consider other supporting systems and provide mitigation if they fail:

- When using the facility Wi-Fi for RTLS positioning and for communication, the Wi-Fi and LAN network must be designed to sustain the same level of availability as the duress system.
    - Wi-Fi predictive mapping and post installation performance mapping surveys are essential if using the Wi-Fi service. The Wi-Fi mapping must consider WAP failures and provide sufficient cell overlap to ensure that positioning is not compromised. The supplementary use of BLE beacons and further help positioning discrimination.
- RF systems that do not use the facility Wi-Fi may also support specific area or whole-of-site duress system installations. The same requirements for duress positional accuracy apply however the methodology for achieving that may vary.
    - Mesh network systems, often using Zigbee wireless communication provide locational accuracy by measurement of the nearest repeater or mesh transmitter device. Mesh technologies are typically self-monitoring with the repeaters being either powered or battery powered. Should a mesh repeater fail, the communication path from event location to headend dynamically resets and positional sensing and alerting is not compromised. Zigbee does not require the facility Wi-Fi to operate.
    - RF triangulation may be used to locate positions. Typically, the duress activation must be received by three RF receivers to provide accurate locations. These types of systems often operate in the 900MHz ISM bands and have no reliance on the facility Wi-Fi.

Service availability

Duress systems must function reliably and continuously. Although component failures will happen, the integrity of the overall system must be maintained to the highest extent possible.

- Duress systems must be able to operate, although potentially with some degradation of service during component failure events. Wi-Fi networks must have sufficient overlap to compensate for the loss of a WAP, Wi-Fi and Bluetooth beacons may be used to supplement the original Wi-Fi design. Mesh networks are generally self-healing and compensate for the loss of a mesh transceiver. On both cases, the monitoring system must report an error condition to allow rapid rectification of a failing device.

- Duress systems using the facility Wi-Fi network will not operate should the Wi-Fi network be unavailable. The Wi-Fi network must therefore be designed with the same resilience an uptime objective of the duress system. In many healthcare facilities, the LAN network is maintained by local Data and Digital personnel and may not be afforded the same level of response as other ICT system failures particularly out-of-hours. Areas using the Wi-Fi, and the supported backbone connections must be provided with high levels of response for 24x7 operation.
- The LAN devices including network switches and backbone communications to the servers must be supported with backup site power supply in the event of a site power failure. These networks may be supported by local UPS or configured to the facility Emergency Power network to ensure service continuity. As the WAPs are typically PoE enabled, maintaining the network switches with power will maintain the WAP operation however loss of network backbone may degrade duress service and, in some configurations, take it offline completely. Systems with some local capability to operate despite loss of network are recommended.
- Mesh based systems may be supplied by distributed power, often 12Vdc and are typically supported by localised Battery Backup providing reliability in the event of a power outage. Loss of server connection from the area headend should not significantly disrupt local operation however this must be addressed in the risk analysis and the detailed design.

Maintenance and service support

Maintenance support contracts should be commissioned to provide both proactive and reactive service to the duress system and its supporting devices.

- Most duress systems include self-monitoring and alerting of potential failures. It is recommended that remote monitoring by the service agent be provided to provide immediate alerts to the appropriate technical response teams, allowing remote access where possible to shorten response times and initial diagnosis of faults.
- These systems have both firmware and software components. All software should be supported by maintenance contracts with firmware and software updates undertaken when available. The facility ICT team and the supporting contractor must be able to review release notices for firmware and software updates to ensure critical updates are undertaken quickly, and lower priority updates can be scheduled appropriately utilising change control procedures
- All electronic systems have an end-of-life roadmap provided by their vendors. This generally informs the time when firmware/software updates will no longer be available, and a time after where maintenance support is no longer sustainable. Healthcare facilities should monitor the product roadmap to ensure that aging systems can be budgeted and scheduled for upgrade or replacement.
- The duress system must be supported with 24x7 support with trained and skilled support contractors providing response. This may be either the vendor themselves or nominated channel partners however it is essential that these companies maintain local support, spares parts, and where practical local repairs to reduce inventory holding and service times.

Location accuracy

Fixed duress does not present any issues for location awareness as the duress call point location is known. In contrast, mobile duress systems require a high degree of positional accuracy to allow responders to quickly respond to a duress activation at the right location.

None of the reference standards reviewed specifically state the positional discrimination needed, rather they refer to the risk assessment as the basis of determining location. The general recommendations are:

- A mobile duress system must be able to track and follow an event activation if the person who activated the call is moving. Typically, not more than a 5-second delay should occur in the notification of the revised area for response in confined and restricted wards and facilities.
    - "Right side of the wall" location accuracy is essential in high-acuity environments. Right side of the wall needs to address areas where blind spots exist when entering a nearby or connecting space, for example corridors, cupboards, bathrooms, and ensuites where positional accuracy of even a few metres may not be sufficient to quickly locate and reach a person under duress.
    - This is particularly important in areas where visibility is limited or concealment more likely. In acute inpatient mental health facilities this often includes the ability to identify the activation as being in a patient ensuite or bathroom where less accurate discrimination could leave responders searching many rooms and spaces causing delay in the response.
    - "Right side of the wall" discrimination must address the potential inter-floor issues where the alert activation may be identified as being directly on floor above or below the activation as this will cause critical delays in the responder locating the at-risk person.
- 5-10m discrimination is generally considered acceptable for open spaces such as lobbies, dining rooms, and external courtyards and spaces. In larger outdoor spaces with clear line of site, less discrimination is required. This should be determined during the risk analysis.

Duress alarm types and response

There are two generic forms of duress alarms, fixed duress and mobile duress. Both should work the same way with silent alarms sent to the responders and security monitors. Most facilities have fixed duress call points at key locations and the AHFG provides design guidance on minimum locations where these should be in the published Standard Components room layout sheets. (AusHFG, n.d.). The requirements for mobile duress are less definitively identified however NSW Health require all Emergency Department (ED) workers to wear a personal duress alarm when on duty. (Health, 2022). Although a contributor to the AHFG, this requirement is not recognised in the AHFG which has limited content on mobile duress but notes that it should be considered for all high-risk areas including Emergency Department, Ambulance Entry, mental health facilities and consult spaces as a minimum. (Alliance, 2018)

- Fixed duress - Typically fixed to the underside of a desk or counter and used to discretely summon assistance without causing local alarm or escalation. These are effective only in areas where there is no possibility of the aggressor to get between staff and the call point.
    - In most cases, the fixed duress call point will be a part of the security system network and not a duress system network. Communication between the security system and the mobile duress system is required should the call need to be relayed to clinical staff for joint response.
- Mobile duress - Wireless duress personal alarms are used by staff members who are mobile during their shift. These are generally worn clipped to a belt, in a pocket, or as a fob device either clipped to clothing or formed as a wristwatch like device.

- Mobile duress calls may be responded to by Security personnel, but in many cases notably Mental Health and within wards and emergency departments, the immediate responders may also be clinical staff as a function of already being present, and as clinical staff particularly in mental health facilities are trained in de-escalation and may also know the aggressor as a resident or visiting service user.

Mobile device technologies

There are a range of technologies and location defining techniques used in RTLS Mobile Duress. While they perform the same basic function of location identification, each has its advantages and disadvantages and positional accuracy. Selection of the technology used must be done based on the risk assessment and the clinical and security requirements. The most common technologies used are:

Wi-Fi

This technology utilises the facility Wi-Fi network to estimate the location of an activation with the activating device emitting Wi-Fi signals. Typically, Wi-Fi positioning offers accuracy within 10-20 metres which can present problems when precise location identification is required. Discrimination may be improved with greater Wireless Access Point density however this may negatively impact general Wi-Fi performance due to RF channel contention and network traffic. Increased WAP density may also require the automated power levels of the Wireless Access Points to be disabled adversely affecting Wi-Fi network performance when the network may also be supporting real time voice communication or heavy traffic loads. Increased Wireless Access Point density also increases the capital cost of the installation. Wi-Fi networks must have sufficient coverage overlap to compensate for the loss of a Wireless Access Point on network.

Bluetooth Low Energy (BLE)

BLE operates over Wi-Fi networks capable of receiving Bluetooth signalling, or as dedicated networks of Bluetooth sensors placed throughout the monitored area. BLE beacons are small, battery powered devices that emit signals at regular intervals. When a duress activation is triggered, the BLE badge or device sends a signal to the nearest BLE beacon which then relays the location information to the headend system. BLE systems can generally deliver positional accuracy typically within the range of 3-5 metres using Received Signal Strength Indication (RSSI). BLE systems using RSSI should be tuneable to improve positional discrimination.

Mesh networks

Although a wireless network operating in the 2.4GHz ISM band, the Zigbee network is a standalone network with its own protocol that does not communicate or interoperate with a standard Wi-Fi network. It is a low power system typically used for low data rate applications that require long battery life and secure networking. Its defined data rate of up to 250kbits/s is best suited for intermittent data transmissions from a sensor or input device. Zigbee mesh networks primarily use the Received Signal Strength Indicator (RSSI) to assess the quality of communication between devices providing 3-5 metre discrimination. RSSI measures the power level of the received signal, which helps determine the strength and reliability of the wireless links. Location discrimination can be improved in high-risk areas with the inclusion of more Zigbee transceivers. This metric is essential for efficient routing, reliable data transmission, and network stability in a mesh topology. In addition to RSSI, Zigbee networks also use the Link Quality Indicator (LQI), which provides a more comprehensive assessment of the communication link's quality. LQI considers factors like signal-to-noise ratio (SNR), error rates, and packet reception quality, making it a better indicator of link reliability. Mesh networks are designed to be resilient and can operate even if some nodes fail as the network is self-monitoring and the communication path dynamically resets if a mesh repeater fails. As with the BLE RSSI requirement, the Zigbee network should be tuneable to support accurate positional discrimination.

Infrared and Ultrasound

Both Infrared (IR) and Ultrasound (US) technologies provide precise location discrimination, often down to 1 metre positioning. The IR and US technologies require a receiving device to be installed in every location or room making them the most cost and labour-intensive options to deploy. Both wired and battery powered options are available with wired devices being more expensive to install, and battery devices requiring frequent battery changes during its operational lifetime. Although these systems have been available for many years, their use is decreasing with the increased use and performance and better price point of other options.

Mobile device activator types

There are several varieties of activators for generating mobile duress calls. Within the clinical and supporting spaces the two common options are:

Handheld mobile devices

Handheld mobile devices are typically Android based mobile handsets but may also be proprietary operating in the RF 900MHz ISM band rather than on the Wi-Fi.

- When used, these devices are generally supplied as an integral part of the area Nurse Call system and in addition to having an easy duress activation such as an accessible button on the top or back, they are also used to coordinate staff responses to standard nurse call system activations. This approach helps reduce the number and type of devices on-duty personnel need to carry.
    - Both duress and nurse call systems available from the many vendors have standard and common features supporting clinical operations. Many Nurse Call vendors include additional features in their handsets such as staff/patient voice communication, call escalation and call transfer, and advanced features such as integration with auto-initiated calls from sensors, smart-beds, and patient movement systems. Support of the clinical operations and workflow is essential and therefore when considering these types of activators, the required clinical consultation in design and product selection becomes more complex and critical.
    - Usually worn on a belt clip or kept in a pocket, the device can become a target for an offender and the wearer of the device prevented from accessing or activating it. Several of the options include man-down or fall detect and can auto-generate a call if the holder is being restrained. They may also transmit audio of the event during an activation to first responders. This feature can be very useful in larger facilities but in smaller wards and areas the limited response distance reduces the need to this feature. It is better in “silent wards” with limited or no corridor annunciators but of limited value in areas where annunciators are prolific such as Emergency Departments.
    - The handsets must have the capability to last a full shift with hand-over time. Shift lengths may vary from 8 to 12 hours. Battery life can be compromised if the handset is being used extensively as a Nurse Call system component or running Apps and voice calls during the shift. Generally, handsets specially adapted for the use as a Nurse Call / Duress device will have exchangeable batteries to reduce the number of handsets required however to support shift changeover and visiting clinicians, visitors or staff, as many as twice or more devices are needed for the number of staff on the ward.

- These types of devices are expensive, often in the order of NZ$3000 so cost of purchase, support and repairs can be expensive. They are also more complex and require some staff training in their use. This makes them much less acceptable as duress alarms that can be given to visitors to the facility including judicial personnel in mental health facilities, and visiting clinicians and consultants, or contractors who may be required to work in the facility where duress risk is identified.
- Healthcare facilities often issue mobile devices to staff to support their daily work functions. Clinical and operational staff do not want to carry multiple devices. When using a handheld mobile device for Nurse Call, the handset must be able to perform the functions of the issued mobile device in addition to providing easy-to-use duress capability. This may require careful review by the Data and Digital teams to ensure that these mobile devices which are aften running locked-down older versions of Android or proprietary operating systems do not present a cyber security risk to the facility. The device would therefore need to be managed on the facility Mobile Device Manager platform.

Pendants/Fobs

Pendants and fobs come in a variety of form-factors and may be lapel fobs, wristwatch like activators, rip-off tags and may also include man-down capability.

- These are lower cost devices and not integrated at the device level into the Nurse Call system. Typical costs for fob devices are in the order of $400 with associated pagers being closer to NZ$600.
- These devices feature rechargeable batteries with typical charge times exceeding 12 hours, sufficient for shift with shift changeover times.
- As lower cost devices they are more suitable for casual issue to visiting clinicians, other visitors to the ward or area, and to contractors who may need to carry personal duress alarms when working in higher risk areas with supervision or monitoring by clinical or security personnel.
- These types of devices may operate on Wi-Fi but more generally they operate in mesh receiver systems using Zigbee protocol or similar. Some iterations may also operate in the 900MHz ISM band as an RF system.
- A lapel, rip-tag, or fob pendant is a wearable and does not limit the clinical staff from using a handheld mobile for the daily functions, it may provide additional benefit in that a mobile device is more likely to be targeted by an aggressor which may restrict duress activation. Should the aggressor attempt to remove a fob device, its alarm would be generated.

Reference standards

1. Health New Zealand Guidance, Procurement considerations from Mobile Duress Alarm Systems (Health New Zealand - Hauora Aotearoa, 2022)

This guidance notice is restricted to implementation within mental health facilities notes that mobile duress alarm systems are only one element of the protective services and systems needed to work together as a homogenous safety and security structure needed to support the safety and security of staff, patients, and visitors in mental health facilities.

The document provides considerations for designers to reduce the risk of flawed design and implementation but does not provide detail on risk assessments throughout different wards and facilities nor does it identify the key stakeholders who need to provide input. Being limited in its scope to mental health facilities, the document does not consider the differences between other wards and facilities such as the Emergency Department or Maternity where visitors and patients may arrive out-of-hours, and the differences in these spaces where annunciators are prolific, and the "silent ward" expectation of the mental health facility is not a critical design element.

2. AS3811 – Hard-wired consumer communication and alarm system for use in healthcare facilities.

Although AS 3811 was withdrawn in June 2017 it remained widely referenced in Australia and New Zealand as a reference standard. This did not include references to mobile systems or duress systems in its first edition. As of January 2025, this standard is being rewritten and has released for public comment prior to being accepted and issued. Although retaining the hard-wired reference in the title, there is now content relating to the design of systems with mobile duress capability. It is anticipated that the final released version of this standard will be in the second quarter of 2025.

3. ACT Healthhub /technology (Saxena, 2019)

The St-08 Security ICT Standard issued by the Australian ACT (Australian Capital Territory) Health Digital Solutions Division contains references to both fixed and mobile duress system implementation. The preference of this standard for mobile duress is Wi-Fi (802.11n) with staff members carrying either a pendant or handset, neither is given preference. While the system uses the Wi-Fi RTLS capability, additional beacons and transceivers may be required to allow "right side of the wall" location discrimination.

4. AHFG (Alliance, 2018)

The AHFG Part C Design for Access, Mobility, Safety and Security includes content on both fixed and mobile duress systems. Fixed duress locations are advised in the AHFG Standard Room Layout data sheets. Additional requirements for mobile duress support are included and recommended to be implemented when appropriate through the risk assessment process.

This standard contains many references to the need for Duress systems to integrate and communicate with Nurse Call systems, the Electronic Access Control System (EACS), and with CCTV systems to provide a homogenous security environment. This standard does not specify brands or technologies directly and allows for fixed duress and mobile duress to be separate vendor solutions assuming the ability of these systems to communicate and share alerts and data.

5. Protecting People and Property, NSW Health (Health, 2022)

Like the ACT document, this standard also provides references to both fixed and mobile duress. It also provides guidance on these systems noting that fixed and mobile duress may be separate systems subject to the ability of them to communicate activations and data, and that they also should communicate effectively with other security systems such as EACS and CCTV.

This document provides more guidance on risk assessment and risk mitigation with less engagement in the technical characteristics of any duress system.

Reference standards summary

The five referenced documents provide significant guidance on risk assessment, the major features of the duress and safety systems, and the need for these systems to integrate effectively in real-time with other systems such as EACs and CCTV. This interface allows appropriately programmed EACS systems to confine risk and for CCTV to engage and collect evidentiary recordings of events generally with higher frame rate recording and longer before/after recording intervals.

None of these standards specifically reference vendors, unique vendor features, nor do they influence the choice or product or technology beyond that which appropriately addresses the risks identified in the risk assessment process. Although the Health New Zealand Guidance for mental health facilities notes that it could consider further assessment to see if a one-size-fits-all approach could be developed, this is not an approach favoured by any other international standards nor the AHFG which is the guiding document suite for the design and development of Health New Zealand facilities. Given the disparity even between high and lower acuity mental health facilities and community based residential and outpatient facilities, and areas other than mental health facilities that also require fixed and mobile duress systems, a one-size-fits all approach seems unlikely to yield the safety and personal protection required.

Whole of life cost considerations

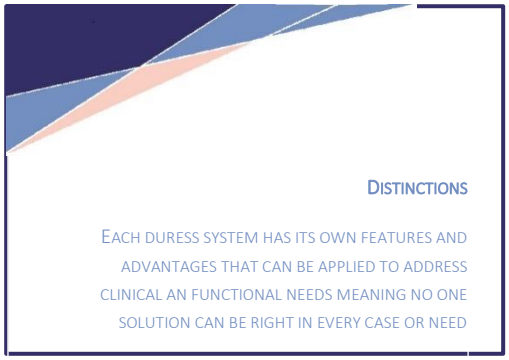
The duress systems must meet the requirements of the Risk Assessment and provide the safety and security needed by staff and visitors in the identified areas. The initial installation of the selected product set represents a significant capital expenditure however the system must continue to function providing the surety needed and this can represent substantial ongoing operational expenditure. The selection and design of the duress system needs to consider both capital expenditure and operational expenditure and should include:

- The capital expenditure must be appropriate to meet the risk assessment needs but also needs to be appropriate to the construction budget. There are generally several options for duress systems that will provide and satisfy the performance expectations however over-engineering with unnecessary features and functions is likely to escalate costs without providing tangible return.
- Duress systems include firmware and software components. These should be reviewed to ensure that appropriate firmware and software updates and available, any costs for these updates are considered, and the facility is made aware of changes and updates in firmware and software that can affect performance through vendor release notices. This will allow the system owner to prioritise critical updates for urgent application and schedule minor updates to a more convenient or less disruptive time.
- All duress systems require maintenance and support to ensure ongoing reliability. The system owner should review this operational expenditure during its assessment of vendor solutions. Options should be considered for 8x5 maintenance on non-critical faults and 24x7 maintenance for critical outages and recognise the capability to provide service in regional locations. It is recommended the supporting agent have the ability to log in to the system remotely and where possible implement solutions to resolve problems. A duress system that self-monitors and auto-alerts the supporting agent is recommended.
- User devices such as mobile handsets, fobs, pagers, and pendants are subject to normal damage during usage. The cost of repair or replacement of these becomes and operational expense and may become significant as these devices age.
- User devices, beacons, and some transceivers include integral batteries. Batteries do age and need replacement. A typical replacement cycle may be three years therefore the availability and ease of replacement of these needs to be considered. This can be considered and included in maintenance contracts.

- When selecting a vendor solution, consideration must be made of the product development roadmap and longevity of support the vendor will provide for the selected components. This includes releases of both firmware and software updates and the longevity of maintenance and repairs before product obsolescence and repair is no longer supported.

Conclusions

An effective duress system must be considered a component part of a facility's overall risk reduction and risk mitigation strategy. The duress system cannot be considered a standalone system without the need to interoperate with other key security measures such as Electronic Access Control, CCTV, Nurse Call, and ICT systems.



The first step in considering design and application for any duress system is the risk assessment. This assessment cannot be done as a "desk-study" but rather needs comprehensive engagement with the critical stakeholders including the clinical staff who will be those using the duress system for their own safety. (Health, 2022)

Business continuity plans using the Risk Assessment observations must account for any potential loss of critical systems and security measures that support the duress system and the staff, service users, and visitors to all healthcare wards and departments. This includes planning for loss of communication, loss of electricity that may affect electronic access control or duress measures, theft or vandalism of key components, processes for emergency repairs, and loss of security services. Risk of theft or vandalism may impact the placement of duress system receiver devices, similarly in high acuity mental health facilities devices with illumination or flashing lights and trigger service user responses and discrete or "above the ceiling" installation may be required which will affect signal propagation.

There are many different duress system vendors installed in healthcare facilities in New Zealand. While accepting that all have similar core sets of function and capability, they also have their own specific features, product set extensions, and capabilities that can be applied to the installation to satisfy the specific environment and stakeholder needs.

As the needs of various wards, spaces, and facilities will vary even on a single healthcare facility site, it is apparent that identical configurations in disparate areas may not deliver the level of personal safety and duress response required in each case. It is therefore considered that a predetermined configuration or device selection is unlikely to deliver the support required in all instances and design and product selection can only be undertaken once a comprehensive risk analysis and response strategy has been determined.

Torque IP

Head office

Phone +64-9-526-4396
Fax +64-9-526-4394
Email info@torqueip.co.nz
Web www.torqueip.co.nz

4 Turama Road
Royal Oak
Auckland
New Zealand