

How to Evaluate Lone & Remote Worker Solutions



A Guide to Selecting the Right
Solution for Your Organisation.



Protecting Your Employees

If your organisation needs to ensure the safety of your staff when working alone or remotely, you need to understand the different offerings available on the market.

Finding the best fit-for-purpose lone worker solution and provider can be a minefield. Once you start investigating the market, you'll find there's a great deal of choice. And once you start looking at things in more detail, you will realise it can get very complex.

There are so many moving parts to consider: the hardware functionality, the software functionality, the processes for use, the incident response co-ordination, the training of end users, the maintenance of the data and the regular testing.... it is not surprising that many organisations find it challenging to understand the right requirements for their lone and remote worker safety solution.

At Guardian Angel, we've worked with these solutions for over 12 years and still we investigate new products and have to ask many detailed questions to understand the suitability of the solution. Additionally we are protecting thousands of people across Australia and New Zealand every day with our solutions, and we have co-ordinated response to many incidents from missing persons and remote vehicle break downs, to serious threat and violence so we know how exactly to deliver true safety.

It's a lot to expect someone without a background in networks and GPS technology to try to figure it out and you have a big job to do already. There are some fundamental understandings required and some probing questions you need to ask, to ensure you don't go down the wrong path (or indeed get led down the wrong path).

We hope that this buyer's guide will help you in the evaluation process.



1. Core knowledge

Glossary of terms and functions

Satellite based solutions:

Means they rely on a satellite network to send/receive data, and therefore only work outside

Iridium:

The only satellite network with 100% cover and forwarding technology

Cell based solutions:

They use GPS to locate, but need cell cover to send/receive data

GPS:

Global Positioning System (used for location – not for transmitting)

Working inside buildings out of cell cover:

If you're out of cell cover, and working inside buildings, you will need to use a bridge/pendant system with the bridge staying outside. Satellite cannot see through roofs and dense cover.

Working inside buildings in cell cover:

If it's a fixed site, it's not a problem but if staff are entering various buildings throughout their day, you need to ensure the solution is tracking (and sending updated location to a mapping hub) at a min 1-3min rate. This way, should they have an incident inside a building where the GPS doesn't work, we can look at the breadcrumb trail and work out where they are. You may also require indoor locating beacons if you have vast or multi-storey buildings.



1. Core knowledge cont.

Glossary of terms and functions

App based solutions:

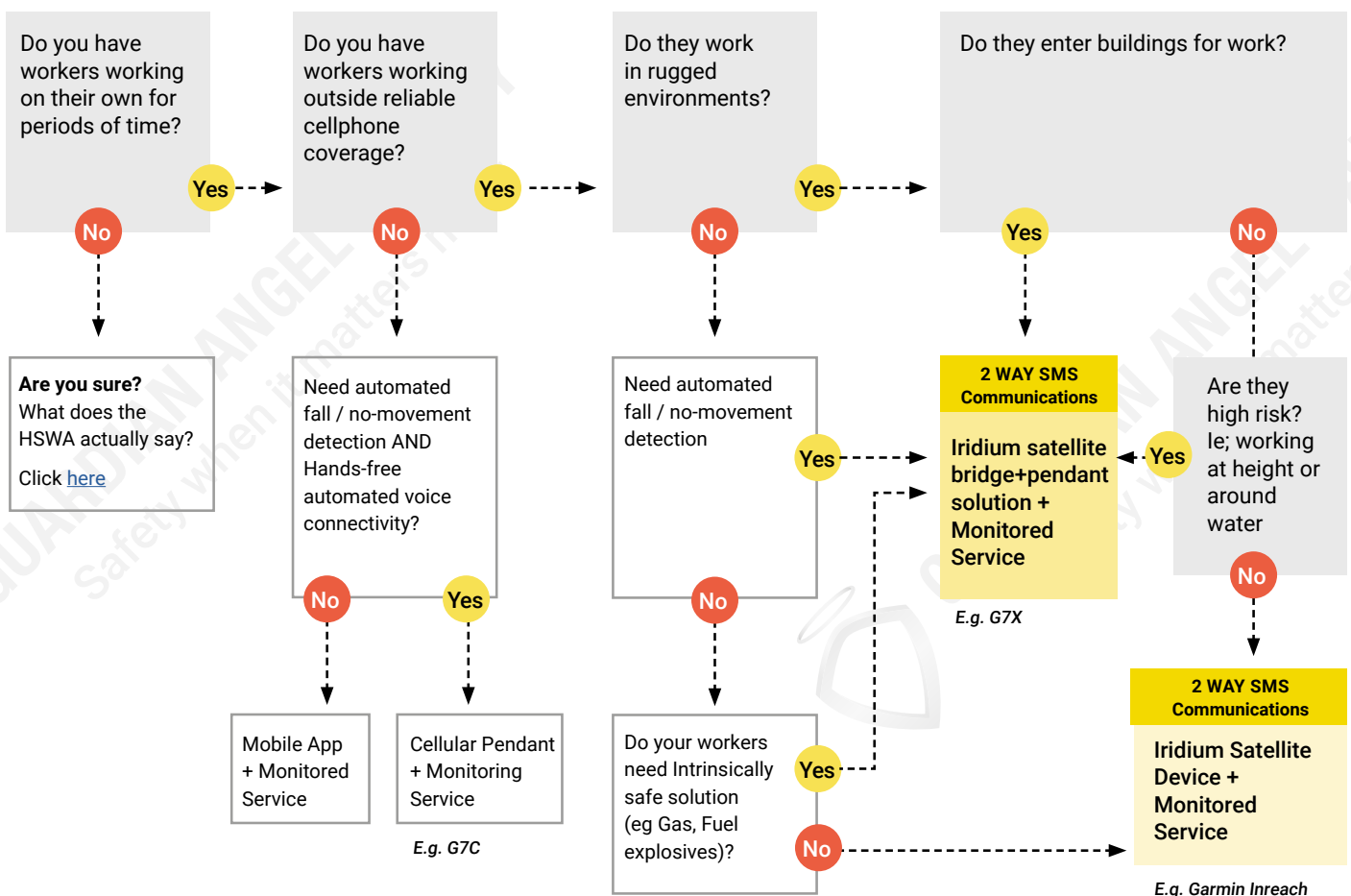
- Location services are required to be active
- App needs to be launched –
 - Battery drains approx 30% faster when a GPS tracking app is in use
 - Older phones experience particularly bad battery drainage
- Phone needs to be in their hand (unless paired with a Bluetooth button)
- Difficult to report on compliance / hours of operational use
- Antennas and GPS chipsets on panic devices are typically superior to cell phones
- Software update compatibility –
 - When new Android and iOS operating systems are released they can disrupt the functionality of the App
- If your staff are at risk with threats from other people, evidence suggests the perpetrator will not allow their victim time to activate an SOS – as their priority will be to disarm or disable their phone



2. Decision process

Understanding the right solution for your organisation.

We've compiled a detailed decision flow in the diagram below which helps you to understand the right solution for your organisation.



ALL GOOD SOLUTIONS HAVE 2 WAY COMMUNICATION AND WELFARE CHECKS AS STANDARD



3. Important Questions

Understanding the right solution for your organisation.

1. Can your staff rely on cellular network coverage ("cell cover")?

If it's "mostly yes" ask around and work out what percentage of time they can't (if ever). Is it 5, 10, 20% of the time? If they're simply driving through patchy areas, that's less of a concern than if they are actually undertaking tasks outside of cell cover. Then you have to decide what percentage out of cell cover you are willing to accept as a risk.

2. Are they out of cell cover but working inside buildings?

(most satellite solutions need a view of the sky to work)

3. Are they in cell cover and working inside buildings?

(GPS can't see through roofs so we need to establish tracking rate, and if you need to use indoor locating beacons)



4. Important Questions

Understanding the right solution for your organisation.

If your workers are always in cell cover and you're looking at a cell based duress device; ask these questions:

- 1. What is the polling rate of the device?** (look for 1-3 min location send so that we can find them if they've entered a building by looking at the breadcrumb trail)
- 2. How often does it poll when in alarm?**
(you need to find your person if they're running or driving)
Make sure it doesn't just send location when in alarm
- 3. What is the battery life of the device set to 1-3min polling?**
(look for at least 15 hours)
- 4. What is the accuracy of the location? (look for +/- 5m minimum)**
- 5. Has it been SAR (Saturation Absorbency Rating) certified? (safe to wear)***
- 6. Will it still work when 2G and 3G is decommissioned**
Be aware of 2G devices with 3G or 4G SIMs
- 7. Where is it manufactured and what are the warranty terms and support?**
You want to know that your chosen device is not going to end up an orphan product, but is going to be continuously invested in and improved upon and keep your staff safe for years to come.
- 8. What is the IP rating?** (rating should be 65 to 67)
- 9. Does it have fall/no movement and automated welfare checks functionality ?**
- 10. Are settings configurable and how are updates received?**
(you want to be able to change tilt angles, delays etc over air)
- 11. Does it have two way voice functionality?***



5. Device Requirements

Understanding the right solution for your organisation.

***SAR (Specific Absorption Rate):**

A SAR certified device means that it does not emit harmful levels of radiation. You are asking your staff to wear this device for hours at a time, they need to know it's safe. All mobile phones sold in New Zealand and Australia must pass the SAR test. Unfortunately, there is not any policing in regards to other devices such as duress devices so many products are imported and sold on our markets without the necessary certifications. You should ask to view the SAR certificate (the full report is around 60 pages, but you only need to see the signed certificate page). The certificate should state that the testing has been carried out in a NATA approved test lab.

***Voice:**

If your solution has voice capability there are a few things to consider. Does the device auto dial a number? Or does the monitoring station call the device which then auto answers? Both are worth considering depending on the monitoring station and risk environment. You do not want the call getting lost in the monitoring station phone system loops, or terminating at the voice mail, so you need to ensure this can be overcome. If this cannot be assured, then having the monitoring station call the device on activation and having it auto answer is a better option. A good monitoring station will record the calls which is powerful for future evidence in any legal proceedings and/or training. Likewise if you are managing response in-house, you don't want the call terminated when it hits an answer phone service.

Some devices only have one way voice. So, the monitoring station can hear the user and what is taking place, but the user cannot hear the operator. This can be useful if you do not wish the sounds from the monitoring station to exacerbate the situation the user is in. Although some devices allow the volume of the outgoing microphone to be turned down very low so that any noise from the monitoring station will not be too audible. This would however allow the user to put the device up to their ear if it is safe to do so. They can then communicate what assistance they require or to allow Emergency operators to triage the worker until assistance arrives. We do find in real situations that it is a great comfort to our worker to have an operator providing updates on how far away Emergency Services are.



6. Important Questions

Understanding the right solution for your organisation.

If your workers will be outside cell cover, then you will need a satellite solution. Ask these questions:

1. **Does the device use the Iridium satellite network?**
(this is the only network with no gaps in cover and forwarding technology)
2. **Does it keep sending the message until a satellite receives it?**
3. **Does the user get a confirmation that the message has been received?**
4. **What is the minimum and maximum tracking interval and associated cost?**
5. **Where is it manufactured and what are the warranty terms and support?**
6. **What is the IP rating?** (rating should be 65 to 67)
7. **Are settings configurable and how are updates received?**

If your staff are working inside buildings, out of cell cover:

1. **There are solutions which can bridge a pendant for the worker to wear to a hub in the vehicle (or elsewhere on site) which means it will work anywhere**
2. **What frequency is the pendant on?**
(should be 915-928 for NZ/AUS – anything outside of this is illegal)
3. **Is the location of the actual pendant sent as well as where the base station/car is?**



7. Monitoring Questions

Understanding the right solution for your organisation.

Questions to ask of your monitoring centre:

1. **Is your centre graded or government audited to supply medical monitoring?**
2. **Is it a professional monitoring centre with trained operators and commercial response software for managing signals in priority?**
(or is it a customer service department)
3. **Is the centre staffed 24/7?**
(yes we know of places where the signals go to a mobile phone after hours)
4. **What business continuity systems, policies and procedures are in place?**
(they should have multiple providers for their internet, phones and power and a back up centre in case their building has to be evacuated)
5. **What reporting do you have available?**
6. **How often are operators trained?**



8. Monitoring Requirements

Understanding the right solution for your organisation.

Communication paths:

Most devices will send the GPS location and emergency alert via SMS/Email and of course via IP or API to the mapping hub that it “lives” on. The server that receives the alert, then generates the SMS/email to contacts that have been set up on that account. Relying on email or SMS to colleagues or indeed a monitoring centre, is really not robust enough for critical alerts. Emails and SMS, especially if generated on an overseas server are very likely to get caught in spam filters.

Of course you might choose to have the mapping portal open on a monitor at all times so that someone will see/hear an alert come in. Without two people, 100% dedicated to just this monitor there is no guarantee that someone will see it (and sick/lunch break cover etc). Even a monitoring centre relying on a platform being open is not good practice.

A graded monitoring centre with API integration in place means that the alert cannot get delayed or lost. It will come straight into the response software and create an alarm with the response instructions popping up in front of the operator.

A graded centre will also have all the business contingencies in place so that no matter what happens to the building or the systems within it, your staff are always safe.


A graded monitoring centre will have a direct dial line to Emergency Services. This means our operator does not have to waste time on the public queue and then talk to the operator first about what service they require, the location of the incident and provide further information. This considerably speeds up response time.

In both New Zealand and Australia, Emergency Services will be hesitant to respond to a panic alert if it is not monitored by a reputable provider. In Australia the Police requires an Alpha Code to facilitate dispatch and these are not issued to monitoring providers outside Australia.



9. API Integration

Understanding the right solution for your organisation.

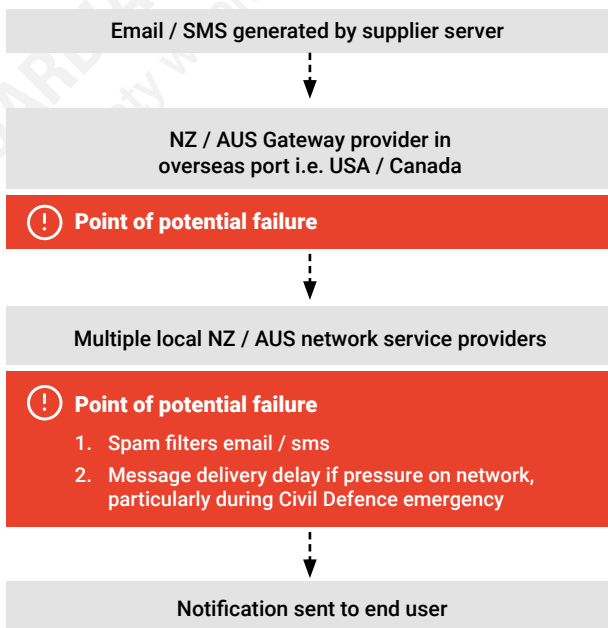
 **SOS Activated on device**



Alert received by device supplier mapping portal i.e. Everywhere, Garmin, Blackline Safety



Without API



Alert received by Guardian Angel Monitoring station response software platform in **REAL TIME**

API



Application Programming Interface



With API



10. Additional Considerations

Understanding the right solution for your organisation.

Nice to haves

Good solutions will be able to provide you reporting on how often and how long devices are in use, alerts raised (with location) and other insights.

Privacy Act considerations

- **In NZ – Changes to the act came into effect on 1st December 2020.**
- All staff handling personal information (response instructions and escalation lists etc) should undergo privacy training. Suppliers should also have all the systems in place for notifying of any breaches, as should their suppliers, and data collected should never be permitted to be used for any other purpose outside of supplying you our services.

Cyber Security

- Cloud solutions should be implemented, operated and governed in accordance with a clearly defined and documented security model
- Automated tools for malicious code detection, vulnerability detection and other code quality issues should be used. Production deployment should use digital signed code to prevent unauthorised code use. Access to the system should be limited to essential personnel only, using the least privilege model.



Fit for Purpose Solutions

Get the right solution for your organisation.

At Guardian Angel Safety, we know from experience that the 1% of the time that things go wrong, they often go terribly wrong and **our solution needs to be 100%**. No compromises. That's our promise to our lone workers. They need to trust us and our solutions or we don't have a business (and we wouldn't sleep at night!)

We understand the market is a minefield, so we take the time to get to know the risks your people face and make unbiased recommendations tailored to your business, as like many of our clients, you may require a combination of solutions to suit the risk profiles of different staff. Our solutions are backed up by our own best in class training and support services.

If you'd like to talk to someone about the right solution for your organisation, please contact us:

info@guardianangelsafety.co

NZ +64 9 480 0860

AUS +61 7 39111332

Petra Hakansson | CEO & Founder
petra@guardianangelsafety.co
+64 211916024

The content contained in this publication is provided only for educational and informational purposes. Guardian Angel Safety Ltd. attempts to ensure that content is accurate and obtained from reliable sources, but does not represent it to be error-free. All material appearing in this publication ("content") is protected by copyright under New Zealand Copyright laws and is the property of Guardian Angel Safety Ltd. You may not copy, reproduce, distribute, publish, display, perform, modify, create derivative works, transmit, or in any way exploit any such content, nor may you distribute any part of this content over any network, including a local area network, sell or offer it for sale. Date of publication July 2021.





GUARDIAN ANGEL SAFETY

Safety when it matters most

