



A consideration of reasonably foreseeable scenarios with the RedDNA Sentry 500 RedWeb Security (UK) Ltd.

April 2008

Version 1

Produced by: Human Applications
The Elms, Elms Grove
Loughborough
Leicestershire
LE11 1RG, UK
Tel: +44 (0)1509 211866
Fax: +44 (0)1509 218344
Email: enquiries@humanapps.co.uk
Web: www.humanapps.co.uk

Author: Matthew Trigg BSc (Hons), DPS, CMIOSH
Quality Check: OOR

Management Summary

This study was commissioned by Clive Smith of RedWeb Security (UK) Ltd. RedWeb wishes to identify any reasonably foreseeable scenarios in which persons may be harmed by the installation or deployment of its products.

This study considers three usage conditions for the Sentry 500:

- Installation and maintenance
- Automatic deployment (arming and triggering)
- Manual deployment (manual arming, automatic triggering)

We have considered a range of scenarios, some of which present no risk of harm to any parties. Where a scenario has been identified that presents concern, we have identified measures that RedWeb may take to control those risks.

The following scenarios have been identified as being reasonably foreseeable:

- 1 Installer triggers deployment whilst working from a ladder
- 2 Person subject to deployment falls down a change of level of floor
- 3 Person makes authorised entry to premises whilst system is armed
- 4 Innocent party is sprayed as a result of manual arming of system

In addition, systems designed to trigger when assets are tampered with are discussed. Here, consideration is given to the protection of those whose normal activities might expose them to accidental deployment, such as cleaners or maintenance personnel.

For each scenario, the conditions that are required to trigger an incident are described. Existing controls are identified.

For each scenario, actions on the part of third parties are described. For each scenario, we make recommendations for action by RedWeb. In most cases, RedWeb's role will be to direct the installer or customer to consider the identified scenarios.

In normal deployment, we do not consider that the product presents reasonably foreseeable risk of harm to people. In two of the scenarios, consideration is given to the effect of sudden deployment on a person who may fall a distance likely to cause injury.

Contents List

1.	BACKGROUND AND INTRODUCTION	4
1.1	Background.....	4
1.2	Scope and approach	4
1.3	Structure of this report.....	4
1.4	Caveats	4
2.	ABOUT THE REDWEB SENTRY 500	5
3.	DEPLOYMENT SCENARIOS.....	6
3.1	Installation and maintenance	7
3.2	Automatic deployment	8
3.2.1	Automatic deployment following unauthorised entry	8
3.2.2	Automatic deployment following authorised entry	9
3.3	Manual deployment.....	10
3.4	Other usage scenarios.....	11
4.	CONCLUSIONS	12

1. BACKGROUND AND INTRODUCTION

1.1 Background

RedWeb Security (UK) Ltd. brings to the market a range of delivery systems of its patented security products. As part of its desire to ensure the safety and usability of its products, Clive Smith, Chairman of RedWeb requested a review of reasonably foreseeable scenarios for deployment of the RedWeb Sentry 500. Matthew Trigg, Senior Consultant, Human Applications met with Clive and his colleagues on April 11th 2008. This report presents an analysis of the usage scenarios developed as a result of this meeting.

1.2 Scope and approach

This study considers three usage conditions for the Sentry 500:

- Installation and maintenance
- Automatic deployment (arming and triggering)
- Manual deployment (manual arming, automatic triggering)

We have considered a range of scenarios, some of which present no risk of harm to any parties. Where a scenario has been identified that presents concern, we have identified measures that RedWeb may take to control those risks.

The findings of this report are based on consideration of technical materials provided to us by RedWeb, and on discussions between RedWeb and Human Applications.

1.3 Structure of this report

This report is presented in 4 sections.

- Section 2 describes the Sentry product and its intended use.
- Section 3 lists the usage scenarios and presents, in table form, the conditions for the scenario to lead to an adverse incident. Recommendations to control the conditions for the scenario to lead to incident are given.
- Section 4 summarises the findings of the study.

1.4 Caveats

The application of reasonable foreseeability necessarily requires a subjective judgement to be made. Most of the scenarios presented here are unlikely to occur, though we consider them to be within the bounds of reasonableness.

The sprayed product (RedDNA) has been assessed by A.J Collings of Product Safety Assessment Ltd. The associated report states that “product made to this formulation is unlikely to produce an abnormally high number of adverse reactions”. Given the deployment scenarios considered in this toxicology report, “minimal eye irritation” appears to be the most significant harm arising from contact. As a result, we have made the assumption that RedDNA will not cause harm. Our focus therefore is on the delivery system, the Sentry 500. Our findings are likely to be broadly applicable to other models currently in the range and to future models where the same substance is delivered as a misted spray.

2. ABOUT THE REDWEB SENTRY 500

The RedWeb Sentry 500 is designed to deliver a unique marking substance (RedDNA) onto the perpetrators of crimes at the scene of crime.

It is designed to be installed in a variety of configurations, with the sentry unit that delivers the misted spray typically sited over routes of entry and exit. It can be installed as a stand alone system though it will typically augment existing and new security systems.

The system is passive until armed. Arming may be in the form of an automated signal or manually, using a “panic alarm” system designed to be activated by the system user.

Once armed, each Sentry unit is triggered when its microwave Doppler senses a body passing through its field of detection.

On triggering, the full contents of the spray canister are released in the form of a very fine, misted spray. One standard application directs the spray downward from an overt unit (such as one mounted over a door) or from a covert (typically roof-mounted) unit via a discreet nozzle.

It is likely therefore that the system will not deploy other than at a person who is passing through the sensors on foot. The system will, however, deploy when the Doppler is activated regardless of the direction of motion of the target. As a result, it is possible that a person entering a site after the system has armed may be sprayed.

3. DEPLOYMENT SCENARIOS

The three modes of deployment that we have identified are as follows:

- Deliberate or accidental deployment during installation and maintenance
- Automatic deployment, where the system is armed by automatic sensor and triggers by microwave Doppler
- Manual deployment, where the system is armed by the user and triggered by microwave Doppler

We also consider the use of systems designed to deploy when equipment is tampered with.

3.1 Installation and maintenance

Specialist personnel will install the Sentry system. To date, RedWeb have installed the majority of systems. It is anticipated that ADI Gardiner will supply the systems via a network of approved and licensed security installers.

The installation of this, as with any, security system should be the subject of risk assessment by the installers. We understand that installing this system is broadly similar to installing other detection equipment.

<p>Reasonably foreseeable deployment scenario 1: Unit is armed and triggered whilst installer is in proximity to the unit.</p>
<p>Incident conditions:</p> <ul style="list-style-type: none"> • Installer is working on live system. • Live aerosol is inserted in Sentry unit. • Unit becomes armed.
<p>Incident:</p> <ul style="list-style-type: none"> • Installer is sprayed with product. Product is not harmful at levels present with full contents discharged • Installer falls from ladder/platform
<p>Existing controls: Installation requires the use of water-only aerosol, so no contact with product should occur. RedWeb report that system has fail-to-safe mechanism that prevents accidental discharge. System is installed without aerosol. Aerosol canister is inserted only once mounting and connection are complete.</p>
<p>Actions by third party: Installer: Installers must include consideration of Work at Height Regulations 2005 in their risk assessment strategies.</p>
<p>Actions by RedWeb Security (UK) Ltd.</p> <ol style="list-style-type: none"> 1. Check that standard installation protocols deal with issue of installing and maintaining systems when live. If not, include as part of product-specific instructions. 2. Product-specific instructions must include note to use water-only aerosol for all test applications.

We understand that RedWeb has already considered the following scenario for non-operational activation:

- Following deployment, a specialist evidence-gatherer may enter premises to collect swabs and other materials. Once one unit is deployed, other linked units in the same system are stood down. This prevents the evidence gatherer being subject to a secondary deployment.

We consider therefore that there is no reasonably foreseeable condition in which evidence gatherers may be placed at risk by the system.

3.2 Automatic deployment

There are two scenarios where automatic deployment may occur:

- In intended operation, following arming of the system as a result of unauthorised entry
- In unintended operation, following arming of the system by the premises occupier gaining entry without first disarming the system.

In both cases, following arming, a person passes within the field of detection of an armed unit and triggers the deployment.

The product is sprayed in a mist, typically from above head height.

3.2.1 Automatic deployment following unauthorised entry

<p>Reasonably foreseeable deployment scenario 2: Unit is armed on unauthorised entry and triggered, deploying misted product at person.</p>
<p>Incident conditions:</p> <ul style="list-style-type: none"> • There has already been activity to arm the system • Person passes through the field of detection, typically on exit • Person is in some location that makes them vulnerable to falls, such as on a ladder or platform, or on the threshold of a change of level such as steps, stairs or a window-ledge
<p>Incident:</p> <ul style="list-style-type: none"> • Person is sprayed with product. Product is not harmful at levels present with full contents discharged • Presence of mist disorientates person causing them to fall.
<p>Existing controls: None applicable.</p>
<p>Actions by third party: Installers: selection of location for unit should take account of potential for person to fall immediately following deployment.</p>
<p>Actions by RedWeb Security (UK) Ltd.</p> <ol style="list-style-type: none"> 1. Instruction to installer should advise that unit should not be placed at a point where there is a significant change of floor level.

It is important to note that the deployment of the aerosol generates no significant force on the person sprayed. Rather, in this scenario, the presence of an unexpected airborne substance may cause the person to react and fall. In consultation with RedWeb, it is considered unlikely that a person making their escape from the scene of a crime will notice the deployment. This scenario is therefore at the limits of what we might reasonably predict may occur. Nevertheless we have considered that it fits within the bounds of reasonableness.

Note also that where there is no risk of falling from one level to another, this is the normal intended deployment and there is no reasonably foreseeable source of harm to the sprayed person.

3.2.2 Automatic deployment following authorised entry

<p>Reasonably foreseeable deployment scenario 3: Unit is armed on authorised entry and triggered, deploying misted product at person.</p>
<p>Incident conditions:</p> <ul style="list-style-type: none"> • On authorised entry to premises, the system is not first disarmed • Person passes through the field of detection, potentially on entry, possibly when approaching a unit once inside the premises
<p>Incident:</p> <ul style="list-style-type: none"> • Person is sprayed with product. Product is not harmful at levels present with full contents discharged
<p>Existing controls: In some cases, we understand that installation may link entry to premises with the need to disarm the system. One such system might require a maglock to be powered down before the main door can be opened. Since this is not a universal condition, some systems will require the user manually to disarm the system. In these cases, we predict that accidental discharge is likely to be a regular occurrence. Note that the result of accidental discharge is not harm to people.</p>
<p>Actions by third party: Installers: in specifying systems to customers, recommendation should be made to install an interlock that disarms the RedWeb system on authorised entry.</p>
<p>Actions by RedWeb Security (UK) Ltd.</p> <ol style="list-style-type: none"> 1. Since the systems are in many cases designed to be covert, there is no practicable means of alerting the authorised entrant of the need to disarm the system without alerting others to the presence of the system. 2. Consider mandating the design of systems to include an interlock. 3. We recommend that RedWeb monitor incidents of this type of unintended discharge (possibly via their re-seller). Should these incidents prove common, the need to mandate an interlocked design may increase.

Where an interlocked installation is present, this event should not be foreseeable. Where the system relies on manual disarming, we anticipate that accidental discharge will occur in significant frequencies. The consequence of this scenario will be inconvenience to the customer, rather than injury.

3.3 Manual deployment

In this scenario, the user arms the system. In a typical installation, this may require the premises operator to activate a “panic button”. The system will then deploy once triggered.

Since the system will deploy at the next person to pass through the Doppler field, it is possible that an innocent party may be sprayed, either as they enter the premises or as they leave. The consequences of this deployment will be as described previously – the non-toxic product will be misted over them – and no physical harm should result. The consequences may therefore be limited to managing the concerns and associated grievances of the innocent party.

<p>Reasonably foreseeable deployment scenario 4: Unit is armed manually and triggered, deploying misted product at person.</p>
<p>Incident conditions:</p> <ul style="list-style-type: none"> • User arms system by activating panic button • Person passes through the field of detection, potentially on entry, possibly when approaching a unit once inside the premises • Person sprayed is innocent party
<p>Incident:</p> <ul style="list-style-type: none"> • Person is sprayed with product. Product is not harmful at levels present with full contents discharged
<p>Existing controls: None applicable.</p>
<p>Actions by third party: Installers: provide briefing to customer regarding this scenario. Customer: cascade briefing to all potential users regarding this scenario. Check with public liability insurer to identify where damage to property of innocent party may be an insurable loss. Where appropriate, generate materials to present to innocent party explaining what has happened and any recompense package (such as payment of cleaning bills or goodwill payments).</p>
<p>Actions by RedWeb Security (UK) Ltd.</p> <ol style="list-style-type: none"> 1. The current “Responsibility Code” describes this scenario effectively. 2. Replace “if its (sic) places any persons in the vicinity in danger” with wording such as “if it is likely that a person other than the intended target will pass through the detector first.” Consideration may also be given to an instruction to wait until the perpetrator is walking towards the unit, though this may require a degree of judgement that is unreasonable to expect from a user who is being robbed. 3. Consider whether the production of simple, high-impact instruction material may offer added value to the customer. For instance, a short DVD showing the system being deployed may reassure users that they will not cause harm by deploying the unit.

Again, in this scenario, the consequence of deployment being against an innocent party is not harm. Customers must be made aware of the potential for this scenario. RedWeb as part of its customer service should guide the actions by third parties suggested above. The extent of liability of RedWeb for damages claimed as a result of this scenario is a matter for legal advice.

We understand that future systems may include the provision of RF tags for property, allowing the trigger to be made as the tagged property passes by a sensor. This technology should reduce further the likelihood of innocent parties being sprayed.

3.4 Other usage scenarios

In addition to the systems designed to be installed above access points, some systems are designed to be installed within or around particular targets inside a property – AV equipment, vending and gaming machines, safes, etc. Here the arming and triggering systems may differ from those described previously. For instance, the system may deploy when an asset is tampered with.

As with scenario 3, where there is no interlocking system provided, it is possible that authorised activities such as maintenance, cash collection or even cleaning may trigger the system to deploy. In these cases, systems must be designed to protect the authorised user.

Depending upon the variety of different installation technologies that may be used with these systems, RedWeb should create a matrix of measures to protect the authorised user from unintended deployment. These measures should be provided to installers to guide the selection of technologies to reduce the likelihood of accidental deployment.

Again, we emphasise that the consequence of these deployments is not harm.

4. CONCLUSIONS

The RedWeb Sentry 500 should not cause harm to people as a result of its activation in normal circumstances.

Two scenarios recognise that the sudden release of product could cause a person to unbalance – an engineer working at height or a person at a point of change of floor level – but in neither case is the deployment technology itself the source of harm.

In all other scenarios that we have identified, the consequence of deployment is not harm to people.

Our recommendations broadly direct RedWeb to ensure that critical information is made available both to installers and users of the system. In scenarios 3 and 4, where innocent parties are sprayed, RedWeb's concern is driven by the desire to ensure customer satisfaction, rather than the need to protect people from harm.

In summary, the product as described and demonstrated should not cause reasonably foreseeable harm, other than in combination with other factors as described in scenarios 1 and 2 here.