Version: 2.0
Date established: 2021-02-10
Reviewed by: Richard Ankarman

Securify Best Practices

Guide to successful SpotterRF project **1**
Overview 2
1.1 Project responsibilities 2
1.2 Scope of work 2
1.3 Radar system integration 2
1.4 Fault tolerance 2
1.5 Scene stability 3
Project process 3
Milestones 3
Step 1: Live Demo 3
Step 2: Identify and specify requirements 3
Step 3: Desktop Design 3
Step 5: Installation 4
Step 5.1: Prepare for installation 4
Step 6: Commissioning 5
Step 7: Final Phase: Follow on Alarm Review and Tune 5
Build your quote 5
Design considerations 7
Operator view 7
Alarm presentation 7
Health Monitoring 7
NIO Alarms to VMS 8
PTZ-priority 8
VMS event to NIO 8
Network 9
LAN 9
Remote access 10
IT security 10
Infrastructure 10
Apportionment of liability 10
Liability 11

1. Overview

1.1 Project responsibilities

The value-chain from manufacturer to end-user is:
SpotterRF(manufacturer) → Securify (distributor) → Superior Security (integrator) → Feeling Safe (end-user).

An overview of the installation process that the integrator is responsible for is:
Demonstration → Site Design → Site Survey → Commissioning → Alarm Review
Further details about each step, see paragraph 2.

In case integrator has a shortage of certified personnel performing these steps; Securify can offer consultant services on parts of the process. The result of such a service will be a completed report on the specific step.

It is essential to appoint responsibility for project management at the integrator level.
Who is the appointed project manager for the project?

1.2 Scope of work

Describe what issue/problem that should be solved by the radar system.

For each radar position and area that it covers; describe:

- Purpose
- Hot spot, i.e. what location that the radar is covering is most important.
- What conditions should be met to trigger an alarm?
- How should the functionality of the radar be verified during Site Survey and Commissioning?

Who is going to perform Site Survey and Commissioning of the radar system?

1.3 Radar system integration

Describe how the radar system will be part of, or integrated with, other systems.

1.4 Fault tolerance

What is the level of fault tolerance? How many false-positive alarms per radar or per site and per 24 hrs. is acceptable?

1.5 Scene stability

The settings for one radar are specific to the environment and the scene. The alarms zones and actions in the zones are configured with the environment of the scenes as preconditions. Will the scenes be stable? If not, who is going to re-configuring the alarm-zones?

2. Project process

2.1. Milestones

Step 1: Live Demo

This first step is important to provide an understanding, in regards to how radar works. It is a good idea to not only provide a live demo but if possible, in the client's specific environment.

Step 2: Identify and specify requirements

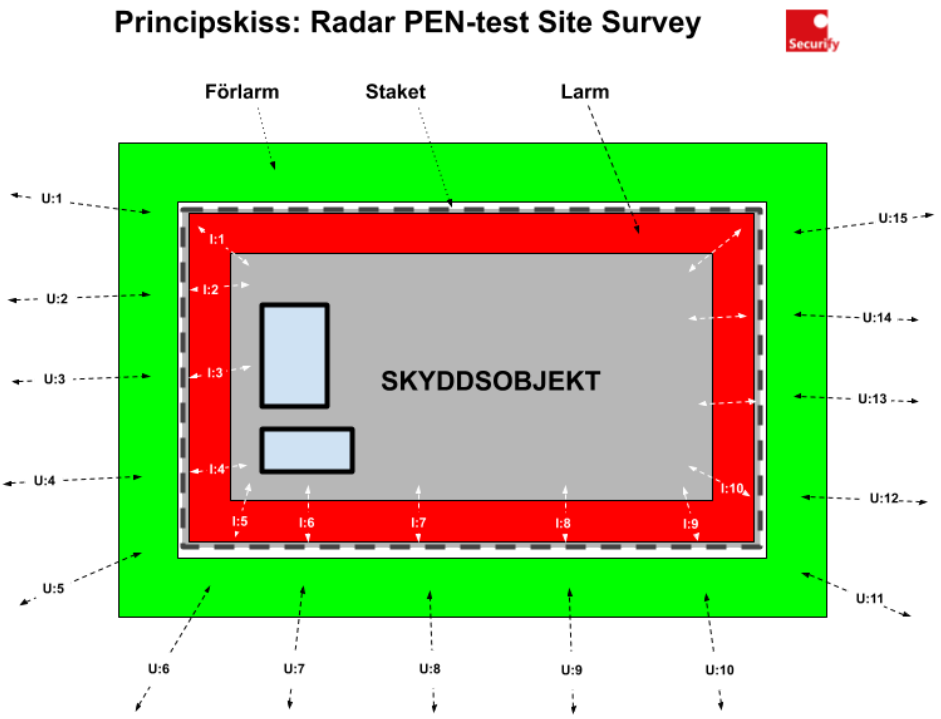
In this step, it is important to understand the client's needs and requirements. Identify critical areas that are supposed to be protected. Consider how and when alarms should be triggered; it is essential to take notes concerning when the alert zone is supposed to be armed and not. In many situations, the alert zone is also the work zone. Input from this step is used to create the PEN-test Map, see image Step 4.

Step 3: Desktop Design

Make a desktop design using "mock radars" and place them on the map. Do consider that this suggested solution might easily be taken for fact or as the final result. Therefore it is important to emphasize and point out that this is only a desktop design. Nothing can be said for the final result until a Site Survey is complete. See the next step.

Step 4: Site Survey

On-site, follow the Site Survey template to compose results from actual testing with the Spotter models included in the Desktop Design. This is where you will get confirmation of whether the desktop design works or not. If need be prepared to test different models and/or positions to fulfill the requirements. Make valuable notes and reflections regarding the actual installment based on the tests. This document should be thorough enough so that an installer would know what to do just by reading it.



Step 5: Installation

Install hard- and software according to SpotterRF recommendations, the Site Survey documentation and best practice.

Step 5.1: Prepare for installation

Avoid any surprises and time consuming hazzle on-site by preparing the installation at your office. Preparing at the office also provides benefits such as getting support from colleagues, providing remote access for escalated tasks or trouble shooting. And beyond all, you are indoor. The overall objective is to make all configuration and test all functionality prior to installations and commissioning. We can promise you a much smoother project with potential to save many valuable hours. Note: this is not typical for a SpotterRF project.

Todo at the office

- Prepare IP-address table (often provided by the end-user IT-dept)
  - Also make a system diagram, it will help you foresee potential problems and also be valuable tool further into the project, during troubleshooting (if necessary)
- Suitable map (Spotter tiles, Google Earth 5k or site map in JPEG provided by end-user)
- Define alarm zones and actions (camera cueing, filtering, schedule etc)
- Configure all devices
- Make a checklist: test and verify connectivity, actions, status handlers etc

Rule of thumb: when done with preparations, only 4 things remain: install (mount), connect, calibrate and perform PEN-tests.

Step 6: Commissioning

The Commissioning is done prior to the recommended settings originated from the Site Survey document and is more complex in all its tasks. You will document mounting and configuration etc here. The installation of the site is dependent on the Commissioning so the values here are intended to be final. It will also be an approval of the knowledge about the system.

Step 7: Final Phase: Follow on Alarm Review and Tune

Sometime after the commissioning (at least a week or two) should Alarm Review and tuning be done, on-site while the system is monitored, to improve the wanted and unwanted alarms.

2.2. Build your quote

When you have a clear idea about the client's specific requirements regarding areas to be monitored, alarm zones, the amount of cameras, etc it is time to put together a bill of material. We recommend that you begin with creating a desktop design by using MOCK RADARS in NetworkedIO and place them in ideal positions. This will help you to illustrate the approach to meet the client's objectives. Please be aware that this is nothing more than assumptions, it needs to be verified through a site survey later in the process.

Follow these steps to make sure nothing is forgotten regarding the bill of material.

1. Choose suitable sensors (Spotters) for each area to be covered
2. Add a server (we recommend one of 3 available alternatives of NIO-VM)
3. Add licenses for connecting Spotter to NIO (1 license per Spotter)
4. Add licenses for att PTZ-camera (1 license per PTZ)
5. Add power-kit (choose between 1- or 4-channel PoE-kit)
6. Add mount (1 per Spotter)
7. Add suitable SLA-option (Silver/Gold/Platinum)
8. Option: VMS integration (available for Milestone and Genetec)
9. Finally, remember to add an estimated amount of hours for site survey and site commissioning including a follow up regarding false alarm review.

Securify Partner Portal
Please note, as a partner to Securify you have access to our Partner Portal which provides full access to the full SpotterRF assortment, to your company's agreed prices. In the Partner Portal, you can build a quote and push this by clicking at RFQ to Securify for validation. Here you will also find documentation, our ticket system, quotes, orders and much more.
Log in to Securify Partner Portal at www.securify.se

3. Design considerations

3.1. Operator view

The operator should have access to the NIO-interface. If there is VMS-platform the operator should have access to both the VMS and the NIO-interface or an integrated view.

Best practice:
In the VMS the operator should have a multiview with:

- Auto-tracking PTZ-cameras in live view
- Auto-tracking PTZ-cameras in recorded view
- NIO-map interface
- Auto Tracking PTZ should start recording on an action-event from the NIO with 10-30 seconds pre-record and 1-5 minutes post-record.

Deviations should be noted.

3.2. Alarm presentation

Best practice:

- Each alarm from the radar system to be verified by the operator

Deviations should be noted.

How are the alarms from the radar being presented to the operator?
How are the alarms from the radar going to be validated?
Is a monitoring station going to receive alarms from the NIO? How?
What actions will the station take and why?

3.3. Health Monitoring

In each Spotter radar, a number of thresholds can be set. If these thresholds are exceeded, a warning will be triggered and sent to the NIO server.
Best practice:
Set a warning threshold on Yaw, Pitch, and Roll to 6 degrees in the Orientation Monitor section.

In the Signal Health section:
Jamming to 20
Interference to 40
Saturation to 25
RF Return 15 below the Current Status
Chan Return Diff to 5

Note:
The above values might differ depending on the environment, but some Warning threshold should be set.

Best practice:
If the NIO is integrated into another system (that the operator uses) the warnings should be transferred to this system. Use the Status Handlers menu in the NIO.

Best practice:
For each Spotter-radar create a preset in the NIO for a camera that covers where the radar is mounted. Also, create a Status handler in the NIO with the Alert Type for orientation and disconnect. Action uses the preset for the camera covering the radar.
Recommended is also to send a trigger to the VMS to start recording.

3.4. NIO Alarms to VMS

Best practice:

- Should be sent via the network.
- Each alarm should be marked in the timeline in the VMS or in a separate alarm-log.

Deviations should be noted.

3.5. PTZ-priority

Operator vs NIO. The VMS should have priority over the NIO.
If an Axis camera is being used; set up a user in the camera with lower priority than the VMS.

3.6. VMS event to NIO

Is there any need for integration from VMS -> NIO?
Example: enable/disable alarm zone in NIO based on schedule or trigger in VMS

Who is going to configure the VMS and the NIO?

3.7. AI Training

Training the Spotter AI is an important and precise task.

1. Only confirm the correct tracks.
   The tracks must be visually verified and make sure that the confirmed track is the one that has been verified. No guessing!
2. Balance the data points.
   The AI can only classify what it has been trained on. Try to get equally many tracks and the different classifications (Types). On the "AI" tab in the NIO pay attention to "Track Data Point". The aim is that the different types should have roughly the same data points.
3. Use the "Immobile" type for stationary objects.
   For example, swaying trees or masts
4. Do not use the "Unknown" type.
   If the track is unknown it breaks rule #1
5. Train more than one type.
   The AI needs more than one type to be able to give confidence.
6. Pay attention to the AI statistics before and after training.
   The statistics should increase after training. If not; download all config and reset the NIO to default.

3.8. NIO backup

When doing backup of the NIO:

1. Backup all configs:
   Settings (cogwheel) -> About (info) -> "Download All Configs"
2. Download map-packs:
   Settings (cogwheel) -> Maps (globe) -> Map Regions -> "Download All"
3. Download trained AI-models:
   Download [Left Pane] -> "Trained AI Models"

3.9. Network

3.9.1. Physical layer

Since the radars are mounted outdoors it is essential that the physical layer of the network is well built.

- Cat 6 shielded cables.
- Correct grounded cables.
- Surge protection between switch and radar. We recommend the product ED NET 6 cat from vendor Elrond, Swedish manufacturer with deep ESD knowledge [https://elrond.se/produkter/natverksskydd-cat-5-och-cat6-ed-net-6-cat/]

3.9.2. LAN

What subnet will NIO radars, the NIO and the operator workstation be on?

3.9.3. Remote access

Will it be possible to access the systems remotely?
Best practice:

- No ports for incoming traffic should be open (example; RDP, VNC HTTP).
- Remote access has to be made over secure link such as VPN

Deviations should be noted.

3.9.4. IT security

Are there any requirements for IT-security? Example 802.1x has to be used.

3.9.5. Infrastructure

Best practice:
Follow TIA/EIA 568 standard. We recommend that an equipment outlet is installed within 5 meters of each radar. Deviations should be noted.

3.10. PTZ mounting

When using radars from C40 and up, i.e. ranges over 450 meters, leveling of the PTZ-camera is essential. The NIO will in its calculations presume that the camera is in level.
It is recommended that the mounting of the camera enables fine adjustments of the camera. Preferably with a threaded bolt with a nut assembled in such a way that adjustments can be made while the camera is mounted.
If the horizon is present in the camera view it can be used while adjusting the camera.

4. Apportionment of liability

A clear distribution of task responsibilities at an early stage of a project makes it easier to plan the project but is also a way of mitigating risk and lower cost.

4.1. Liability template draft

Liability	Responsible			
	End-user	Integrator	Securify	Spotter
1. Specify requirements	X			
2. Desktop design		X		
3. Site Survey		X		
4. Installation				
a. Structured cabling network infrastructure		X		
i. Cable certification protocol ISO 11801:2002		X		
ii. Outdoor equipment surge protected		X		
b. Spotter equipment		X		
c. Software		X		
d. Network configuration		X		
e. Network security		X		
5. Commissioning				
a. SpotterRF		X		
b. VMS integration		X		
6. Miscellaneous				

a. Radar frequency usage permission application		X		
b.				
c.				
d.				
e.				