SANDIA REPORT
SAND2019-4251
March 2019

Sandia National Laboratories

Portable Intrusion Detection System Alarm Station Operator Interface Improvements

Ann Speed

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

To address Alarm Station operator performance, Portable Intrusion Detection System team gathered information concerning AS operator data needs when assessing alarms. The purpose was to improve the Portable Intrusion Detection System operator interface to ensure that critical information was quickly presented and easily accessible. To gather the data, the team used a Goal Directed Task Analysis approach. The method of analysis was to prepare a set of interview questions, interview selected AS operator experts, conduct the interviews, create a goal/decision/information hierarchy based on information gathered, and then apply the results to the operator interface. In applying the results, the team had to consider not only the Goal Directed Task Analysis -determined information needs of the Alarm Station operator end-user population, but also account for customer requirements and differences in domain. The constraints in implementing all situation awareness recommendations are summarized and initial potential solutions presented.

ACKNOWLEDGEMENTS

Much appreciation to the Portable Intrusion Detection System Team for recognizing the importance of the human element in interface design, and specific thanks to the two Subject Matter Experts for their patience and thoroughness during interviews on Alarm Station operator performance.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

To address Alarm Station (AS) operator performance, the Portable Intrusion Detection System (PIDS) Team gathered information concerning AS operator data needs when assessing alarms. Specifically, the team used a Goal Directed Task Analysis (GDTA) approach (Endsley and Jones, 2012) [1]. This approach aligned the information presented by the alarm control and management system with the information AS operators would need to make effective decisions when assessing whether alarms were real or false.

The GDTA process breaks down an AS operator expert's task into goals, decisions, and information needs. Using this process, interfaces can be improved by ensuring the information most critical for operator decisions is present and easily accessible. This information can also inform future algorithm development so that the analytics performed on incoming data support the operator's information needs, rather than simply being computed regardless of need.

To conduct a GDTA, the goals of the job are identified and, where relevant, are then broken down into sub-goals. For example, in the AS GDTA performed for this project, the highest-level task goal was—*to act as the eyes, ears, triage, and communications center for facility and responding forces*.

Once the goal and sub-goal structure is defined, the team then identifies the decisions needed by the experts to reach those goals. Goals and decisions are different. For example, a sub-goal of the AS GDTA was—*to determine the cause of each system alarm*. One of the underlying decisions the operator must make to reach that goal was—*Is the alarm a planned alarm, an actual nuisance alarm, an actual false alarm, or a threat?* For each decision ascertained, the information needed by the expert to make the decision is identified and listed.

The method of analysis included the following:

- Prepare a set of interview questions
- Interview selected AS operator experts
- Conduct the interviews
- Create a goal/decision/information hierarchy based on information gathered
- Apply the results to the operator interface

In applying the results to the interface, the team had to consider not only the GDTA-determined information needs of the AS operator end-user population, but also account for the customer requirements. The recommendations also had to consider the command center domain, in which the event of most concern involves an adversary actively engaged in trying to occlude their activities/attack from the user of the interface. Thus, the decision the AS operator must make can be a very complex choice involving much uncertainty. The constraints in implementing all Situation Awareness (SA) recommendations are summarized and initial potential solutions presented.

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AS	Alarm Station
C2	Command and Control
DOE	US Department of Energy
FA	False Alarm
FAR	False Alarm Rate
FIFO	First In, First Out
GDTA	Goal Directed Task Analysis
IM	Instant Messaging
IR	Infrared
KAFB	Kirtland Air Force Base
MP	Military Police
NA	Nuisance Alarm
NAR	Nuisance Alarm Rate
NSEW	North-South-East-West
NTS	Nevada Test Site
PA	Public Address system
PIDAS	Perimeter Intrusion and Detection System
PIDS	Portable Intrusion Detection System
POC	Point of Contact
RF	Radio Frequency
SA	Situation Awareness
SAS	Secondary Alarm Station
SCC	Secure Command Center
SCI	Sensitive Compartmented Information
SOP	Standard Operating Procedure
SPO	Security Police Officer
SW	Southwest
Y-12	Y-12 National Security Complex

This page left blank

1. INTRODUCTION

To address Alarm Station (AS) operator performance, the Portable Intrusion Detection System (PIDS) Team gathered information concerning AS operator data needs when assessing alarms. Specifically, the team used a goal directed task analysis (GDTA) approach (Endsley and Jones, 2012) [1]. This approach was implemented to align the information presented by an alarm control and management system with the information AS operators would need to make effective decisions when assessing whether alarms were real or false.

The GDTA process breaks down an expert's task into goals, decisions, and information needs. Using this process, interfaces can be improved by ensuring the information most critical for operator decisions is present and easily accessible. This information can also inform future algorithm development so that the analytics performed on incoming data provide support that is useful to the operator's goal, rather than simply being computed regardless of operator need.

To conduct a GDTA, the goals of the job are identified and, where relevant, are then broken down into sub-goals. For example, in the AS GDTA performed for this project, the highest-level task goal on which the team focused was—*to act as the eyes, ears, triage, and communications center for facility and responding forces*.

Once the goal and sub-goal structure was defined, the team identified the decisions that the experts needed to make in order to reach those goals. Note that goals and decisions are different. For example, a sub-goal of the AS GDTA was—*to determine the cause of each system alarm.* One of the underlying decisions the operator must make to reach that goal was—*Is the alarm a planned alarm, an actual nuisance alarm, an actual false alarm, or a threat?* For each decision ascertained, the information necessary for an expert to make the decision was identified and listed.

Generally, *yes/no* questions are not considered for inclusion in a GDTA because those decisions are typically straightforward. However, in this case, the decision about whether an alarm is real, false or nuisance is a complex decision that requires AS operators to use a variety of disparate pieces of information. The following sections provide details about the GDTA performed and the results of that analysis.

This page left blank

2. ANALYSIS METHOD

The method of analysis included the following:

- Prepare a set of interview questions
- Interview selected AS operator experts
- Conduct the interviews
- Create a goal/decision/information hierarchy based on information gathered
- Apply the results to the operator interface

2.1. Identify AS Operator Experts

The team interviewed two experts for this GDTA.

- The first expert (Expert 1) had served as an AS operator at Sandia when it was a facility that allowed alarm assessment using cameras. Subsequently, this expert became a trainer in the area of physical protection.
- The second expert (Expert 2) also served as a Sandia AS operator full time for a year. His positions in the AS were both as an operator and a supervisor, including four months filling in at the AS for a facility that allowed alarm assessment using cameras during his tenure. Prior to employment at Sandia, he worked for private security firms and for large companies with alarm systems on their facilities.

2.2. Prepare for Interviews

In this analysis, the team first collected and reviewed several documents relevant to the AS operator's job, including standard operating procedures (SOPs) and General Orders. Often these documents contained information about other physical site security duties for stations other than the AS—in these cases, only those sections specific to the AS were reviewed. From these documents, an initial list of 32 questions was created that focused on the information for the GDTA.

2.3. Conduct Interviews

Expert 1 was interviewed three times and Expert 2 was interviewed one time. Expert 2 was interviewed only one time because most of his experience was not at a facility that allowed camera-based alarm assessment, so the SOPs under which he was operating did not match those anticipated for the current system once deployed.

Each interview was recorded and the interviewer transcribed the expert's responses during the discussion. All interviews began with the interviewer reminding the expert that the session was being recorded. The initial interview with each expert also included a brief description of the kind of

information being sought—specifically, goals, decisions, and information—needed to support those decisions.

The prepared questions were used during each interview; however, the order in which those questions were asked was not identical across experts. Also, as appropriate, additional questions that came up during the discussion were posed to each expert to clarify a statement. In this way, the conversations diverged from both the order of the prepared questions and from one another. However, both experts were asked many of the same questions and the responses from one expert motivated questions for the other.

3. ANALYZING THE DATA

The information gathered during the interviews was used to create a goal/decision/information hierarchy. Questions used to clarify the hierarchy were directed to the two experts as they came up. Once an initial edit of the entire hierarchy was complete, the two experts and the interviewer met again to go over the hierarchy and to receive feedback and corrections from the experts. The result is a first complete draft of the hierarchy and presented in Figure 1 through Figure 4.

The information needs for the two experts form a lengthy list, as is evident in the goal hierarchy. Thus, to better target updates to the interface, the team asked the experts to rate the importance of each piece of information in the interface on a scale from 1 to 5, where 1 was critical and 5 was not necessary. Expert 1 rated 78 out of 85 goal-linked pieces of information as either 1 or 2 in importance for inclusion in the interface. Expert 2 rated 55 goal-linked pieces of information as either 1 or 2 in importance for inclusion in the interface. Thus, to reduce that number to something feasible for inclusion in the next version of the interface, both experts were asked to choose their top 15 most critical pieces of information for inclusion in the interface (no ties were allowed). Those results are in Table 1 where items in bold font were ranked by both experts in their top 15.

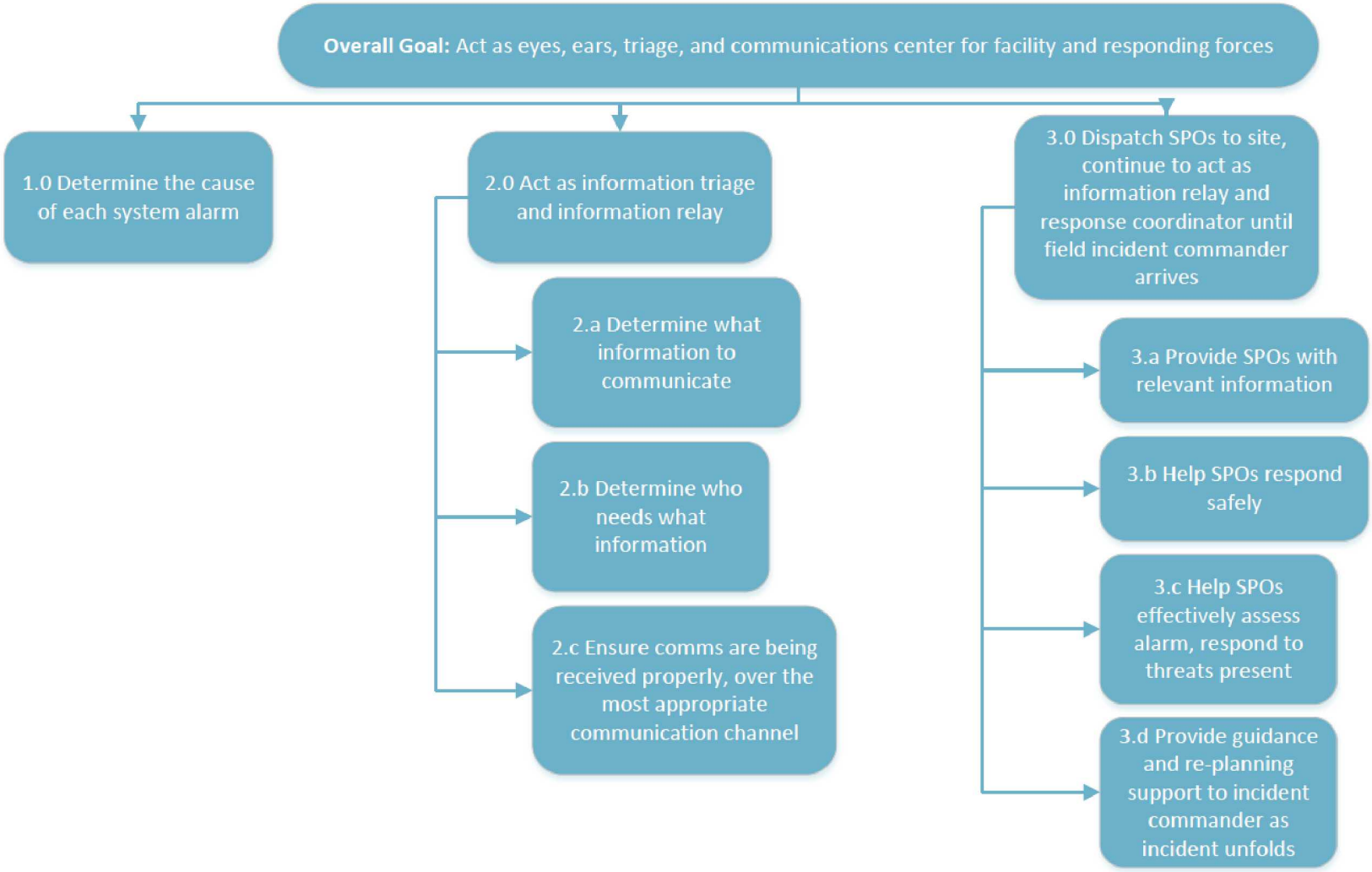

Figure 1. Top Level Goal Structure for AS Operator Alarm Resolution and Response
(*SPO stands for security police officer*)

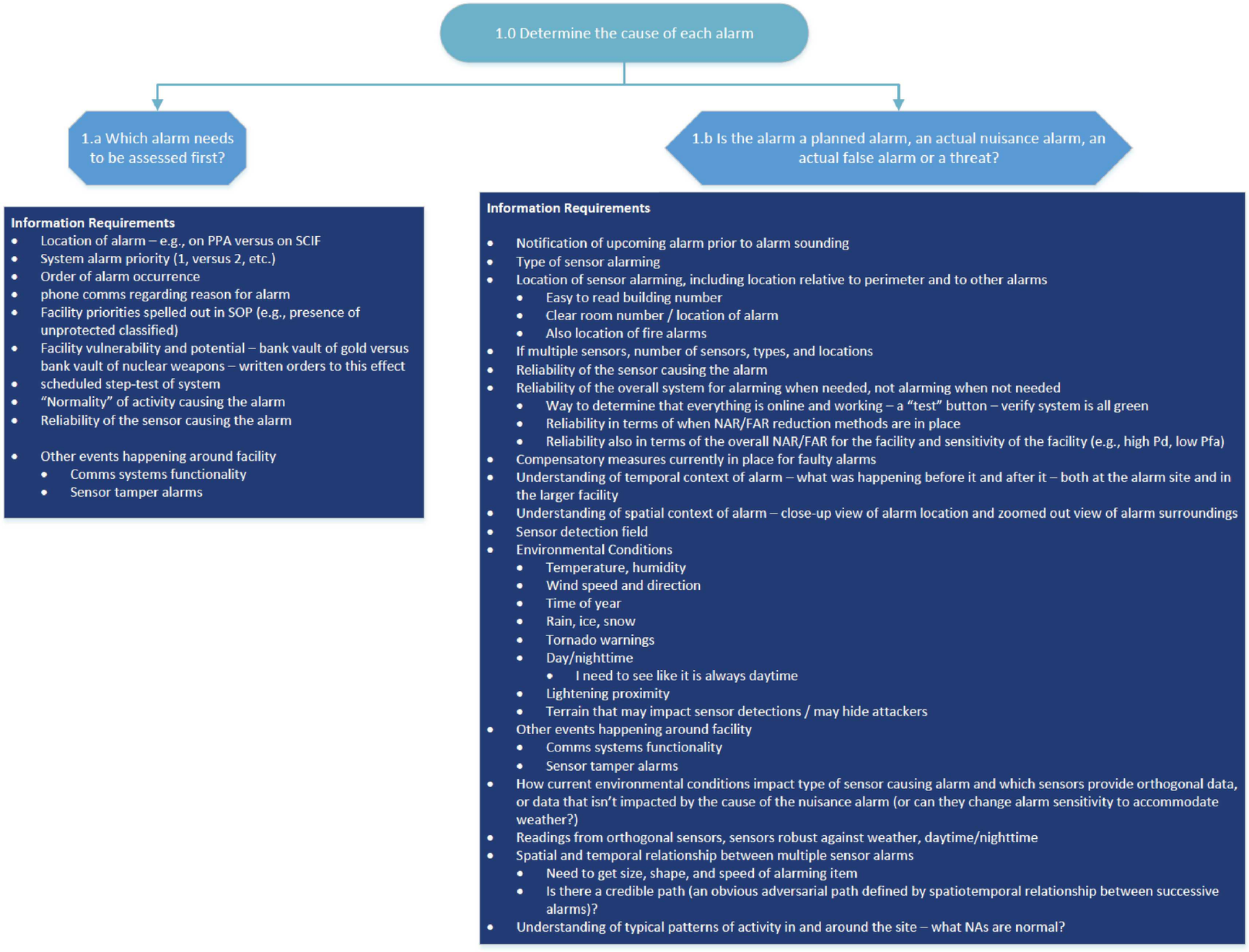

Figure 2. Decisions and Information Requirements for Sub-goal—*Determine the cause of each alarm*

This page left blank

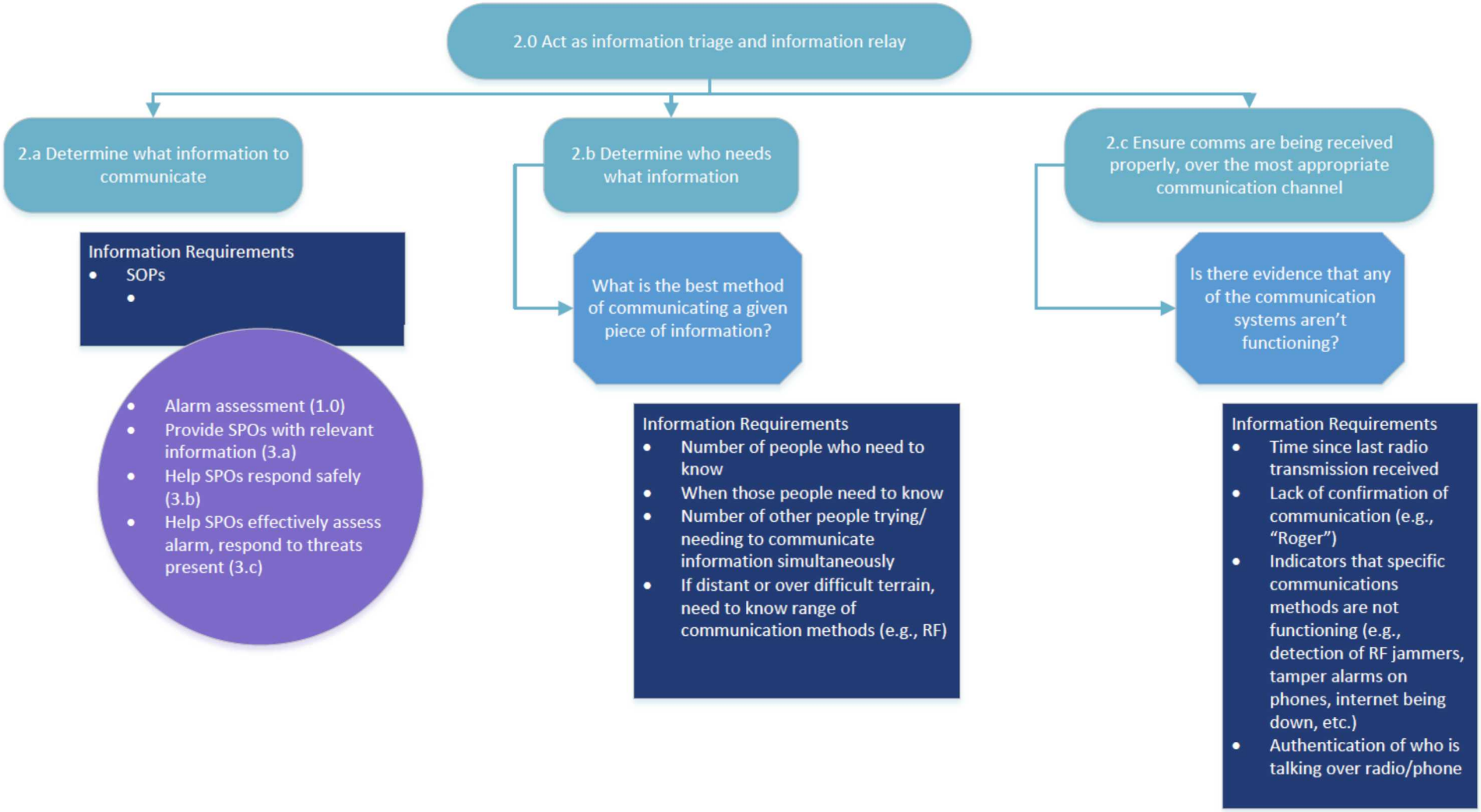

Figure 3. Sub-sub goals, Decisions and Information Requirements for the Sub-goal—*Act as information triage and information relay*

This page left blank

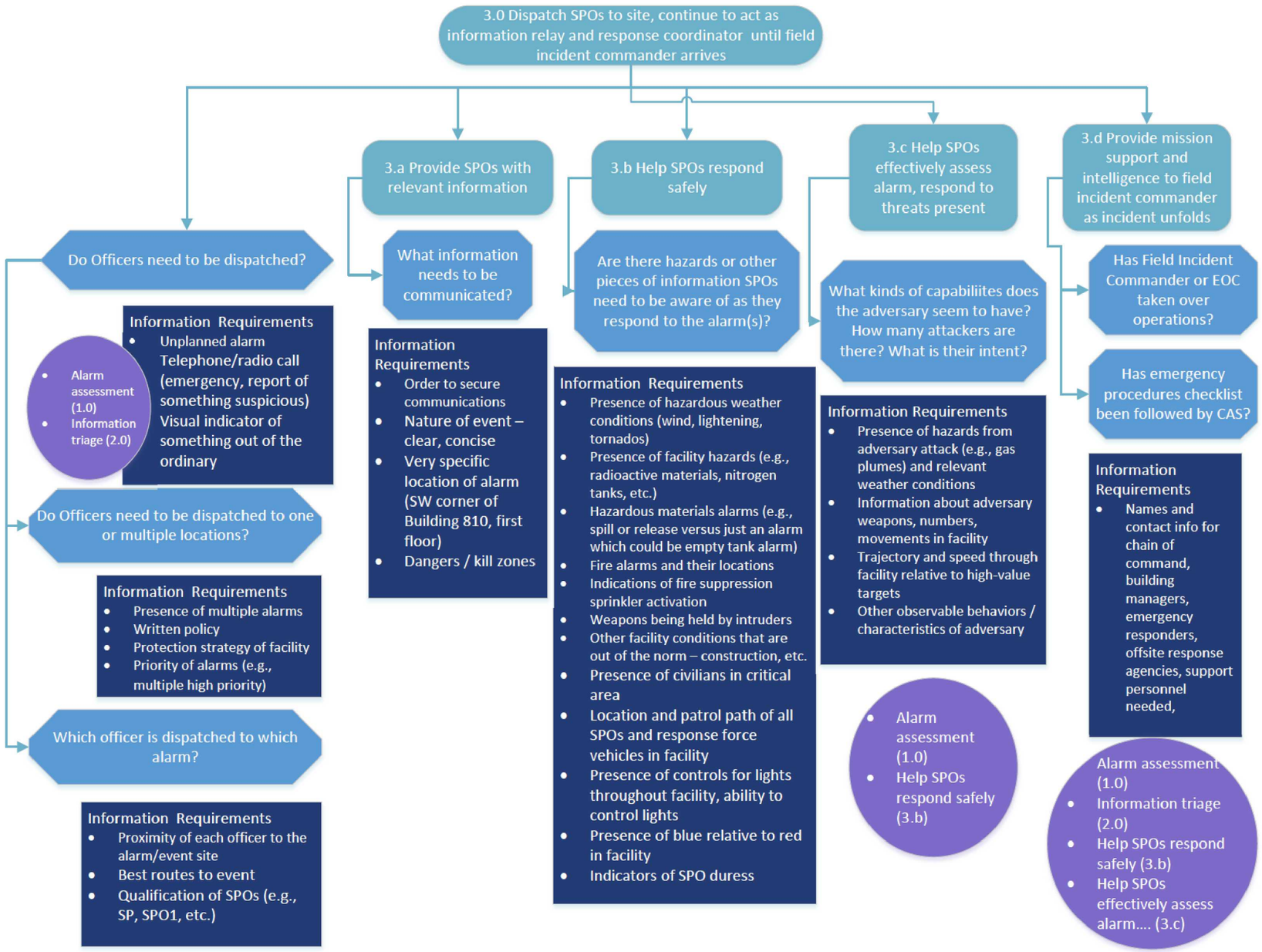

Figure 4. Sub-sub Goals, Decisions, and Information Requirements for Sub-goal—*Dispatch SPOs to site, continue to act as information relay and response coordinator until field incident commander arrives*

This page left blank

Table 1. Top 15 Most Important Information to Include in Interface

Importance Rank	Expert 1	Expert 2
1	Indication that the alarm is unplanned	**Very specific location of alarm (SW corner of Building 2, first floor)***
2	**Indicators of SPO duress***	Type of sensor alarming
3	Understanding of temporal context of alarm—what was happening before it and after it—both at the alarm site and in the larger facility	Sensor detection field
4	Understanding of spatial context of alarm —close-up view of alarm location and zoomed out view of alarm surroundings	Phone/radio communications regarding reason for alarm
5	**Very specific location of alarm (SW corner of Building 2, first floor)**	**Priority of alarms (e.g., multiple high priority)**
6	Presence of multiple alarms	**Nature of event—clear, concise**
7	**Nature of event—clear, concise**	Order of alarm occurrence
8	**Indicators that specific communications methods are not functioning**	**Indicators that specific communications methods are not functioning**
9	**Location of sensor alarming, including location relative to perimeter and to other alarms and type of facility**	**Indicators of SPO duress**
10	If multiple sensors are alarming, number of sensors, types, and locations	Environmental conditions
11	Dangers/kill zones	Location and patrol path of all SPOs and response force vehicles in facility
12	Proximity of each officer to the alarm/event site	**Location of sensor alarming, including location relative to perimeter and to other alarms and type of facility**
13	**Priority of alarms (e.g., multiple high priority)**	Authentication of who is talking over radio/phone
14	Best routes to event	Fire alarms and their locations
15	Visual indicator of something out of the ordinary	Hazardous materials alarms (e.g., spill or release versus just an alarm that could be empty tank alarm)

NOTE: Items in bold font were ranked by both experts in their top 15 selections.

This page left blank

4. APPLYING THE RESULTS TO THE JIGSAW INTERFACE

4.1. Summary of Constraints

Once the list was formed, the next steps in the development of recommendations for upgrades to the interface were to examine, in detail, the various principles for designing S)-enabling interfaces (Endsley & Jones, 2012) [1] and then to mesh these principles with the information needs of the users and the requirements of the customer for the users of the system. That is, there are specific requirements users must meet beyond the constraints of the goal hierarchy and principles for SA-oriented design—such as the requirement to acknowledge and classify the cause of every individual alarm. This requirement, as an example, contradicts some of the principles for SA-oriented design, so recommendations for the interface must account for both the principles and behavioral requirements.

Endsley and Jones (2012) [1] recommend that when adjusting interfaces to enhance SA, consideration should be given to methods for supporting Level 2 and Level 3 SA. In this case, the interface was required to support AS operators' abilities to determine (a) whether the facility was under attack (SA Level 2), especially in the face of multiple alarms occurring in a short period of time, and (b) when possible, the goal of the attack (SA Level 3).

To accomplish support for both Level 2 and Level 3 SA, the team had to consider not only the GDTA-determined information needs of the AS operator end-user population, but also account for the customer requirements for the system per the SOPs under which the AS operators must function.

To illustrate, one example of such a requirement is that the AS operator must acknowledge every alarm that the system generates. The team performed a quick anecdotal experiment to test the ability of the current interface to support this requirement in the event of a large number of alarms occurring in a short period of time (which will likely be the case if the facility comes under attack). The team engaged the lead developer of the interface, asking him to interact with the interface the way a AS operator might, as another engineer activated several alarms on various sensors in rapid succession (i.e., approximately one every five seconds). He was rapidly overwhelmed trying to acknowledge each alarm—in part because of the rate at which sensors were alarming, and in part because of the way the interface was set up to enable the required acknowledgements.

Another issue one must try to account for when developing support for Level 2 and Level 3 SA is that this domain is somewhat different from those Endsley and colleagues usually work with in one critical way. In this particular domain, the event one is most concerned with involves an adversary actively engaged in trying to occlude their activities/attack from the user of the interface. Thus, the decision the AS operator must make regarding whether an alarm, or group of alarms, is nuisance/false or is indicative of a real attack can be a very complex decision involving much uncertainty. Further, these events (i.e., real attacks) are exceedingly rare. Designing a system that supports SA when those events occur, while also supporting SA the vast majority of the time when

nothing malicious is happening, presents a significant challenge. The interface must enable the AS operator to understand when individual sensors are malfunctioning (false alarms) and when they are alarming because of environmental conditions (nuisance alarms, e.g., rain, wind, wild animals) without inducing an overwhelmingly strong prevalence effect (e.g., unclassified Y-12 report; Wolfe, Horowitz, et al., 2007)[2] in which operators automatically turn off alarms without properly adjudicating them. The interface and underlying algorithms must also help the AS operator determine when alarms are occurring due only to environmental conditions and when an adversary is exploiting the environmental noise, such as wind, in order to launch an attack.

Underlying algorithms can help with this problem if they are able to provide higher-level interpretations of alarms without harming the operator's contextual understanding of the situation. However, those algorithms must also be able to present appropriate confidence and uncertainty information to the user in a way that is easy for the operator to understand correctly. This same interface (and underlying algorithms) must also be able to provide rapid, accurate assessments of alarms during an attack. It should not overwhelm the AS operator in the details of adjudicating individual alarms as additional alarms of increasingly high priority pile up in the queue. During any pile up of alarms and lack of assessment, potential attackers could possibly make their way through a facility. This could lead to SPOs being engaged on the ground who are not as well-informed as they could be, had the AS operator received better overall SA at the onslaught.

4.2. The Initial Solution

An initial approach to the problem of helping the AS operator develop Level 2 SA in the face of a rapidly evolving attack scenario was to change the method by which they acknowledge and triage alarms. As alluded to, the original process for acknowledging individual alarms involved drilling down into a number of fairly detailed menus using pull-down menus and check boxes to indicate the type of each alarm (nuisance, false, true) and the cause, if known (e.g., wind, animal, intruder). Because the customer required this process of acknowledging each alarm, the team suggested a new method of triage. In this method, one AS operator adjudicates each alarm via a KEEP or DEFER button.

- The KEEP button sends the alarm information to a second AS operator whose job it is to develop an overall picture of the emerging status of the facility (i.e., Level 2 SA)
- The DEFER button relegates that alarm to a queue for consideration at a later time, when there is time to enter the details regarding the alarm type and cause

In this way, every alarm is acknowledged and eventually characterized, but the AS operators can defer these activities until after a critical situation is over.

A second notion was a method for displaying spatiotemporal information on a shared screen. As shown in Figure 4, the AS will include a shared wall-sized display of the facility map, along with critical videos of intruders. In addition, the order of alarms will be displayed via dynamic coloration to convey time since alarm and alarms will be linked to their physical location in the facility. Still

images can be displayed if they provide critical information to determine whether the intruders are benign (e.g., a deer).

The example in Figure 5 shows the shared display with triaged video and spatiotemporal alarms displayed at the front of the room. Individual AS operators would all have a variant of that shared display on their individual workstations, with different functionality on the other monitor based on their function in the AS. In Figure 5, the operator on the far left is triaging video of individual alarms, using the KEEP/DEFER approach. The operator in the middle is primarily responsible for forming Level 2 SA of the situation, using the triaged video. The operator on the far right has the same shared display as well as the list of contacts to be notified of the event.

Note that the concept of the shared display has not been fully developed or implemented in the software. Further, the suggestions presented here have not been compared to the customer requirements. Ensuring these suggestions and those requirements are consistent is an important step.

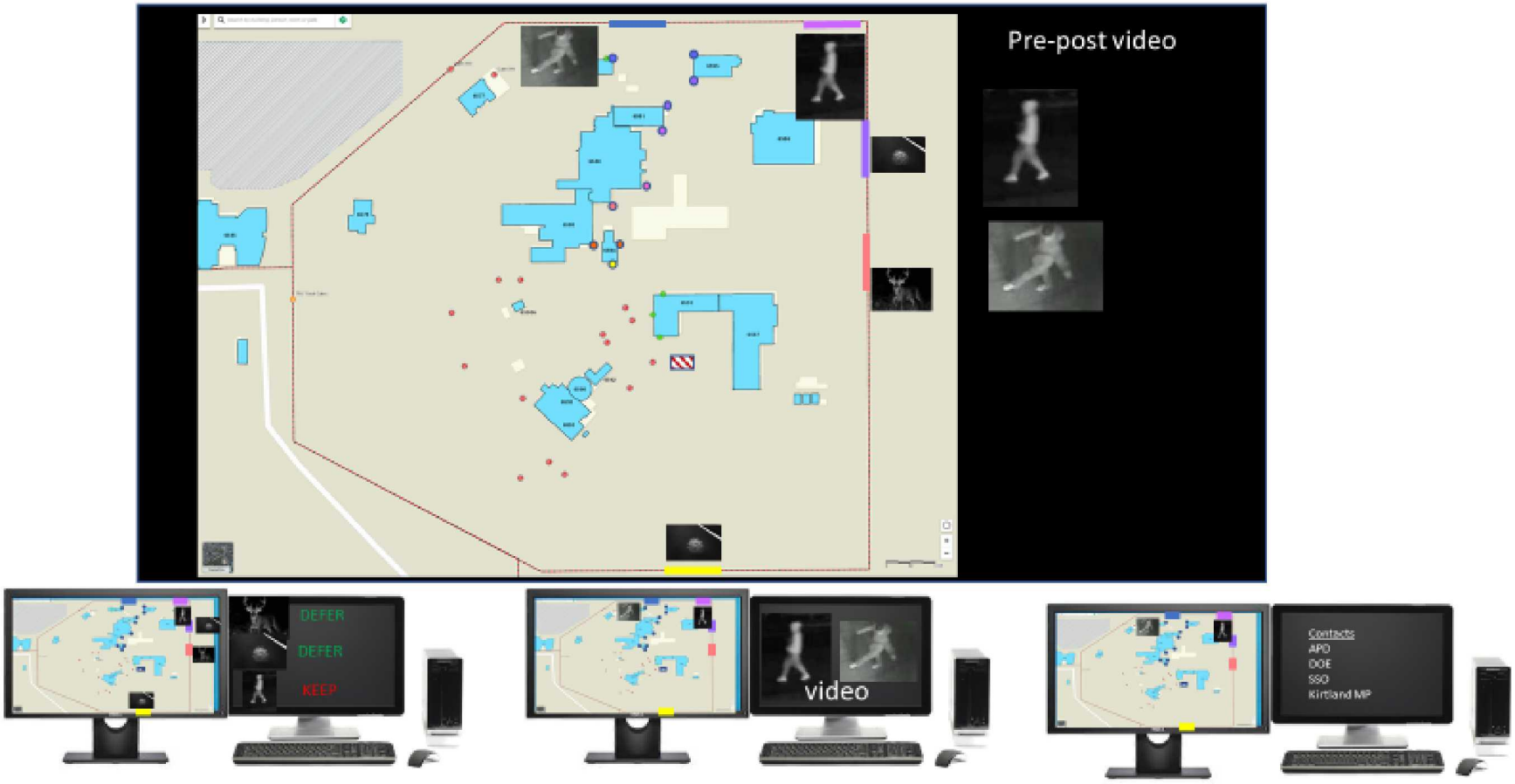

Figure 5. Notional Setup of an Alarm Station

REFERENCES

[1] Endsley, M. R., and D.G. Jones (2012). *Designing for situation awareness: An approach to human-centered design* (2nd ed.). London: Taylor & Francis.

[2] Wolfe, J.M., Horowitz, T.S., Van Wert, M.J., Kenner, N.M., Place, S.S., & Kibbi, N. (2007). Low target prevalence is a stubborn source of errors in visual search tasks. Journal of Experimental Psychology: General, 136, 623-638.

This page left blank

DISTRIBUTION

Name	Org.	Sandia Email Address
John Feddema	1460	jtfedde@sandia.gov
Ann Speed	1462	aespeed@sandia.gov
John Wagner	1462	jswagne@sandia.gov
Dan Barton	6520	bartondl@sandia.gov
Gabe Birch	6524	gcbirch@sandia.gov
Camron Kouhestani	6524	cgkouhe@sandia.gov
Chad Monthan	6524	cwmonth@sandia.gov
Kristopher Klingler	6531	krkling@sandia.gov
Bill Prentice	6531	wjprent@sandia.gov
Steve Hill	6621	skhill@sandia.gov
Greg Baum	6835	gabaum@sandia.gov
Dale vanDongen	9412	dtvando@sandia.gov
Steve Jordan	10756	sgjorda@sandia.gov
Technical Library	9536	libref@sandia.gov
Legal Technology Transfer Center	11500	

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.