



Vol. 44, No. 6 • Nov.-Dec. 2008

Tech Corner

 Download printable
PDF of this page

Detecting Precrime in the Here and Now

by Sherry R. Deatrick

Pages 1 | 2

Does anyone remember the science fiction film *Minority Report*?

It told the story of a dystopian and technocratic future, in which a sophisticated computer system enabled law enforcement to detect potential criminal activity *before* it happens. In the film, this effort was spearheaded by the "Federal Department of Precrime" in Washington, DC.

Well, as so often is the case, life has imitated art — with chilling results. The U.S. Department of Homeland Security (DHS) has cooked up something with the sinister name of MALINTENT, a computer system that can literally read a human being's mind and thoughts. That is, if the hype is to be believed.

What is this MALINTENT? It's a program that claims to be able to monitor and analyze a person's facial features and physical cues to evaluate their potential intent to do harm to others. A network of MALINTENT sensors will theoretically be put into place at airports, as well as large event venues like sports stadiums and shopping malls, etc. Then, as the sales pitch has it, anyone who thinks bad thoughts will instantly be detected and can presumably be tackled by security. The system does what it does without actually physically contacting a person — it operates remotely and supposedly has the ability to accurately read your heart rate and body temperature, and then make judgments regarding whether you're a potential criminal based on that data.

Even without considering the terrifyingly Orwellian implications of such a device, the legal ramifications are sure to keep attorneys busy for decades to come. The public safety issues are numerous, since it's safe to say that MALINTENT cannot possibly be 100 percent foolproof, and the project could end up being more of a menace than a boon to public safety and personal freedoms.

Personally, I think the idea that a computer sensor system can remotely predict a person's malicious intent via bodily cues is preposterous. There are many types of humans with different temperaments, and it's a statistical certainty that terrorists must run the gamut from the shifty and twitchy sort, to the icy calm, cool and collected kind. The advance buzz being generated about MALINTENT's mind-reading and personality-assessing abilities seemingly describes a product that sounds like something straight out of L. Ron Hubbard.

According to a recent report on Fox News Network, Homeland Security put Project MALINTENT to a field test at a technology conference somewhere in Maryland by turning the experimental device on more than 100 "mostly unwitting" human subjects. Now, that alone should be enough to start ringing alarm bells — there's clearly great potential for public safety to be jeopardized by such a device that purports to be protecting that safety. The Fox News story stated that MALINTENT has met "rigorous safety standards to ensure the screening would not cause any physical or emotional harm," but the details of just what these rigorous safety measures are have not, to my knowledge, been fully disclosed. It certainly sounds as if the subjects are being placed in an electromagnetic field greater than that of the everyday store security system or cell phone radiation.

Other questions that haven't been resolved include:

System Safety Training

offered by A-P-T Research, Inc.



Safety
Engineering
and Analysis
Center
4950 Research Drive
Huntsville, AL 35895
www.apr-research.com

Principles of System Safety Engineering

Elements of a System Safety Program

Concepts in Risk Management

Initiating the System Safety Program

Working with the Risk Assessment Matrix

Preliminary Hazard Analysis

Failure Mode and Effects Analysis

Fault Tree Analysis

Event Tree Analysis

Reviewing SS Analyses

Risk Acceptance

Course Instructors: Sid Smith, Tom DeLong

When: See our calendar at www.apr-research.com

Where: APT's Safety Engineering & Analysis Center

Cost: \$1495

Technical Information:
Sid Smith, (256) 327-3397,
ssmith@apr-research.com

Registration Information:
(256) 327-3399,
training@apr-research.com



President's Message

From the Editor's Desk

Outside the Lines

In the Spotlight:

A Tribute to Trevor Kletz

Making Safety-Related Decisions

Gains from Losses:

System Safety Commentary on Accidents and Other Events

Special:

26th International System Safety Conference: Innovations and Legacy

Tech Corner

Chapter News

Mark Your Calendar

About this Journal

Classifieds

Advertising in eJSS

Contact Us

Puzzle

- Who determines the accuracy of a MALINTENT reading when the computer says you're a terrorist?
- How can someone be detained or arrested just because a computer program says you look like you're thinking bad thoughts?
- How can any of this stand up to scrutiny in a court of law?
- Who will have access to the personal data about your thoughts and medical readouts that the program gleans? (They claim the data will not be stored.)
- What oversight abilities will be in place to make sure the technology is not misused for personal gain and/or mischief?

The MALINTENT information is decoded and interpreted by a remote team in a mobile unit, referred to as the "Future Attribute Screening Technology" (FAST) team. Future new technologies in the works for FAST include remote pheromone analysis and eye-scanning identification from a distance, all without the subject's knowledge. This, too, was something used as a plot device in the spooky *Minority Report* film; it would appear that the most terrifying and threatening ideas that sci-fi minds like Philip K. Dick's can conceive of are precisely the same ideas that DHS minds find exciting.

[next page »](#)

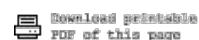
Copyright © 2008 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.



Vol. 44, No. 6 • Nov.-Dec. 2008

Focus

Detecting Precrime in the Here and Now



President's Message

From the Editor's Desk

Outside the Lines

In the Spotlight:

A Tribute to Trevor Kletz

Making Safety-Related Decisions

Gains from Losses:

System Safety Commentary on Accidents and Other Events

Special:

26th International System Safety Conference: Innovations and Legacy

Tech Corner

Chapter News

Mark Your Calendar

About this Journal

Classifieds

Advertising in eJSS

Contact Us

Puzzle

by Sherry R. Deatrick

Pages 1 | 2

Similar DHS Initiatives:

DHS Science and Technology Directorate (S&T) Human Factors Division

Motivation and Intent Program

Violent Intent Modeling and Simulation Project

Project Overview: The S&T Directorate Human Factors Behavior Sciences Division Violent Intent Modeling and Simulation project develops intelligence analysis frameworks, including extraction of terrorist intention signatures, systematic estimation of future terrorist behavior based on social and behavioral sciences, and modeling and simulations of future terrorist behavior influences. It identifies leading-edge social science modeling and simulation technologies and advances social science modeling and data fusion capabilities in such areas as hybrids of neural nets, structural equations, genetic algorithms, social networks, etc.

Suspicious Behavior Detection Program

Hostile Intent Detection — Validation Project

Project Overview: Validation project provides cross-cultural validation of behavioral indicators employed by DHS's operational components to screen passengers at air, land and maritime ports. The project will integrate these validated behavioral indicators into the screening curriculum of each component's existing training program.

Hostile Intent Detection — Automated Prototype Project

Project Overview: Automated Prototype project demonstrates real-time automated intent detection using non-invasive and culturally neutral behavioral indicators. S&T will transition the automated hostile intent prototype to the Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement.

Hostile Intent Detection — Training & Simulation Project

Project Overview: Training and Simulation project develops computer-based simulation to train behavior-based, stand-off detection for future hostile intent using indicators from the interactive screening environment (Hostile Intent Detection — Automated Prototype) and the observational environment (Hostile Intent Detection — Validation) to support screening and interviewing interactions at air, land and maritime portals.

Insider Threat Detection Project

Project Overview: The S&T Directorate Human Factors Behavior Sciences Division Insider Threat Detection project will detect insider behavior that is likely to present or lead to a threat to critical infrastructure using behavioral indicators. DHS will collaborate with other U.S. agencies and international partners to move beyond the current focus on responses to accomplished hostile insider acts, and begin developing a greater capacity to deter and detect insider threats before substantial harm has been done. The immediate operational goal is to produce new and better tools to identify behavior patterns and characteristics before, during and after employment that are associated with insider threats.



27th International System Safety Conference

Aug. 3-7, 2009
Huntsville, Alabama

Call For Papers

Jan 31	Peer Review Paper Submission
Feb 28	Acceptance Notification
May 16	Peer Review Paper Presentation Slides
Jan 16	Forum Paper Abstract Submission
Feb 16	Acceptance Notification
Mar 16	Forum Paper Submission (draft)
April 16	Forum Paper Submission (final) w/ Publication Release Form
May 16	Peer Review Paper Presentation Slides (draft)
June 16	Peer Review Paper Presentation Slides (Final)
Mar 31	Tutorial/Workshop Abstract Submission
June 1	Peer Review Paper Presentation Slides (Final)

For more information about the conference and submissions, visit www.issc2009.org

— Source: http://www.dhs.gov/xres/programs/gc_1218480185439.shtm

« previous page

Copyright © 2008 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.