Assessing, Reporting, and Eliminating Error-Based Security Incidents

Daniel J. Pond
Los Alamos National Laboratory

Shannon Mace
Frank L. Greitzer
Pacific Northwest National Laboratory

LA-UR-05-2234

Background

- The number of security incidents--although low relative to incident "opportunities" and varying year to year--remains unacceptably high and well short of "zero."

- Traditional "corrective actions"—discipline, retraining, stand-downs—have failed to reliably or appreciably reduce recurrence or overall incident rates.

- LANL and DOE-SO have recognized that failure to understand what led to an incident undermines the ability to develop effective corrective actions and to prevent recurrences.

Key Themes

- If you don't know why something went wrong, you have no basis to prevent it happening again. (ESTHER, 2005)
- "Human error. . . is systematically connected to features of peoples' tools, tasks and operating environment." (Dekker, 2002)
- If you only have a hammer, every problem looks like a nail. (ESTHER, 2005)
- "…when the purpose of an accident investigation is to design a prevention program, people tend to make external, system-focused causal attributions, When the purpose is to assign responsibility and blame, people tend to make internal, personal attributions." (Colligan & Cohen, 2004)
- In one circumstance an error can lead to an accident; in another circumstance, the same error can lead to a security incident. (ESTHER, 2005)

Human Error: A Perspective on “Cause”

Human Error Contribution to Accidents (from Hollnagel, 1993)

- Aircraft maintenance 65%
- Air transport operations 75%
- Nuclear power plants 52%

Medical Errors

- 98,000 hospitalized Americans die and another one million are injured from preventable medical errors. This is higher than rates for cancer, traffic accidents, or AIDS. (Institute of Medicine, 2000)
- Reports in July 2004 have re-stated this to “as many as” 195,000 deaths (HealthGrades Inc.)
- The rates of preventable medical errors are improving only at VA hospitals, which have embraced risk assessment and mitigation program such as those used in the aviation industry. (Washington Post, 11/30/02)

Contributors to "Preventable Medical Errors"

Institute of Medicine, 2000

- Fatigue
- Inexperience / Insufficient training
- Inadequate supervision
- Insufficient time to check work
- Increased demands
- Inadequate data = inability to "learn lessons"
- Unclear instructions
- Anxiety over calling superior for guidance

"Human Error"

Pilot Error Blamed for Helicopter Crash

(Baltimore Sun, July 2, 1988)

Paragraph 1:

"Pilot error most likely caused the collision of two Army helicopters that killed 17 soldiers during night training at Ft. Campbell, KY…"

Paragraph 2:

"'Pilot error, to wit, a reasonable mistake in judgment, is the most probable explanation for the cause of this accident,' the Army report said."

“System-Induced Pilot Error”

Paragraph 4:

“The report, however, cited other factors, including exterior and interior design features…limited pilot training…[and] lack of lighting on the helicopters.”

Pilot Error Blamed for Helicopter Crash
(Baltimore Sun, July 2, 1988)

"System-Induced Human Error"

elpasotimes.com news

elpasotimes.com news

507th 'fought hard'

Official report finds 'acute fatigue, isolation, harsh environment contributed to deaths in ambush

Laura Cruz
El Paso Times

The U.S. Army acknowledges in its in
Maintenance Company that huma
Freedom contributed to the de
seven more, a 15-page re

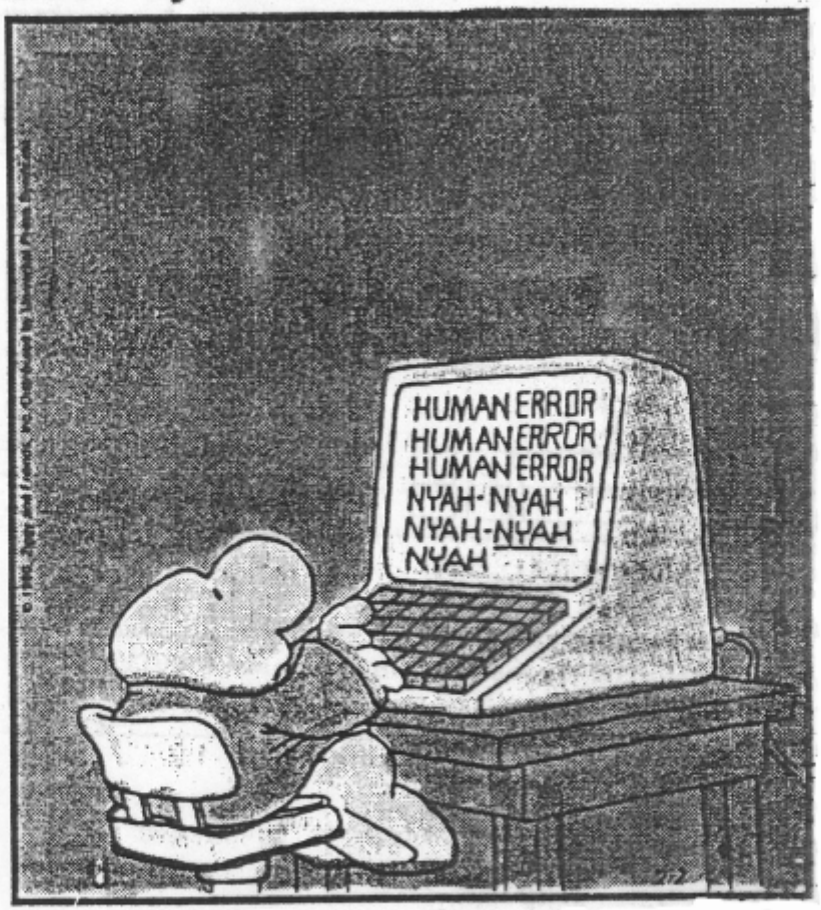
"The U.S. Army acknowledges. . . that human error, fatigue, and the fast pace . . . contributed to the death of nine Fort Bliss soldiers, two others and the capture of seven more . . ."

" . . . [507th] found itself in a desperate situation . . . a navigational error caused by the combined effects of the operational pace, acute fatigue, isolation and the harsh environmental conditions . . .they had trouble with their weapons jamming, partly because they were not properly maintained."

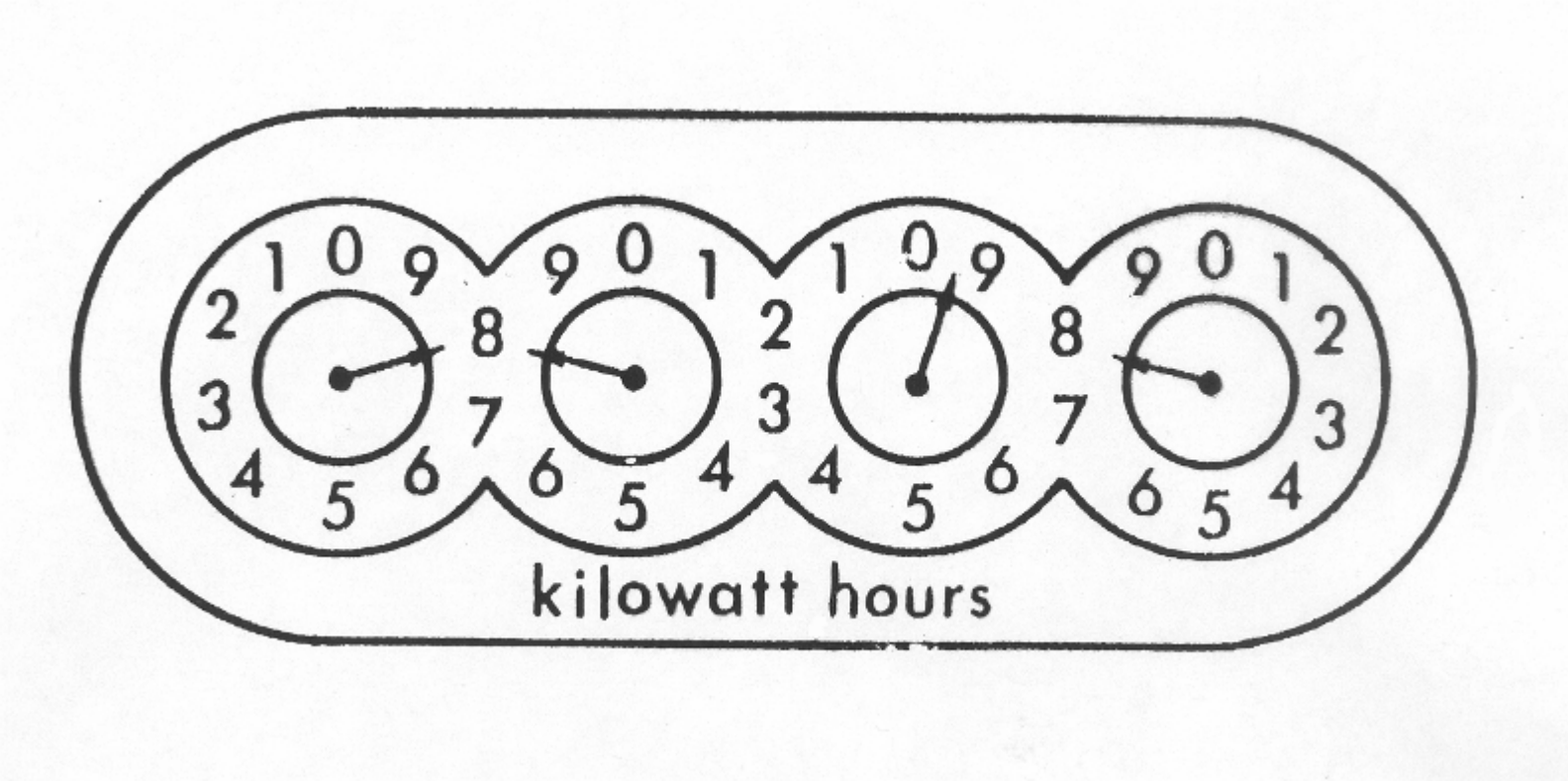
Laura Cruz,
El Paso Times

" . . . [they had] little rest and limited communications . . . the intersection was supposed to have been staffed by soldiers who would direct traffic, but . . . it had not been formally staffed."

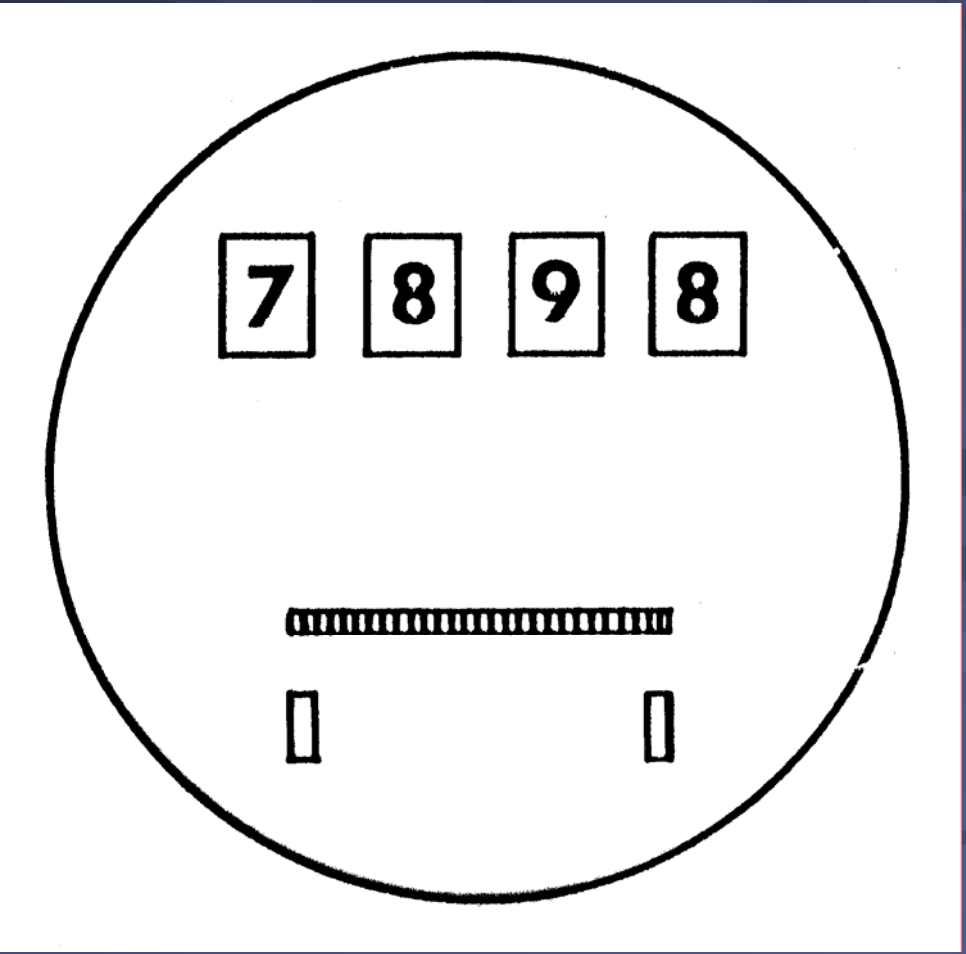
ZIGGY by Tom Wilson



Design Contributors to Error I



Test I: Correct Answer (?)



Air Force: Pilot error led to school strafing

Report says poorly-designed controls contributed to 'mistake'

CNN.com

WASHINGTON (AP) -- An Air National Guard pilot who fired on a New Jersey school during a training exercise was to blame for the incident, but poorly designed controls in the F-16 also played a role,

The report, obtained by The Associated Press, also disclosed that there have been three other incidents fired during nighttime strafing missions. It did not say where and when the other incidents occurred, but no one was hurt.

"An Air National Guard pilot who fired on a New Jersey school during a training exercise was to blame for the incident, but poorly designed controls in the F-16 also played a role . . ."

"…there have been three other incidents this year in which an F-16 pilot unintentionally fired during nighttime strafing missions . . . the report called the incident 'an unfortunate and unintentional mistake.'"

uard, based at Andrews Air Force Base in
taken, and whether any retraining is necessary.

the incident until meeting with residents Friday

Balzano, referred to in the report as the "mishap pilot," or MP, was verifying his aircraft position in relation to his intended ground targets on the Warren Grove Gunnery Range in southern New Jersey, 17 miles northeast of Atlantic City. The school is about four miles from the range.

"Unfortunately, the M
the aircraft gun's disc

fire. The MP immediately realized his error when

Balzano was on a nig
cautioned not to use

on was held before the mission and Balzano was
eport said.

However, shortly afte
ammunition. Eight of
others scuffed the as

d the trigge
s. At least

Balzano immediately

d to Andre

The range reopened
officials shut it down.

sed until t

"In an F-16, the same trigger is used to produce a laser marker to focus on a target and to fire the gun . . . [the pilot's] commander will determine if any punitive or administrative action should be taken, and whether any retraining is necessary."

"A briefing session before the mission and [the pilot] was cautioned not to use his laser marker with the . . .gun mode selected and . . . armed."

Copyright 2004 The

cast, rewritten, or redistributed.

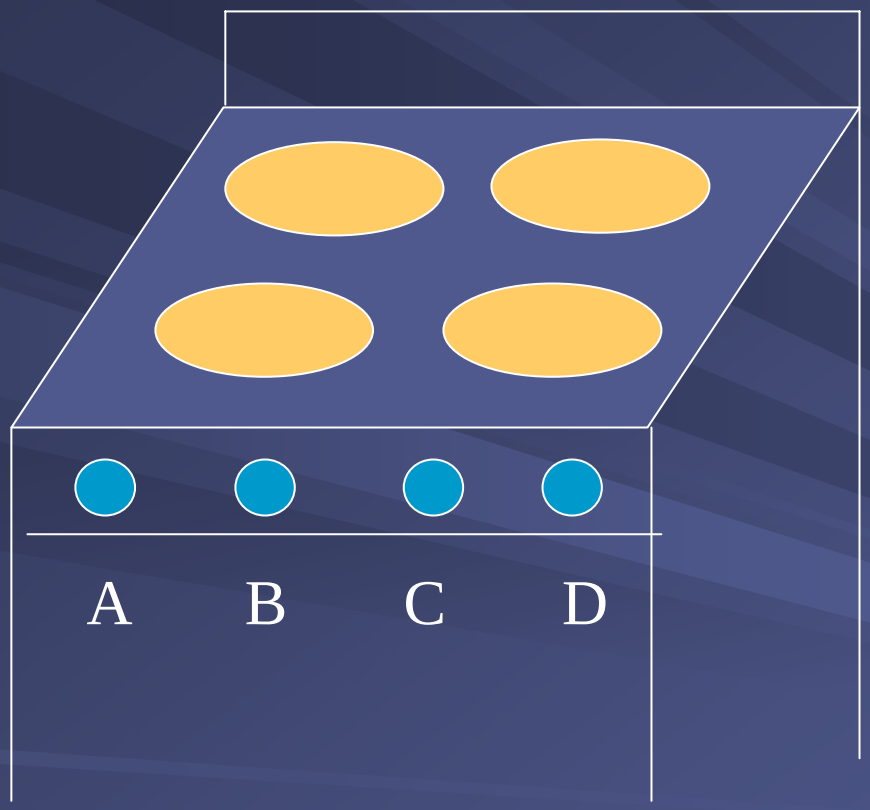
Safety—It's a Serious Responsibility

"You weren't listening. I said, 'Don't fall.'"

American Society of Safety Engineers

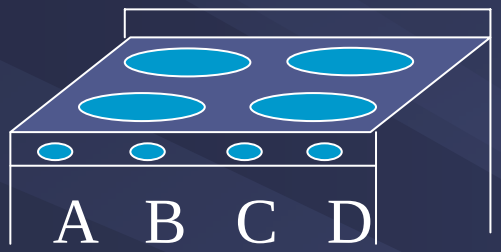
www.asse.org

Design Contributors to Error II

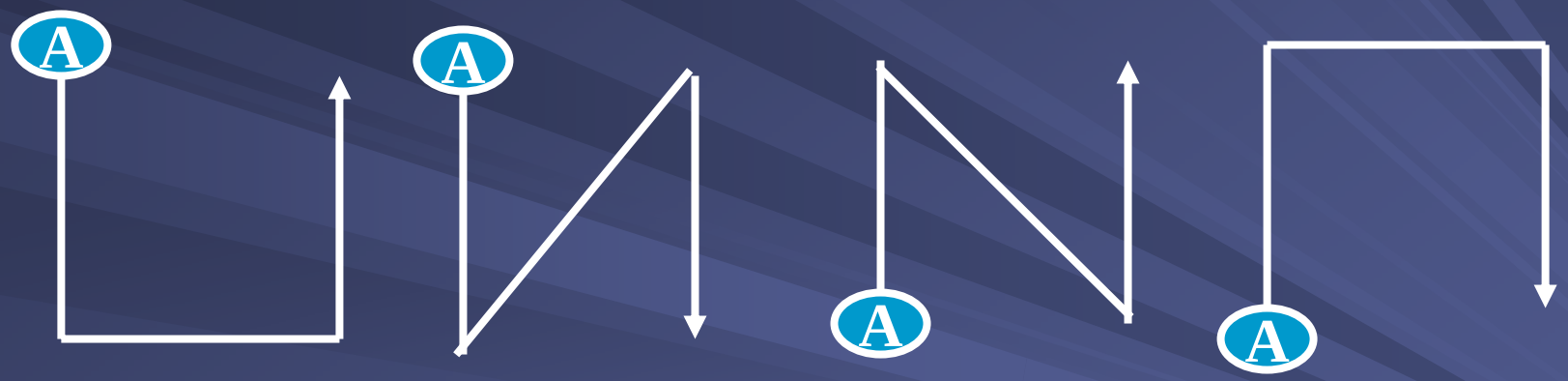


Determine which stove controls (A, B, C, D) are associated with which burners

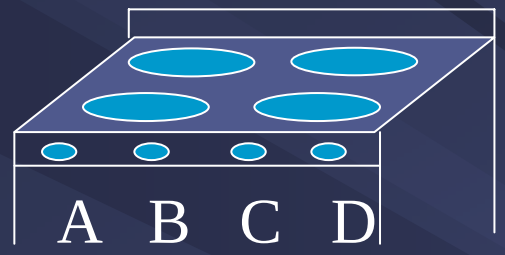
Test II:
“design expert” preferences



147 design students *S. Smith, Psych. Today, 1/84*

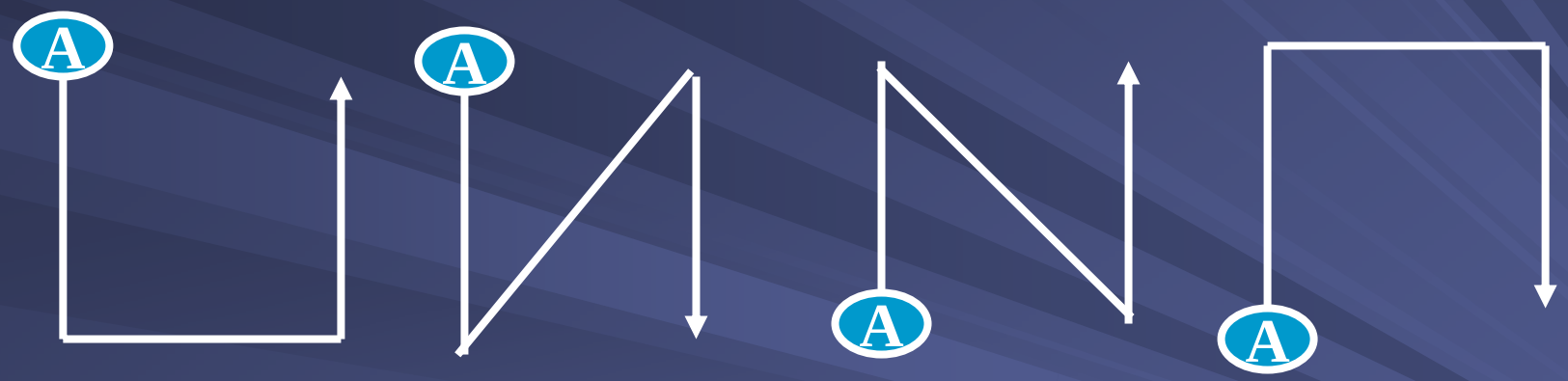


11%	25%	42%	22%

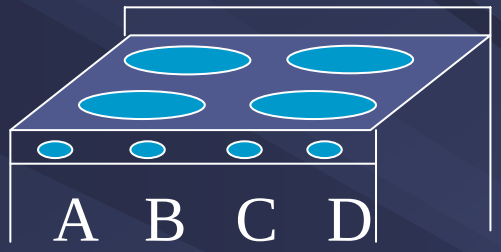


Test II: error rates over 1200 trials

Chapanis & Lindenbaum, Human Factors, 1, 1959

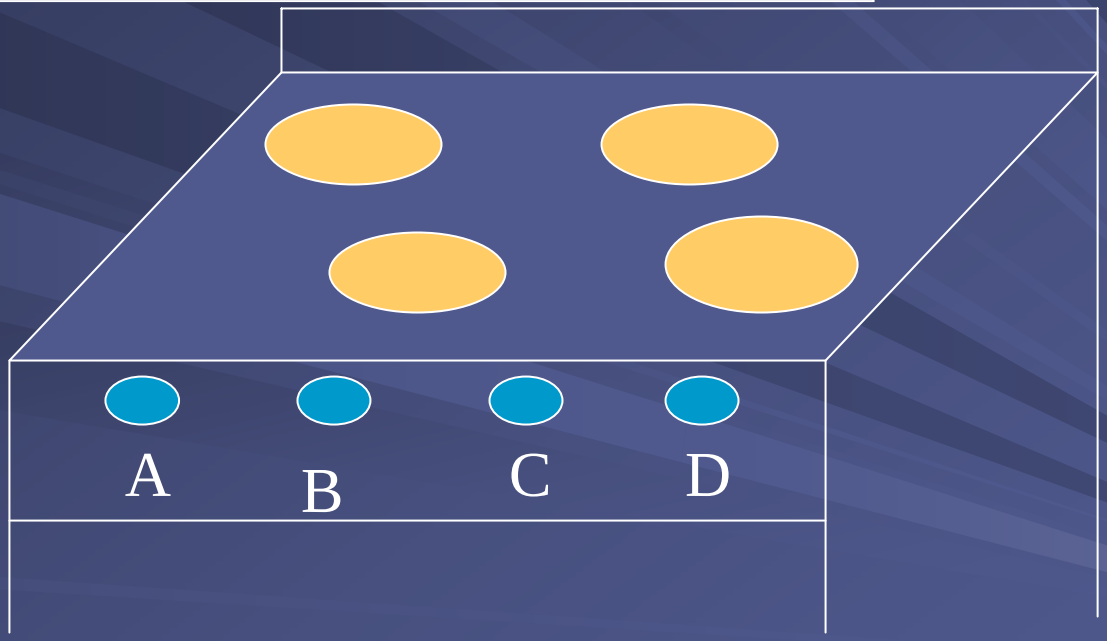


~ 6% errors	~10% errors	~11% errors	NA



Test II: Correct Answer

“Change the QUESTION!”



Number of errors in 1200 Trials = 0

A **New View** of "Human Error"

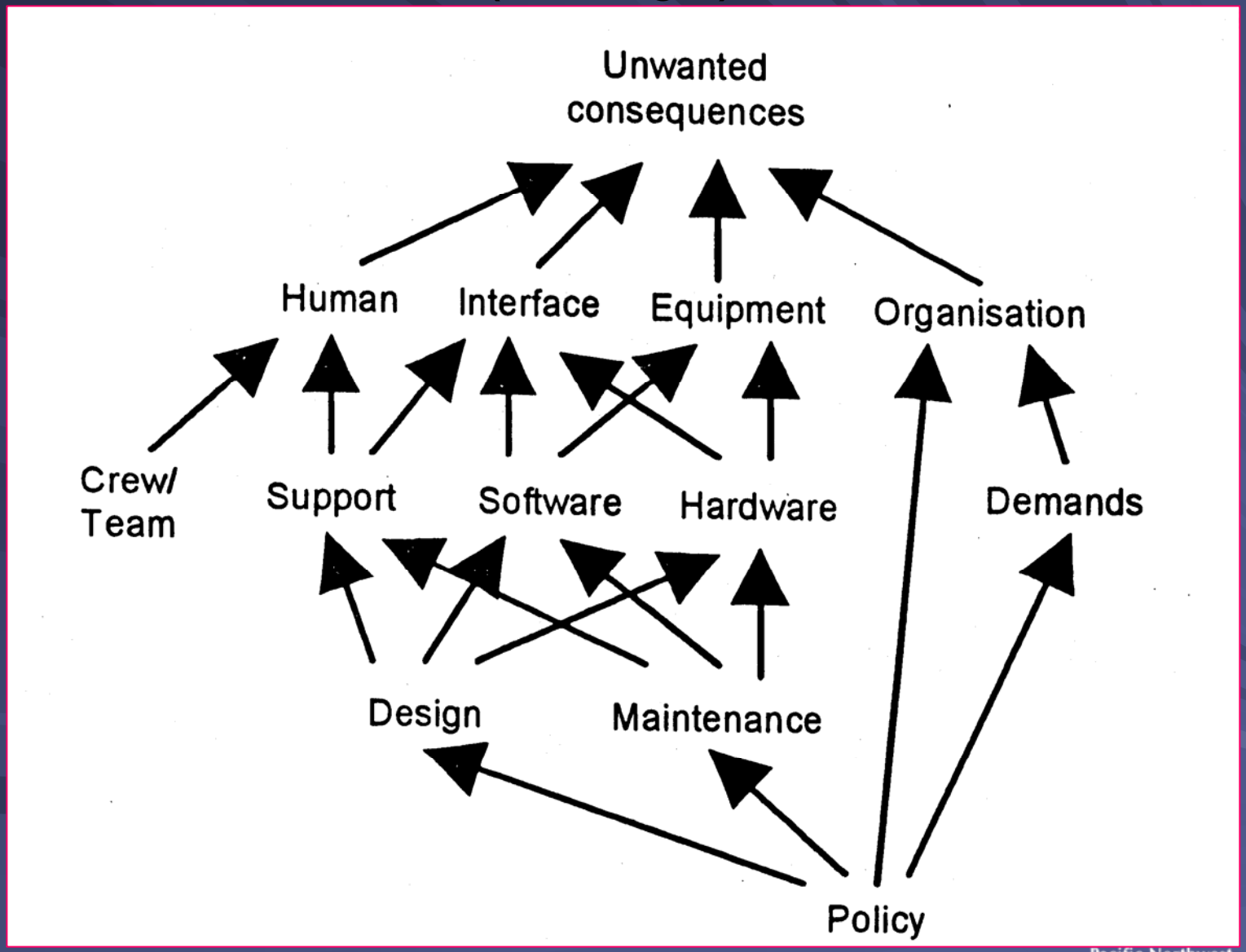
- "Human error is not random . . . it is systematically connected to features of people's tools, tasks and operating environment…[it] is a symptom of trouble inside a deeper system."

- "To explain failure, do not try to find where people went wrong . . .instead, investigate how people's assessments and actions would have **made sense at the time**, given the circumstances that surrounded them."

- "Human error is not the conclusion of an investigation. It is the **starting point**."

The Field Guide to Human Error Investigations, Sidney Dekker, Ashgate, 2002

Causes of Unwanted Consequences
(Hollnagel)



Applying Safety-Based Error Analysis Tools to Security Incidents

Incident Reduction: Premises

- Because the circumstances contributing to system-induced errors are similar in (safety) accidents and (security) incidents:

- Proven safety tools such as direct and contributing-cause analysis, as well as human-error and human-reliability assessments, can effectively be adopted/adapted for application to security

- Error-based security incident rates are likely to be similar to error-based accident rates (60-80+%)

COMPUTERWORLD An IDG company

QuickLink Search Computerworld

Home News Browse Topics Departments Services Subscribe Events Store Jobs

Management Careers Security Hardware Software Data Mgmt Networking Government Mobile Development Industry

COMPUTERWORLD

Study: Human error causes most security breaches

News Story by Grant Gross, IDG News Service

MARCH 18, 2003 (IDG NEWS SERVICE) - Human error Print-friendly E-mail this

not technology, is the most significan

security breaches, acc

released by the Computing Technolo

Association Inc. (CompTIA) today.

The survey, "Committing to Security:

Analysis of IT Security and the Work

more training and certification of IT workers will help the U.S. protect itself against cyberthreats. In more than 63% of security breaches identified by the survey's respondents, human error was the major cause. Respondent amed only 8% of security breaches on purely techn failures.

Brian McCa , CompTIA's CEO, called the results

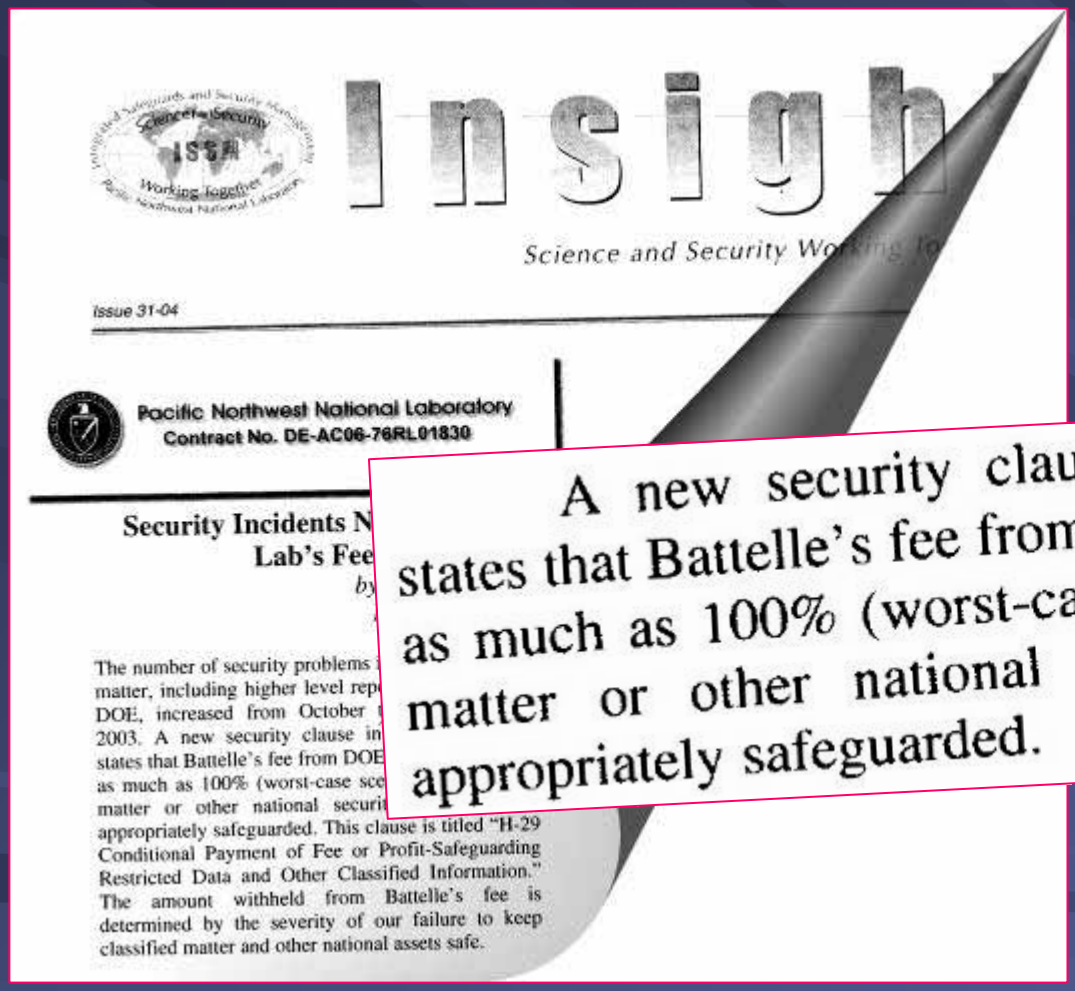
Human Error, not technology, is the most significant cause of IT security breaches, according to a security survey released by the Computing Technology Industry Association, Inc."

"In more than 63% of security breaches identified by the survey's respondents, human error was the major cause."

LANL's Challenge

- 12,000 cleared workers
- 100 security areas
- 6 metric tons SNM
- 100,000 classified weapons parts
- Tens of thousands of email message sent outside firewall daily
- 7,000,000 classified documents
- 650 ADCs
- 100+ Classification Guides in use
- 2,000 stand-alone classified computers

Performance Failures Affect Fees



Insight

Science and Security Working Together

Issue 31-04

Pacific Northwest National Laboratory
Contract No. DE-AC06-76RL01830

Security Incidents N
Lab's Fee
by

The number of security problems
matter, including higher level rep
DOE, increased from October
2003. A new security clause in
states that Battelle's fee from DOE
as much as 100% (worst-case sce
matter or other national securi
appropriately safeguarded. This clause is titled "H-29
Conditional Payment of Fee or Profit-Safeguarding
Restricted Data and Other Classified Information."
The amount withheld from Battelle's fee is
determined by the severity of our failure to keep
classified matter and other national assets safe.

A new security clause in PNNL's contract states that Battelle's fee from DOE can be reduced by as much as 100% (worst-case scenario) if classified matter or other national security assets are not appropriately safeguarded.

PNNL "Insight" February 2004

DOE Order 471.4 – Incidents of Security Concern

- Inquiries must establish the facts and circumstances surrounding an incident.
- Inquiries must be used to determine the [direct cause and contributing causes] and the individuals responsible.
- Procedures must be established to enable error analysis of incidents of security concern.
- Incident analysis must provide the basis for determining the cause of the incident and corrective actions.
- Appropriate corrective actions must be taken for each incident to prevent recurrence.

Effective Error Analysis/Corrective Action Program

- Prompt investigations following an incident or identification of an adverse trend
- An administrative procedure that describes the process and assigns responsibility for investigations of equipment and human performance problems
- Management emphasis on identification and correction of problems that can affect human, organizational, and equipment performance.

DOE-NE-STD-1004-92, ***DOE Guideline: Root Cause Analysis Guidance Document***, *February 1992*

LANL Security Incident "Causes" (2002)

- Most: "Failure to follow DOE/LANL procedures"
- Many: "Personnel error"
- Up to 30% had no "cause" identified and no corrective action recommended

ESTHER

Enhanced Security Through Human Error Reduction

Los Alamos

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

PNNL-SA-42136

Prevention or Blame

"...when the purpose of an accident [or security incident*] investigation is to design a prevention program, people tend to make external, system-focused causal attributions. When the purpose is to assign responsibility and blame, people tend to make internal, personal attributions."

Colligan, M.J. & Cohen, A. (2004). The Role of Training in Promoting Workplace Safety and Health. In: Barling, J. & Frone, M.R. eds. The Psychology of Workplace Safety, pp 223-248. Washington, DC: American Psychological Association.

* modified by ESTHER, 2005

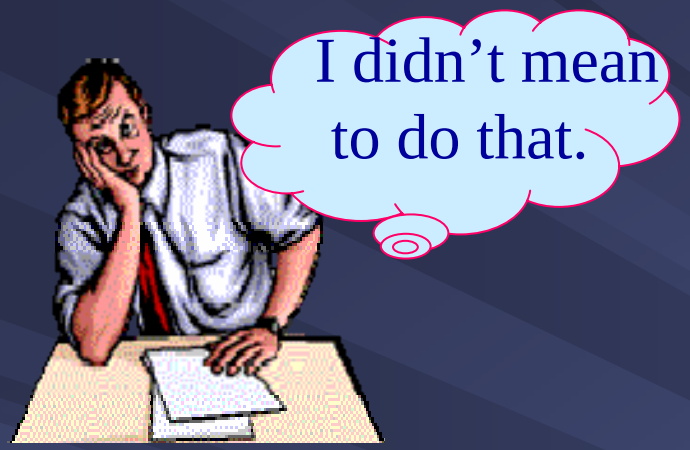
ESTHER

- LANL developed and implemented *ESTHER*—Enhanced Security Through Human Error Reduction
- A process to guide and aid causal analyses and document contributors to security incidents as a basis for developing targeted, effective corrective actions and disseminating *lessons learned* to reduce the likelihood of future incidents.
- Supports compliance with DOE Policies, Orders, Standards
- Adopted by DOE-SO as part of the forthcoming web-based incident reporting process via *ITAC (Incident Tracking and Analysis Capability)*

ESTHER Key Terms I

- Error – non-malevolent action, or failure to act, that is intended to achieve a correct outcome but is inadvertently not in accordance with requirements or procedures.
- Breach – deliberate deviations from policies, procedures, etc. with no intention to undermine correct outcome or incur adverse security consequences.
- System-Induced Errors/Breaches - those errors or breaches made more likely—perhaps virtually inevitable—by existing conditions or circumstances.

ESTHER Error Types



Unintentional Acts

Unintentional Failures to Act

Intentional, But Incorrect, Acts

Intentional, But Incorrect, Failures to Act

Breach Impacts

- Increase the inevitability or severity of accidents/incidents by
  - Expending the "margin of error" designed into the system
  - Negating the recoverability of erroneous actions that may follow

- Safety example:
  - Failure to use a safety harness when working on an elevated platform (breach) can mean that a simple slip (error) results in death rather than a few bruises

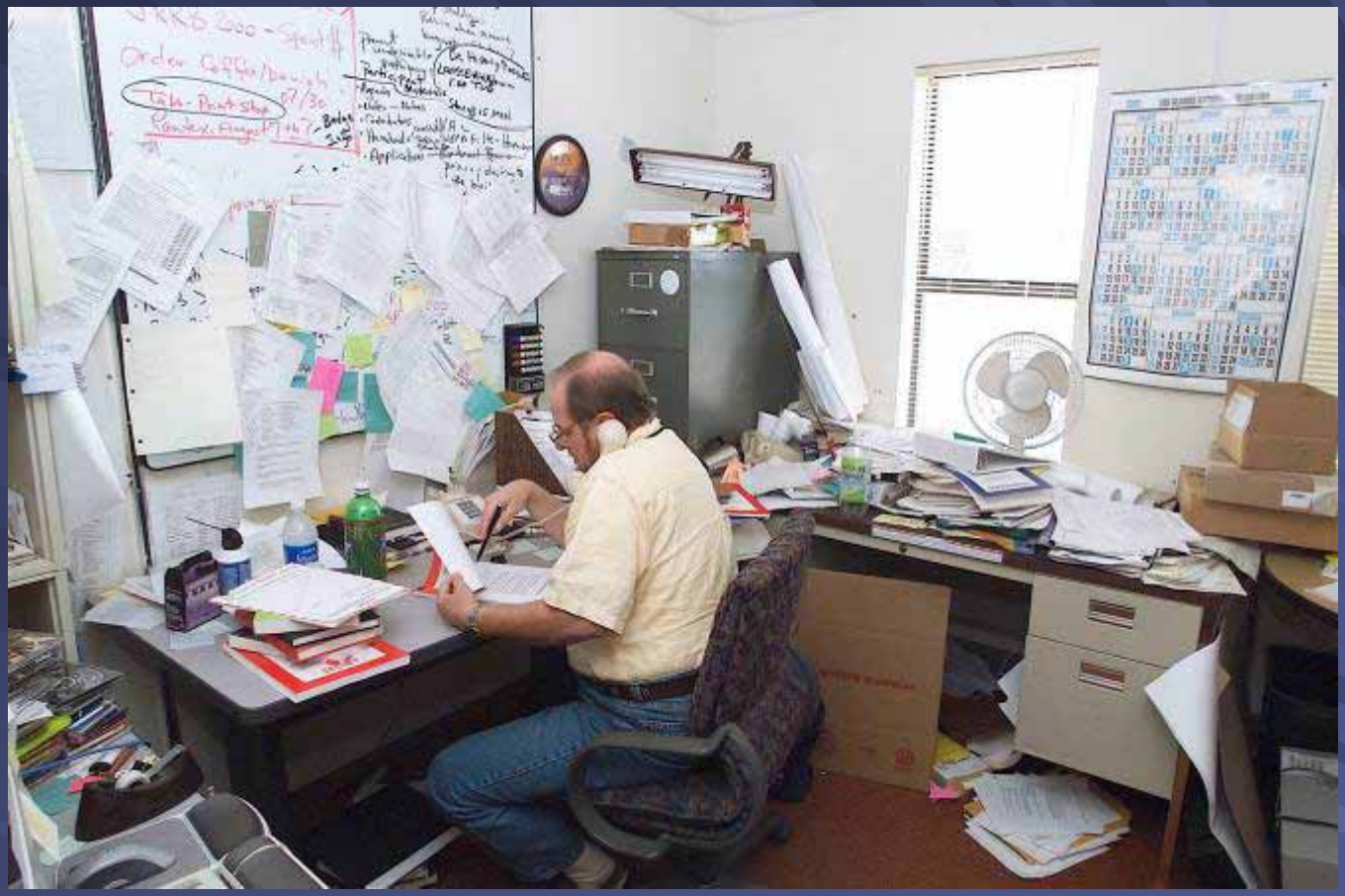
- Security example:
  - Preparing a classified document on an unclassified computer (breach) can have severe national security consequences if this document is then mistakenly attached to an email message (error)

ESTHER: Key Terms II

- Contributing Factors - Actions or circumstances that can influence how people reason or behave and which may increase the likelihood of error
- Direct Cause – Often the most obvious activity or situation resulting in – and frequently immediately preceding – a security event.

ESTHER: Example Situational Factors

- Distractions
- Time Factors
- Routines Changed
- Inadequate Information
- Poor System Feedback
- Deficient Work Planning
- Inappropriate Environment
- Inappropriate Culture/ Local Practices



What could lead to error here?

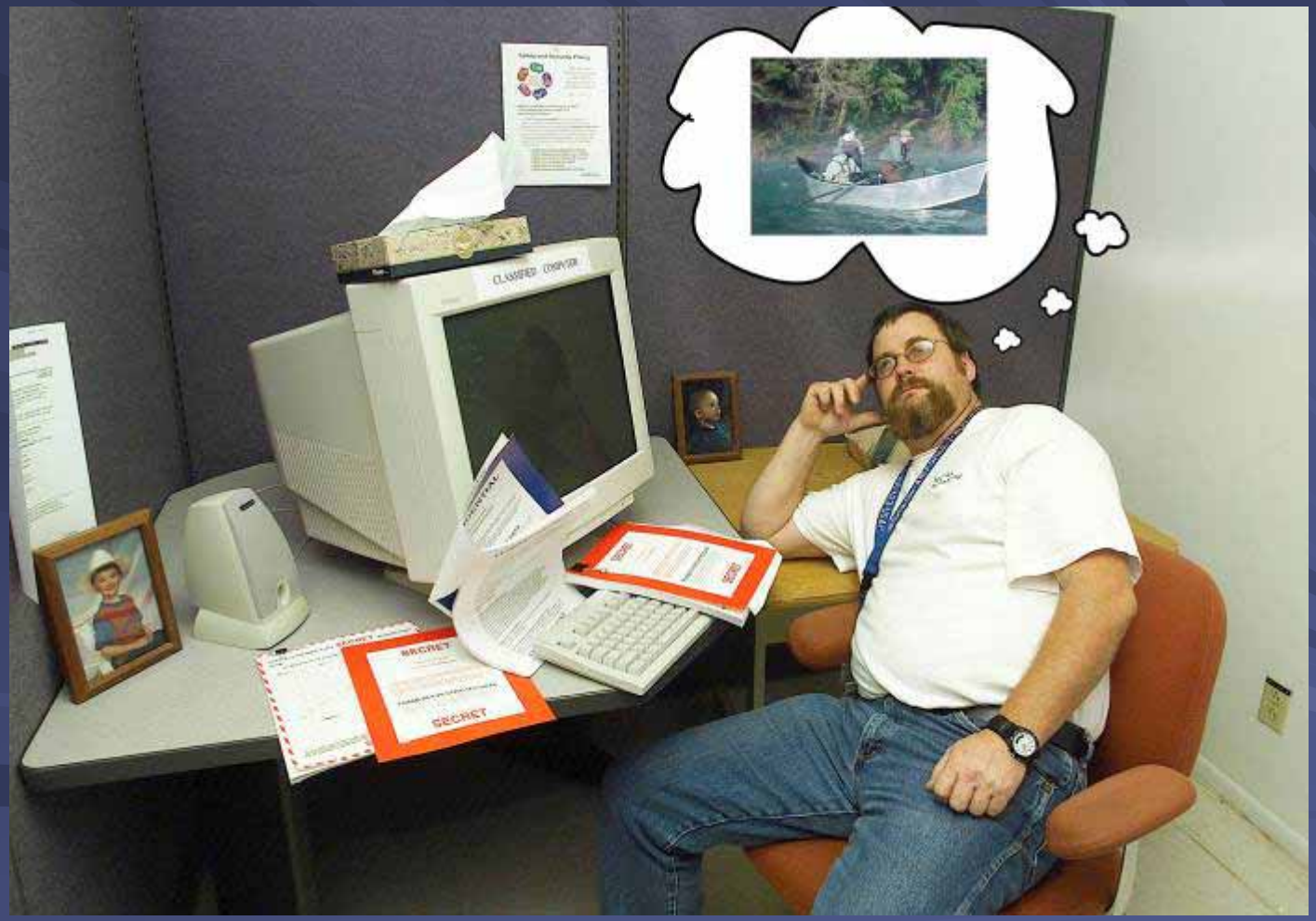
Situational Factor

ESTHER: Example Personal Factors

- Preoccupation
- Stress/Anxiety
- Fatigue/Boredom
- Drug Side Effects
- Inadequate Knowledge
- Misperception
- Memory Failure
- Faulty Reasoning

Personal Factor

Personal Factor



Reactive ESTHER

INCIDENT (or "near miss")

↓

INQUIRY (or error assessment)

↓

ANALYSIS → **FIXES** → **LESSONS LEARNED**

ESTHER Tools

- Reactive
  - Inquiry Field Guide
  - On-site Workshops for Inquiry Officials / Managers
  - CBT for Inquiry Officials
  - *On-site Workshops for Security Responsible Line Managers / Security Staff*

ITAC Incident Reporting: Contributing Factors

ESTHER - Scenario 1: Contributing Factors - Microsoft Internet Explorer

Contributing Factor(s)

These are the factor(s) that, alone, are unlikely to have caused the event, but which (in combination) led to the Direct Cause of the event. **Check all that apply.**

Move your mouse cursor over each factor for its definition and examples.

Data Flow	Work Setting	Work Planning/Control	Employee Readiness
☐ Information	☐ Distractions	☐ Job Pressure	☐ Preoccupation/Inattention
☐ Procedures/Directions	☐ Material/Resources	☐ Time Factors	☐ Stress/Anxiety
☐ Communication	☐ Environmental (Temperature, Lighting, etc.)	☐ Task Difficulty	☐ Fatigue/Boredom
☐ System Status/Feedback	☐ Management Systems	☐ Task Aversion	☐ Illness/Injury
	☐ Security Practices	☐ New Routine	☐ Drug Side Effects
		☐ Task Planning	☐ Misperception
		☐ Management	☐ Memory
		☐ Ability	☐ Reasoning/Judgment
		☐ Experience/Skill	☐ Values/Attitudes
		☐ Knowledge	

Check Factors

ITAC Incident Reporting: Direct Cause

DIRECT CAUSE

The cause that directly resulted in, and often immediately preceded, the event.

Double click each cause for its definition and examples.

Check ONLY ONE and Describe in Detail

☐	Equipment/Material Failure	**Describe in Detail:**
☐	External Phenomena	
	Personnel Decision / Action	
☐	Intentional, Incorrect Action	
☐	Intentional, Incorrect Failure to Act	
☐	Unintentional, Incorrect Action	
☐	Unintentional, Incorrect Failure to Act	
☐	Non-Malevolent Breach of Proper Action	
☐	Willful, Malevolent Act	
☐	Other: **Define**	☐ **Cannot be determined at this time**

Proactive ESTHER

EDUCATION & OUTREACH → **FIXES** → **LESSONS LEARNED**

↓

ASSISTANCE CALL

↓

ANALYSIS → **FIXES** → **LESSONS LEARNED**

ESTHER Tools

- Proactive
  - Management Walk-around Guidance Card
  - *On-site Workshops for Security Responsible Line Managers / Security Staff*

ESTHER Payoffs I

- Comply with Orders, Policies, Standards

- Improved security
  - Local benefit: elimination of discovered/reported error/breach contributing conditions
  - Widespread benefit: dissemination of lessons learned throughout LANL and DOE Complex
  - Direct benefit: fewer inadvertent releases of classified information
  - Indirect benefit: fewer resources devoted to error/breach-based incidents; thus, focus can be placed on true threats and malevolent actions

ESTHER Payoffs II

- Targeted performance metrics
  - Before- rather than after-the-fact indicators of security effectiveness.
  - Useful as positive motivation in recognizing and rewarding effective performance and improvements.
  - The potentially large number of error contributors identified and rectified can be a more meaningful and reliable indicator of security program effectiveness than the relatively small number of incidents. This is also true for year-to-year and inter-organizational comparisons.

ITAC: Online Reporting, Tracking, and Trending

Shannon S. Mace, PNNL
Information Security Resource Capability (ISRC)
April 18, 2005

ITAC Mission

- Established to provide operational and technical support to DOE/SO and Departmental Incidents of Security Concern Programs
- Secure electronic means for Departmental sites to report, track, and trend incidents of security concern
  - Correlation of incidents that have or are occurring within the Department

ITAC Mission, cont.

- Provide information and assistance to the Department in developing:
  - Policy
  - Conducting analysis of inquiries
  - Support NTC training course development and presentations
- Support DOE/NNSA Monthly & Quarterly reporting requirements

ITAC Support

- Perform Incident Analysis
  - Multi-incident analysis using queries & search tools
  - Graphical data representation
  - Individual case analysis support
- Support special query/report requests from HQ, the Program Offices, and the Field
- Track and trend incidents of security concern

ITAC Incident Analysis

- Incident Analysis at the local and national level will assist in evaluating:
  - Significant security and policy implementation issues
  - Root cause and Corrective actions
  - Policy development and security awareness bulletins
  - Provide support for management decisions regarding new policies
  - Updates of site S&S training & briefing material
  - Provide input for various Quality Panel & Workshop discussions

ITAC

- Web Site - http://www.pnl.gov/isrc/itac.stm
- E-Mail - itac@pnl.gov

- Questions??

ESTHER CBT:
Computer-Based Training on Human Errors Contributing to Security Incidents

Frank L. Greitzer

Pacific Northwest National Laboratory

frank.greitzer@pnl.gov

Background on ESTHER CBT

- Los Alamos National Laboratory developed and conducts ESTHER workshops
- Pacific Northwest National Laboratory developed the CBT
  - This is a self-directed computer-based training program to complement the workshops
  - It has been developed as an interactive, scenario-based training application that can be used in the workshop or as online instruction.

Provides distinct and varied pathways to learning by triangulating instructional approaches

ESTHER Pathways to Learning

Classroom

Human Error Overview → Overview of ESTHER system → ESTHER Causes & Contributors To Error (Terms)

Focus of this presentation

Self-Directed

Discovering Contributors, Prompted	Using Contributors, Unprompted	Documentation Using ESTHER Terms
3-level feedback	3-level feedback	3-level feedback

Field Application

Incident Inquiry → Documentation ITAC using ESTHER terms → Data Aggregated For "Lessons Learned"

Guided Discovery Approach

- Guided Discovery differs from traditional “passive” learning
  - In traditional instruction, information is presented in a series of lessons, each followed by objective questions to test the learner’s understanding.
- Guided Discovery (“active” learning)
  - A more experiential approach presents realistic problems (scenarios) and provides coaching to facilitate learning.
  - As the learner gains knowledge and skill, the level of coaching diminishes and more responsibility is left to the student.

Discovery learning imposes a greater cognitive load on the learner…

Managing Complexity of Learning Content

Terminal Learning Objectives

Enabling Learning Objectives

Relating to prior knowledge, experience

Transfer

Conduct Inquiry

Understand concepts

Human Error Contributors

Recognize and discriminate among examples/instances

Observations

complex

simple

Applying knowledge directly in the field

Developing understanding of higher-level concepts

-- Hints, coaching

-- Partially worked examples

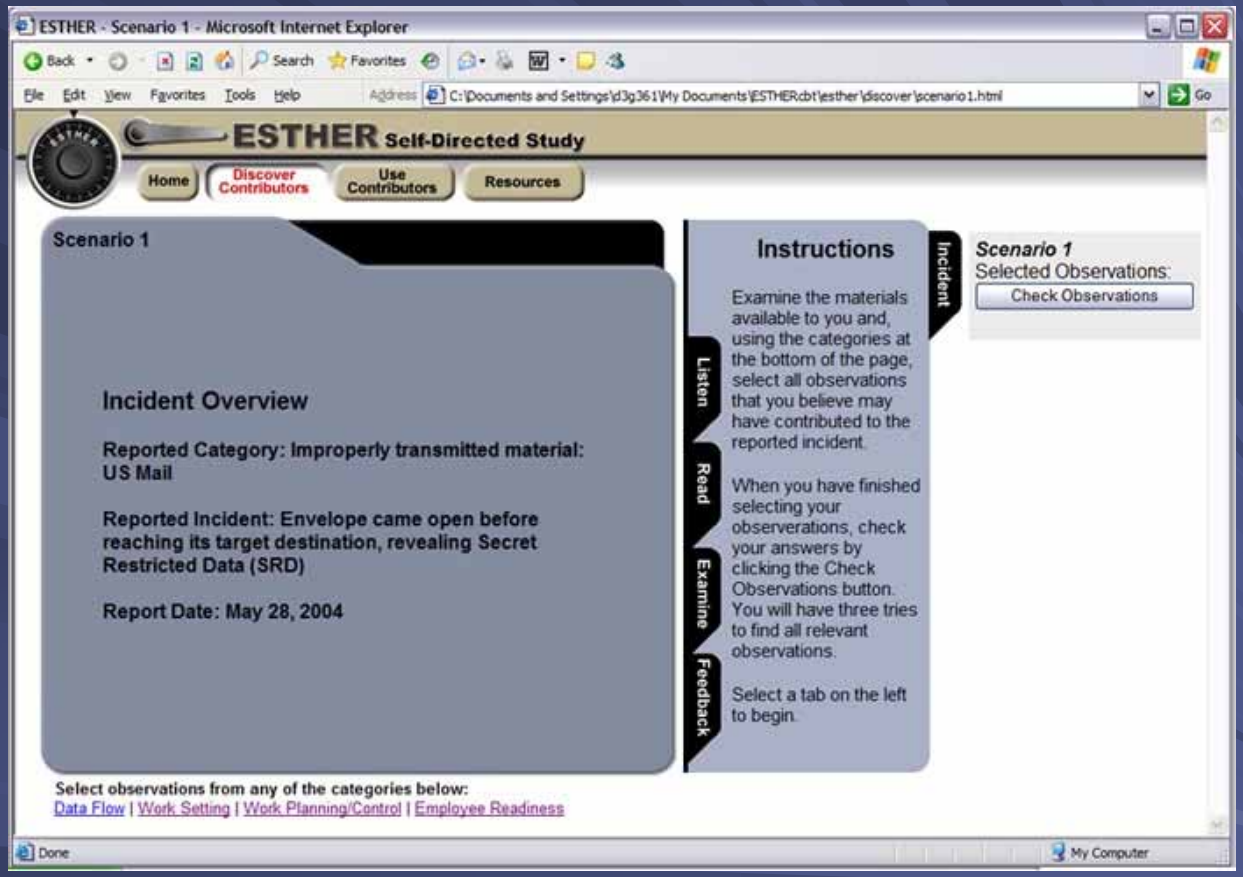
Raising awareness through sample scenarios

-- part-task

Discovery Module – Scenario Description

Learner "explores" evidence to discover observations that apply to the scenario…

Incident tab provides description

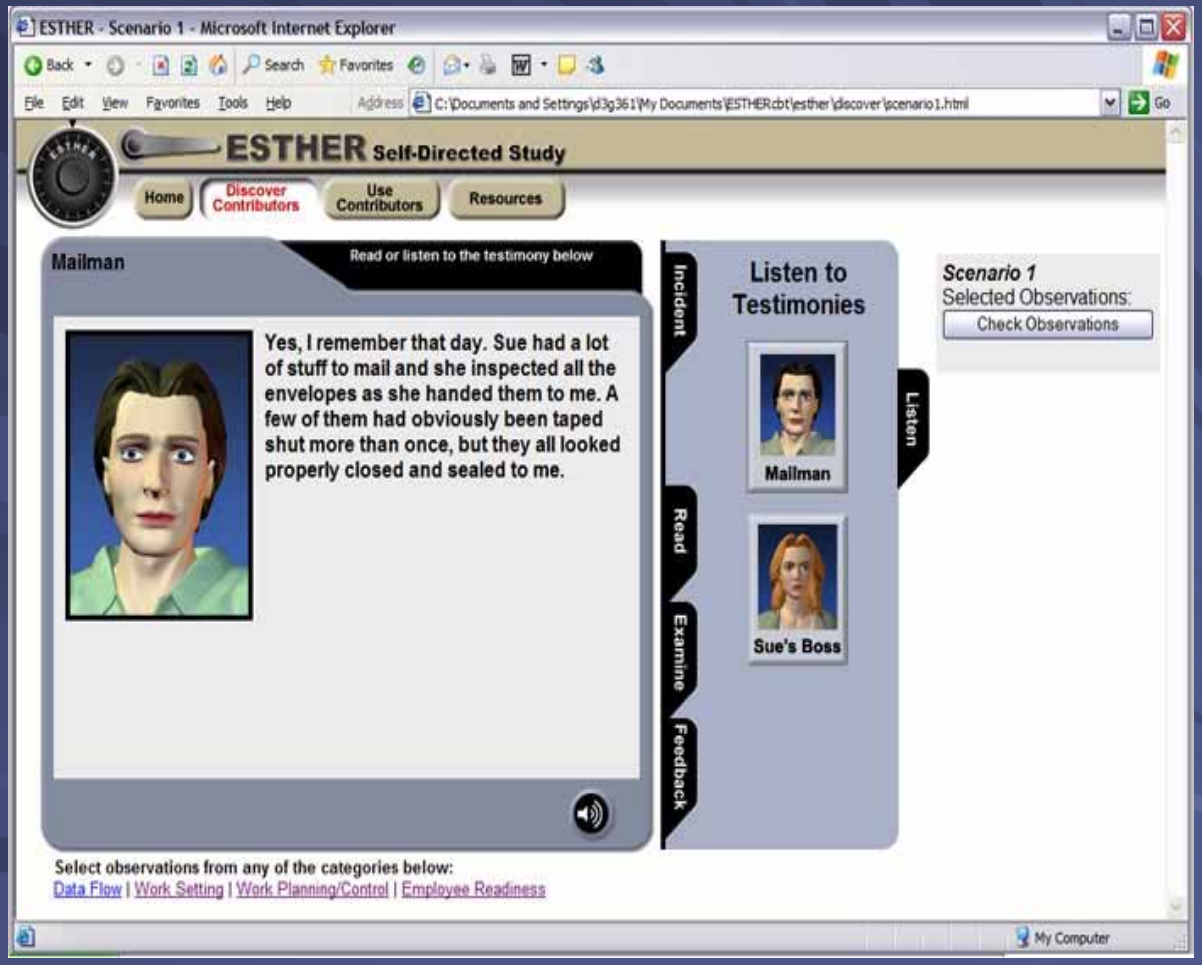


Discovery Module – Testimonies

Learner "explores" evidence to discover observations that apply to the scenario…

Listen tab shows testimonies

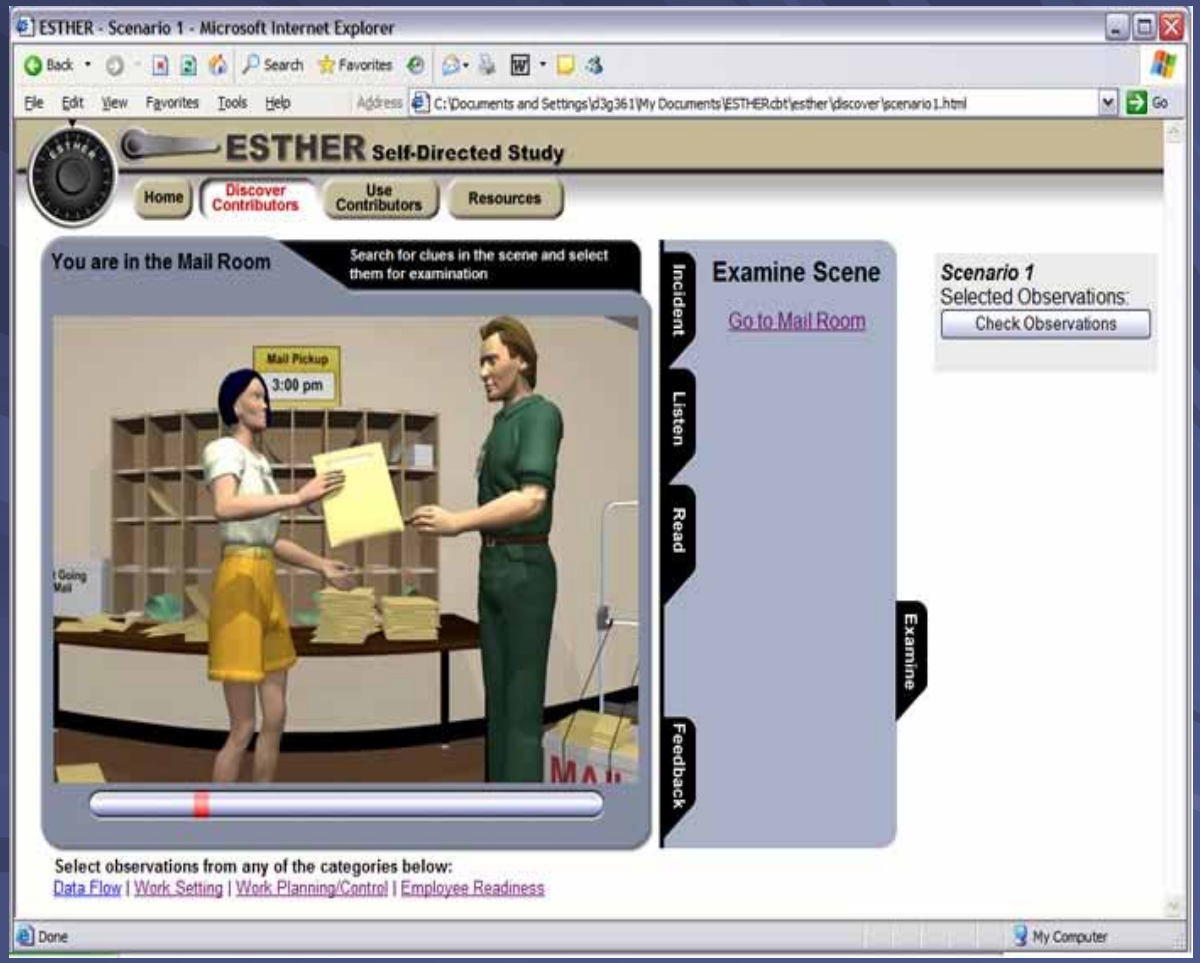
Read tab shows documents



Discovery Module – Simulation/Animation

Learner "explores" evidence to discover observations that apply to the scenario…

Examine tab shows simulated interactive re-enactment of one or more scenes



Discovery Module – Feedback

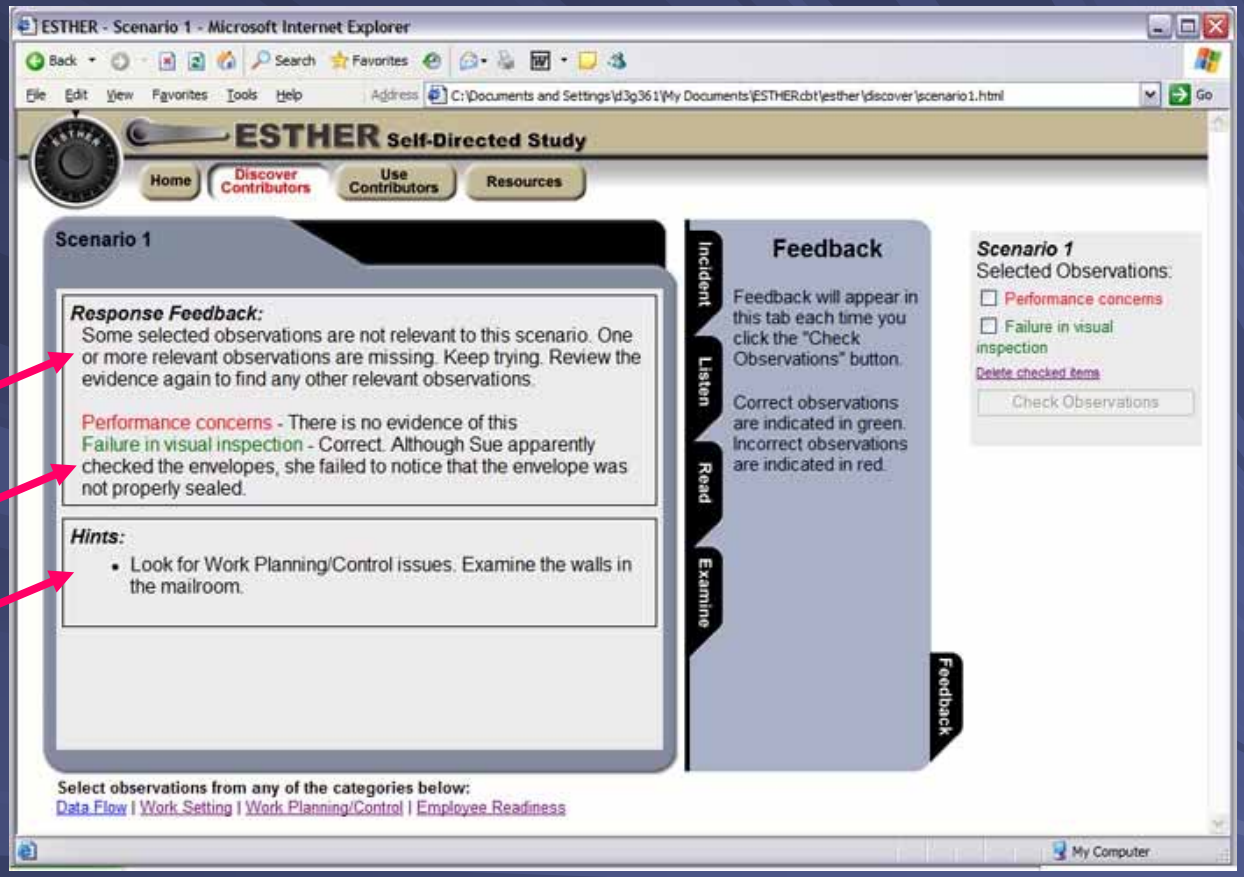
Multilevel feedback is provided after learner selects observations that apply to the scenario

Levels of Feedback:

General

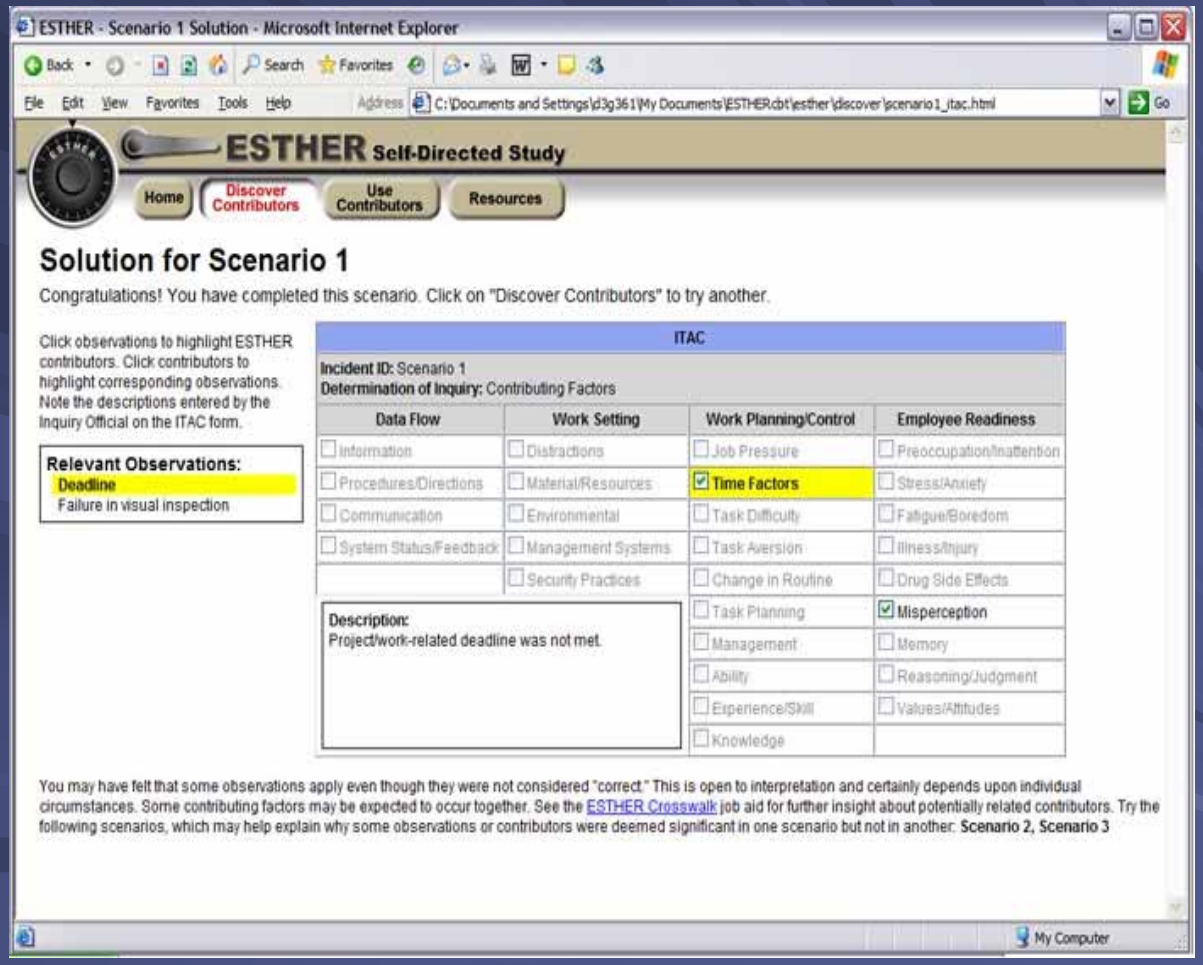
Correct/Incorrect

Hints



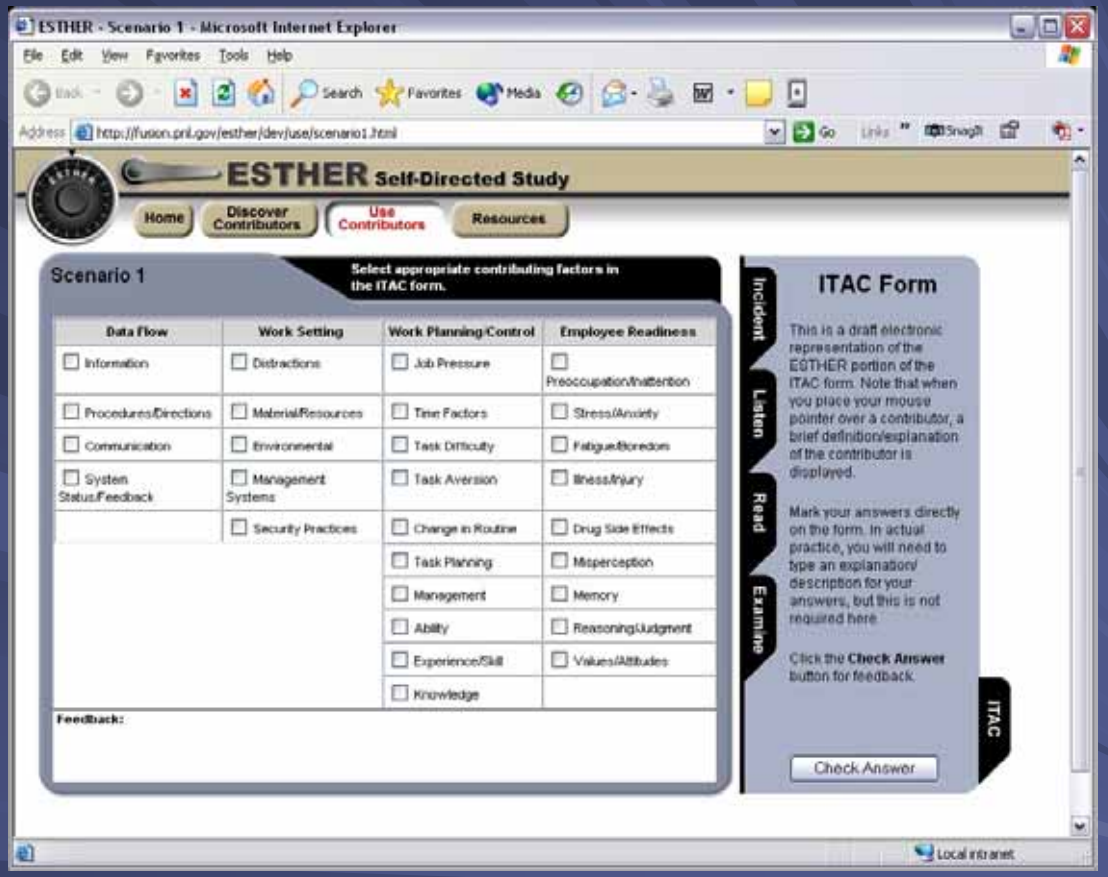
Discovery Module – Higher Level Concepts

Observations are related to the ESTHER contributors on the reporting form



Advanced Module – Use Contributors

Learner works on similar scenarios but must respond directly using ESTHER contributors on the reporting form



Conclusions

- Web-based version of ESTHER CBT is operational. It can be accessed at http://www.pnl.gov/esther/
- The guided-discovery learning is a new approach to computer-based training that is applicable to a broad range of instructional contexts. Possible applications:
  - Online training for general staff to raise awareness about error contributing factors and *help prevent* security incidents
  - Guided Discovery learning to support safety/accident prevention programs
  - Guided Discovery learning to support cyber security training

ESTHER CBT Demo