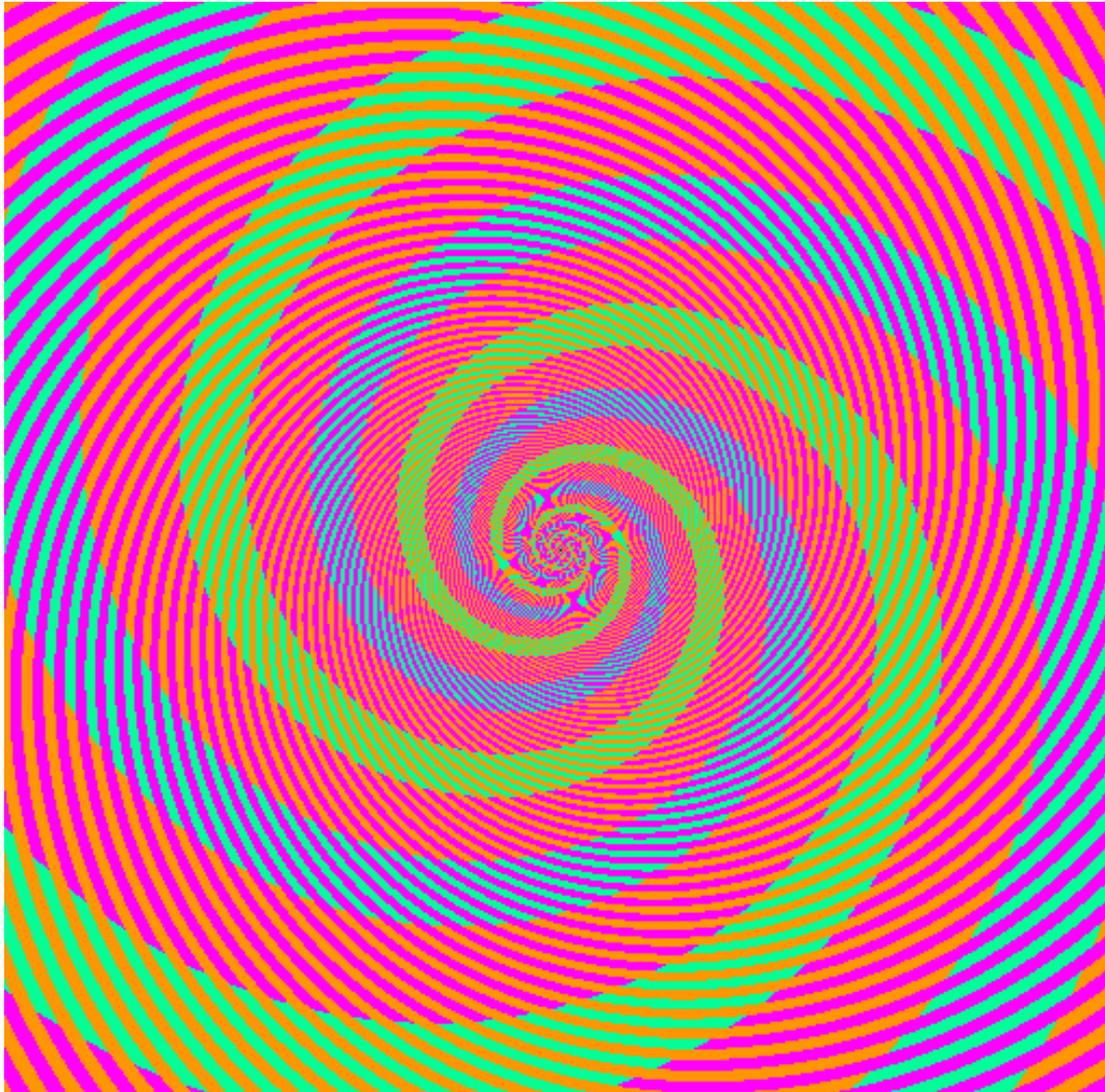


# After lunch gentle wakeup



Invent an algorithm.

How many spirals of each color?

Blue?

Green?

Pink?

# ISRCS 2009

## Tutorial

### Session 3: Human vulnerabilities

Miles McQueen, MS

University of Idaho and Idaho National laboratory



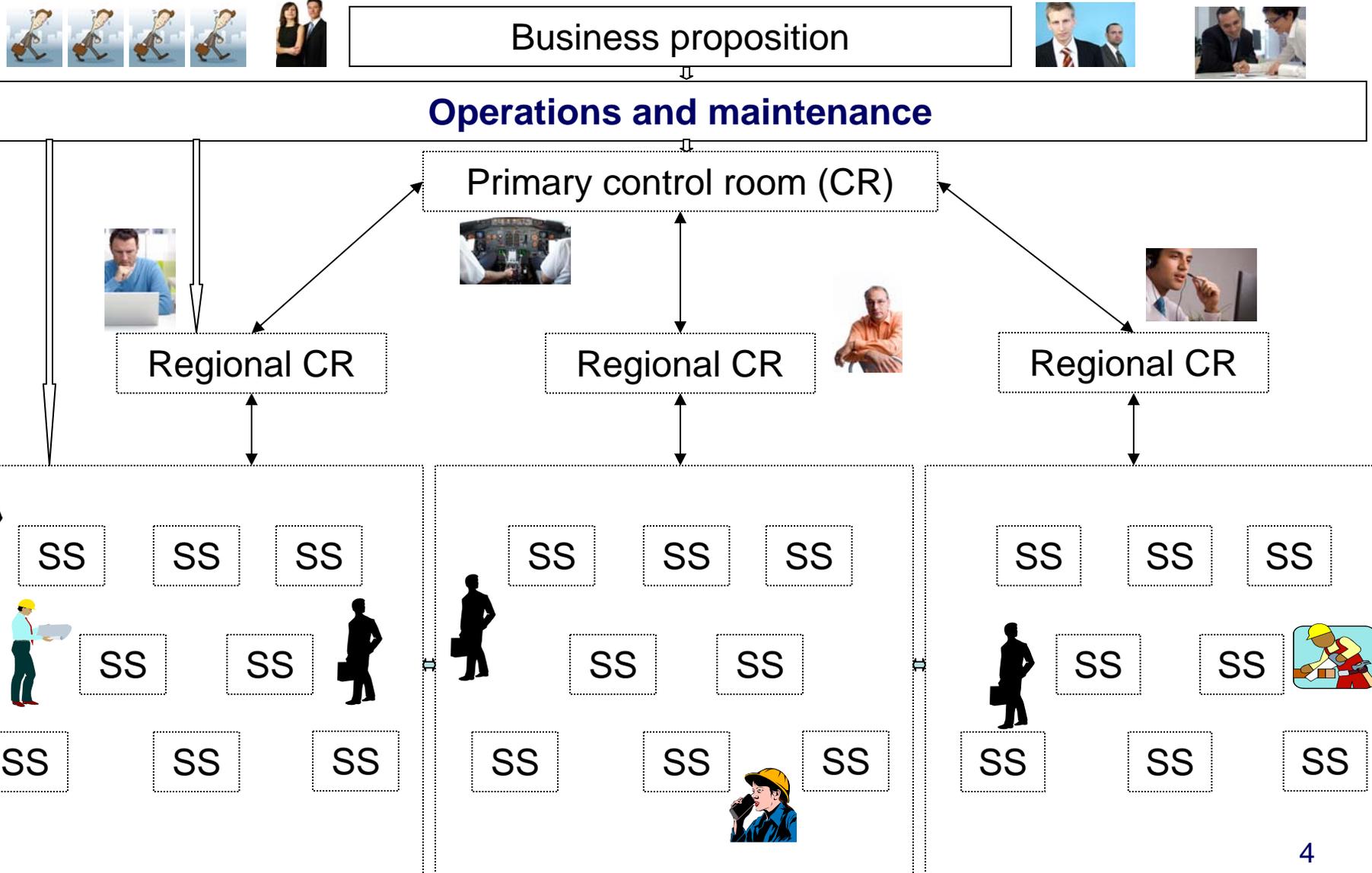
August 11, 2009  
Idaho Falls, Idaho

# Outline for session 3: Human Vulnerabilities

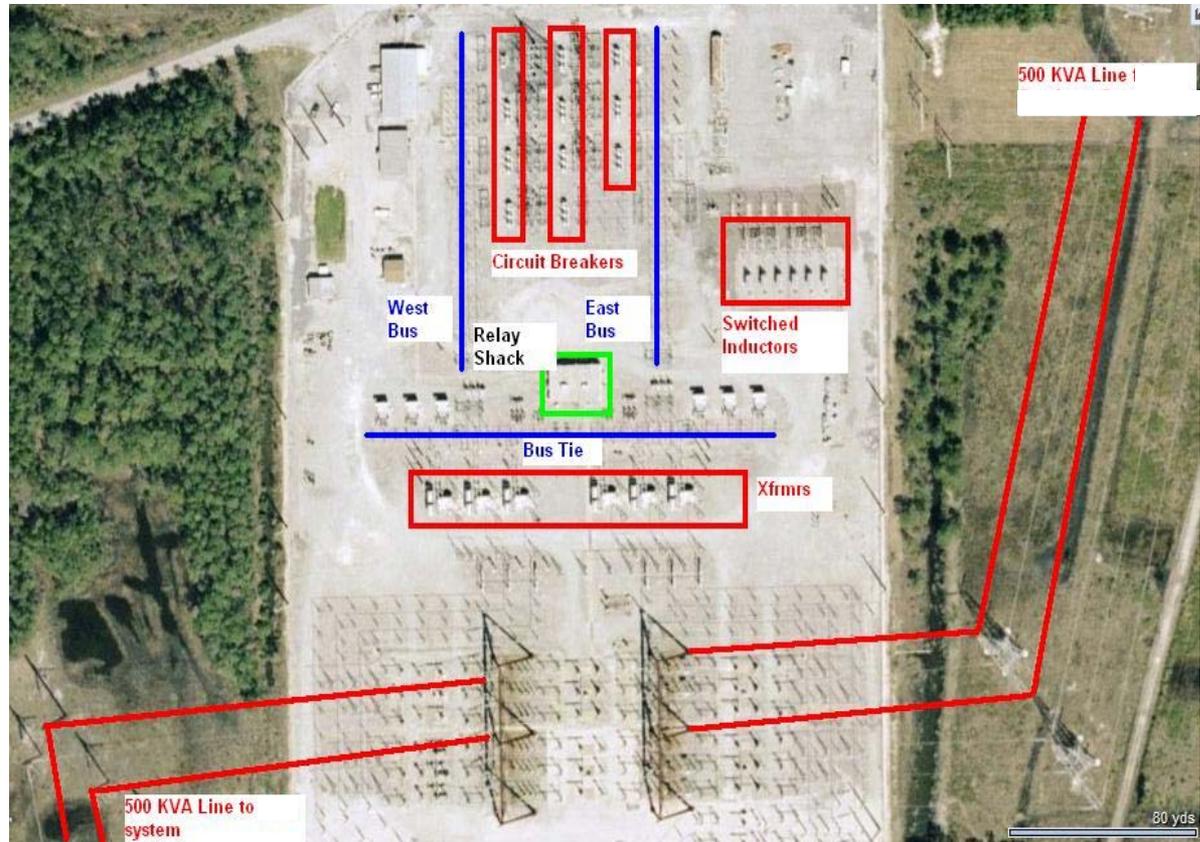
- 1. People are integral to system function**
- 2. Human decision making**
- 3. Operators, and others, may be intentionally deceived**
- 4. Social engineering**
- 5. Addendum**

# People are integral to system function

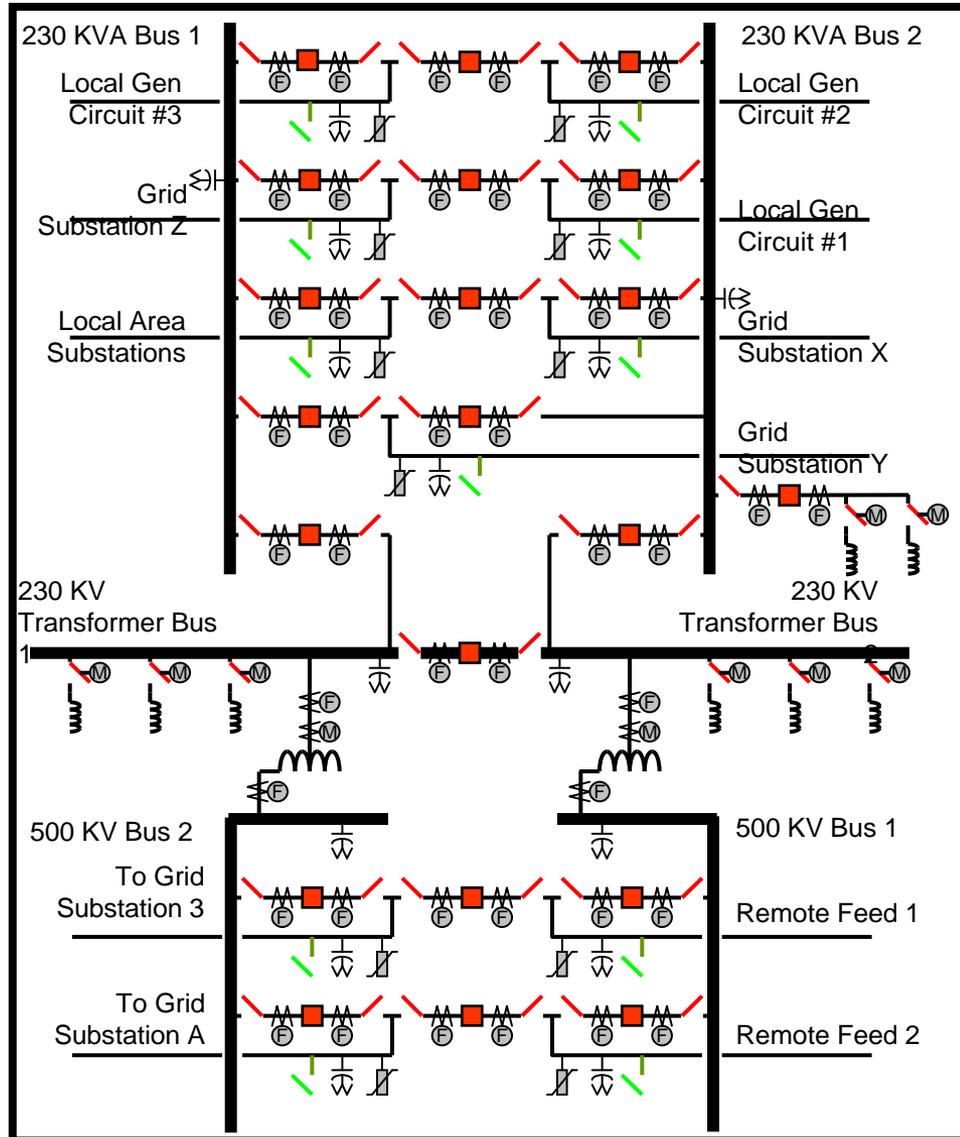
## Power grid example



# Sample substation

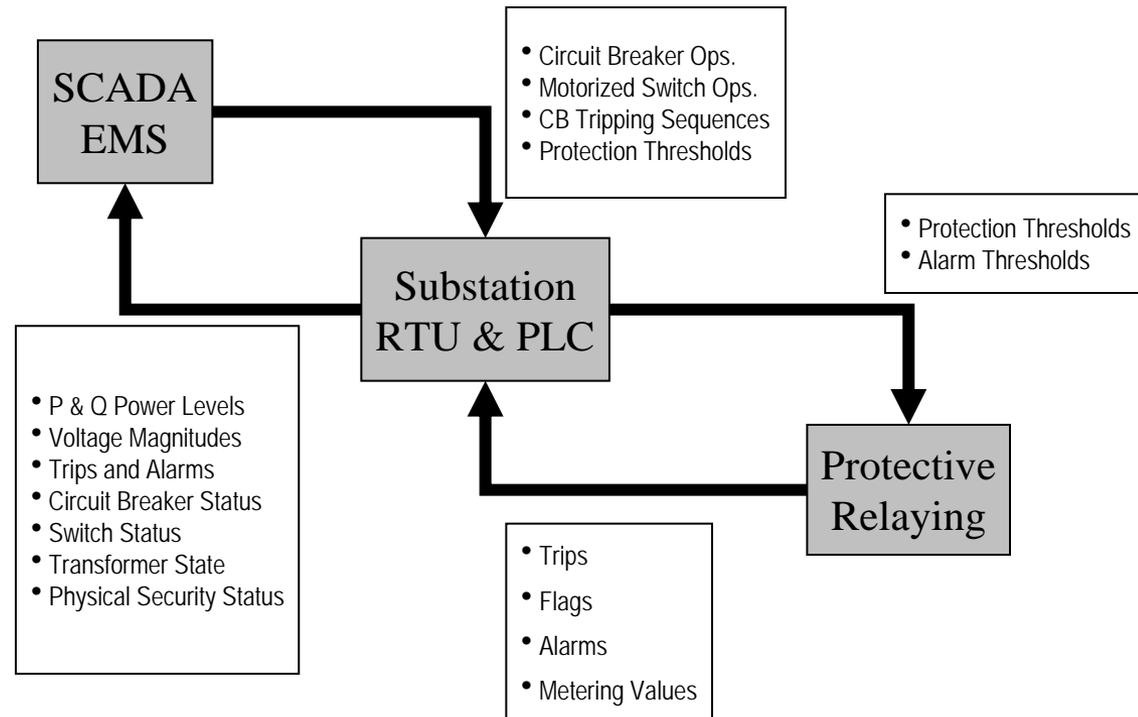


# Notional breaker topology

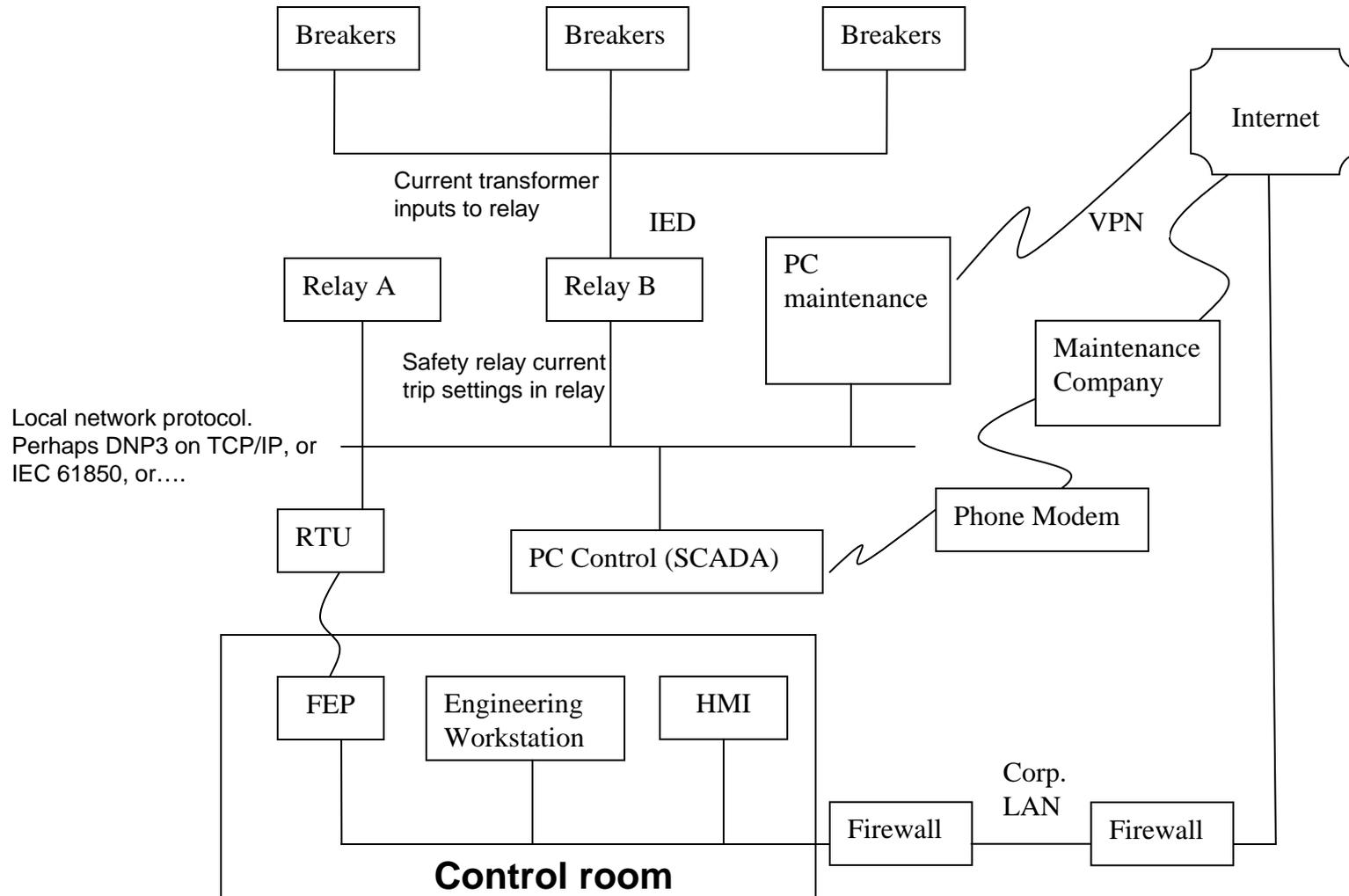


# Substation data

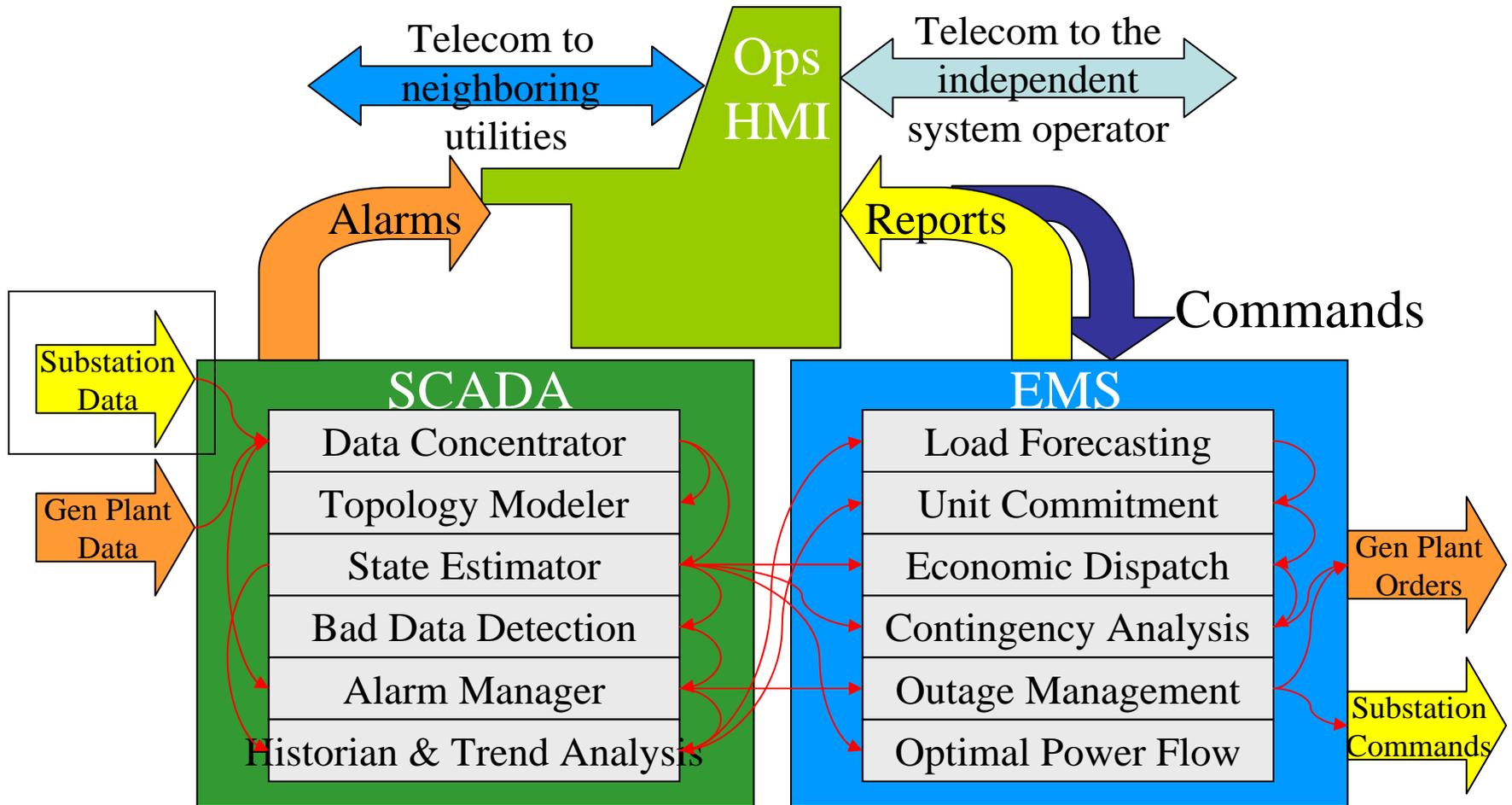
- ❖ Operator view of the state of their system is driven by these features.
  - Feature space open to spoofing
    - alarms, voltages, etc...



# Notional communications



# High level functions in control room



# Sample control room



# The operator

## ❖ Operator tasks

- React to alarm conditions if necessary.
- Dispatch generation
  - aid utility in minimizing costs
- Negotiating with neighboring utilities for power.



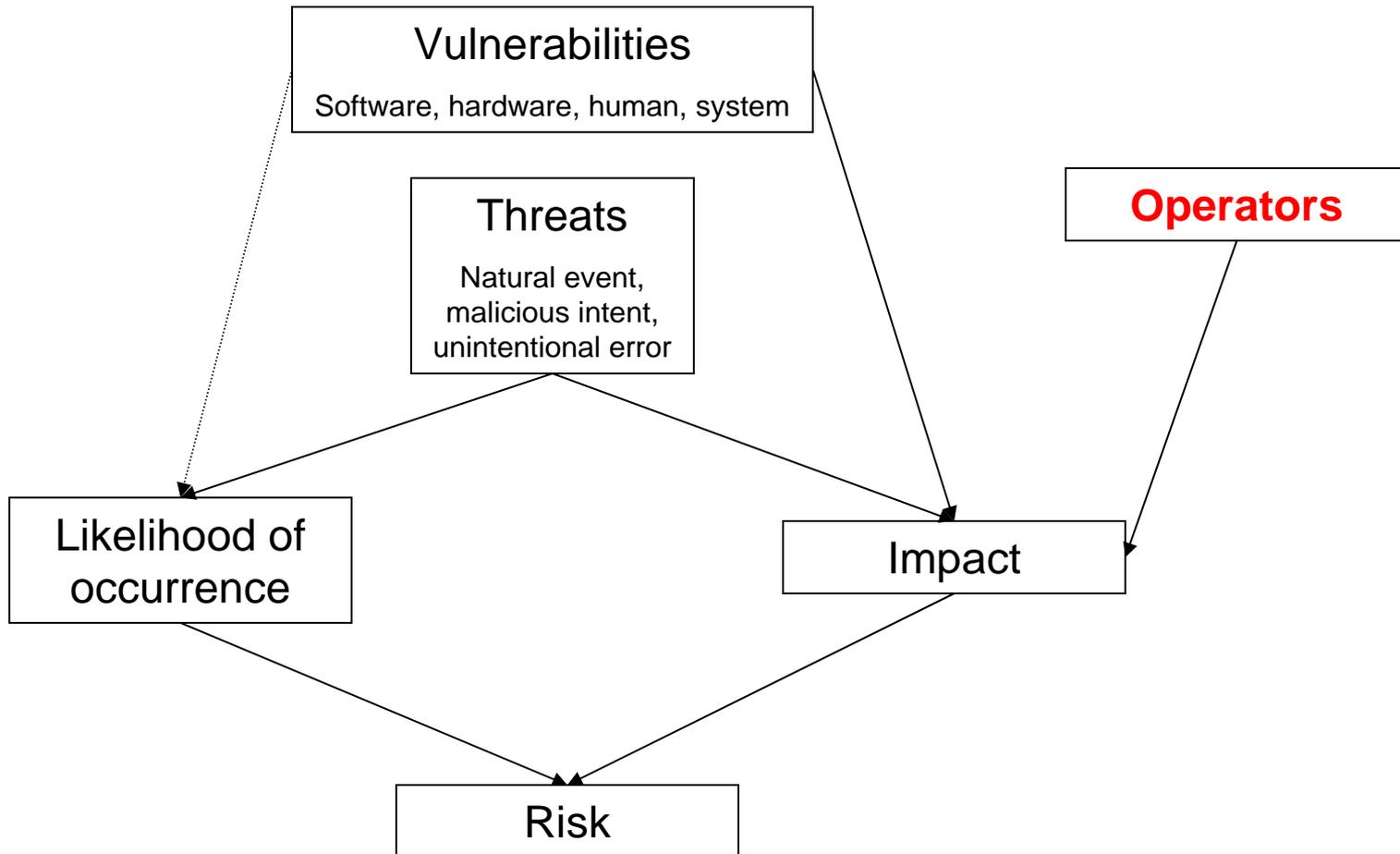
## ❖ Actual operator actions versus automated

- Operators tend to be in the loop.
- Operators must agree to suggested system dispatch.
- Operators must agree to suggested breaker opening and closings.

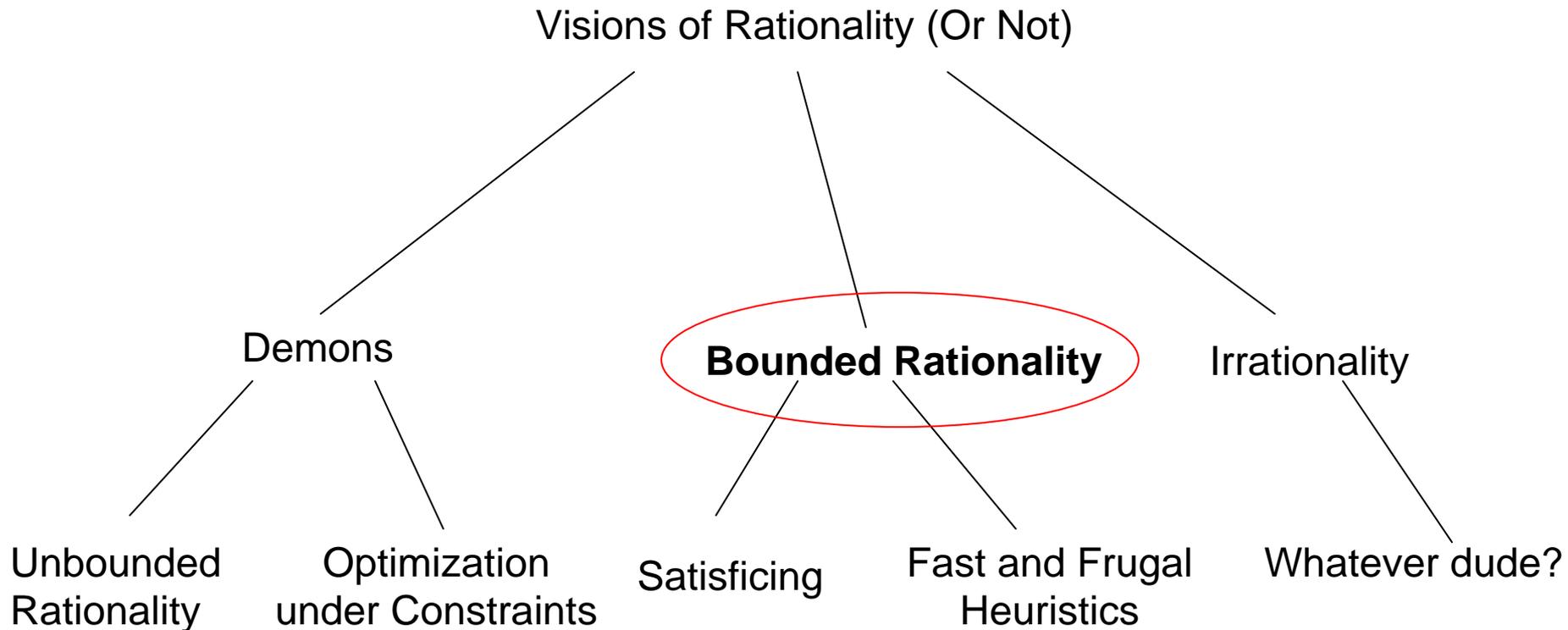
## ❖ Operator stereotype

- Two year degree. Tends not to formally calculate.
- Yearly evaluation is based on efficient running of the system

# People affect system risk



# Human decision making



# Boundedly rational decision making

- ❖ Limited time
- ❖ Limited knowledge
- ❖ Limited calculational ability
- ❖ Heuristics-and-biases notion emerged in the 1970s and emphasized how the human use of heuristics can lead to systemic errors and lapses of reasoning that indicate human irrationality.



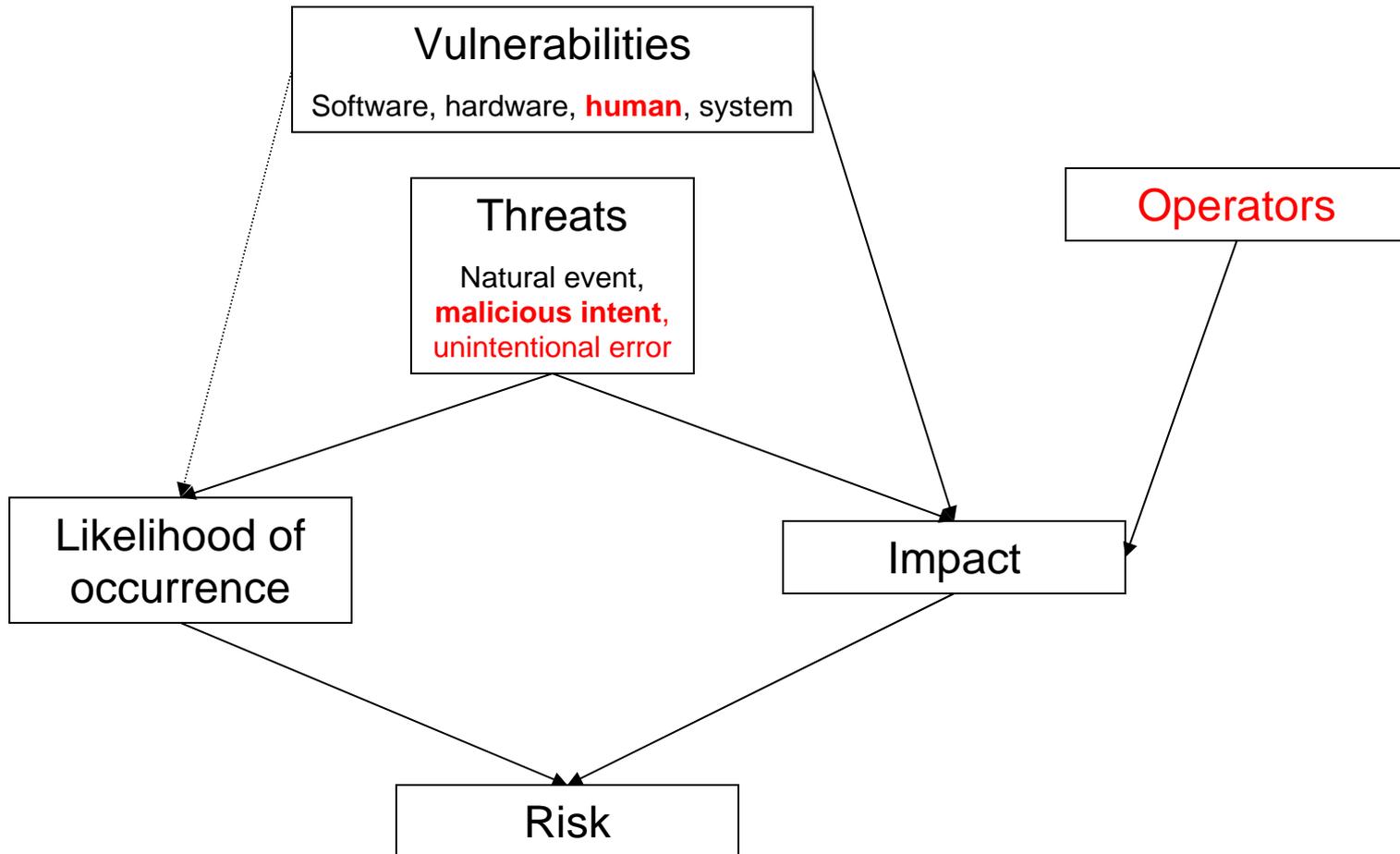
# Human heuristics and biases

- ❖ Heuristics many times succeed and sometimes fail, experimental results were typically, and incorrectly, interpreted as an indicator of some kind of fatal flaw in humans. This was usually attributed to one of three main heuristics.
  - representativeness (judgments influenced by what is typical)
  - availability (judgments based on what comes easily to mind)
  - anchoring and adjustments (judgments relying on what comes first)
  
- ❖ Aside:
  - How have we survived?
    - Maybe adapted to our environment?
    - Human heuristics, Strength and weakness

# Human heuristics and biases

- ❖ More details, experiments, and sample problems related to heuristics and biases are contained in the addendum at the end of these slides.

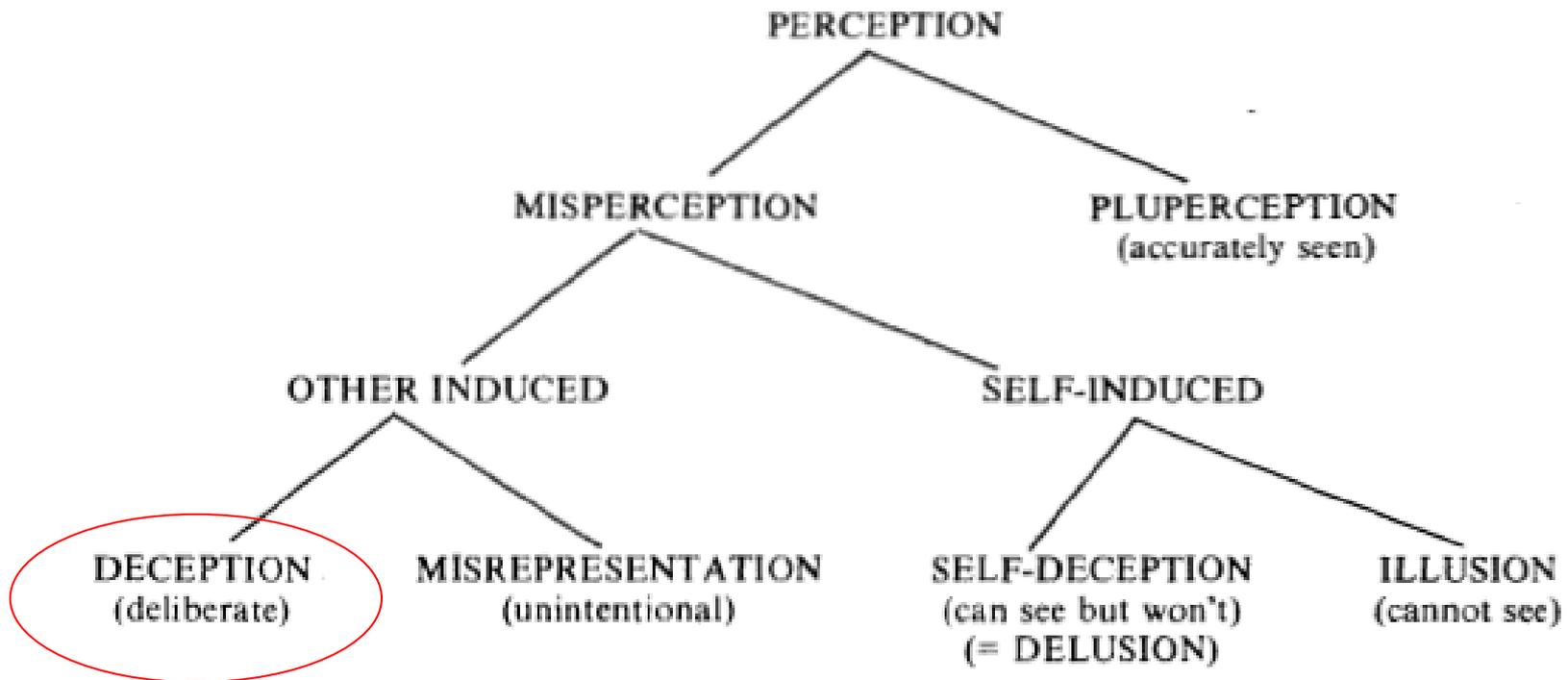
# Operators, and others, may be intentionally deceived (For the attackers benefit)





# Perception taxonomy

- Deception requires a distortion of perceived reality.



# Deception

- ❖ Those **measures** designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in manner **prejudicial to his interests** (U.S. Joint Doctrine for Information Operations )



# Deception methods

## ❖ Every deception is comprised of two basic parts

### – Dissimulation

- Hide the real.
- Purpose is to conceal or at least obscure the truth

### – Simulation

- Show the false.
- Purpose is to portray, profess, an intended falsehood

### – Both are together in every deception

- Nothing is ever just hidden; something is always shown in its stead, even if only implicitly—the man who hides leaving work early every day to drink at the local bar also implicitly displays devoting more hours to work.
- It is these two in combination that misdirect the attention and interest of the target, inducing it to form misperceptions (false hypotheses) about the real state of affairs.



# Three ways to dissimulate

## ❖ Masking

- Hides the real by making features of it invisible

## ❖ Repackaging

- Hides the real by making it appear irrelevant

## ❖ Dazzling

- Hides the real by confusing (includes information overload)

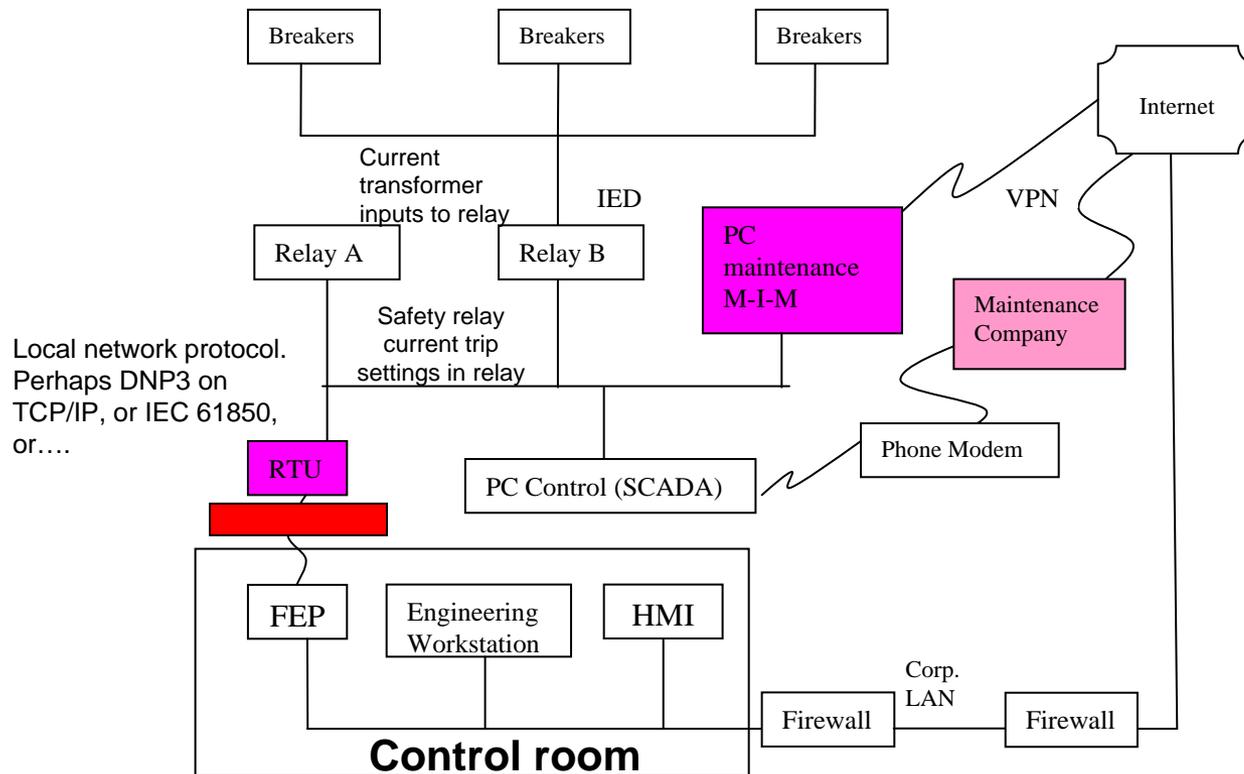
# Masking

❖ Hides the real by making it invisible.



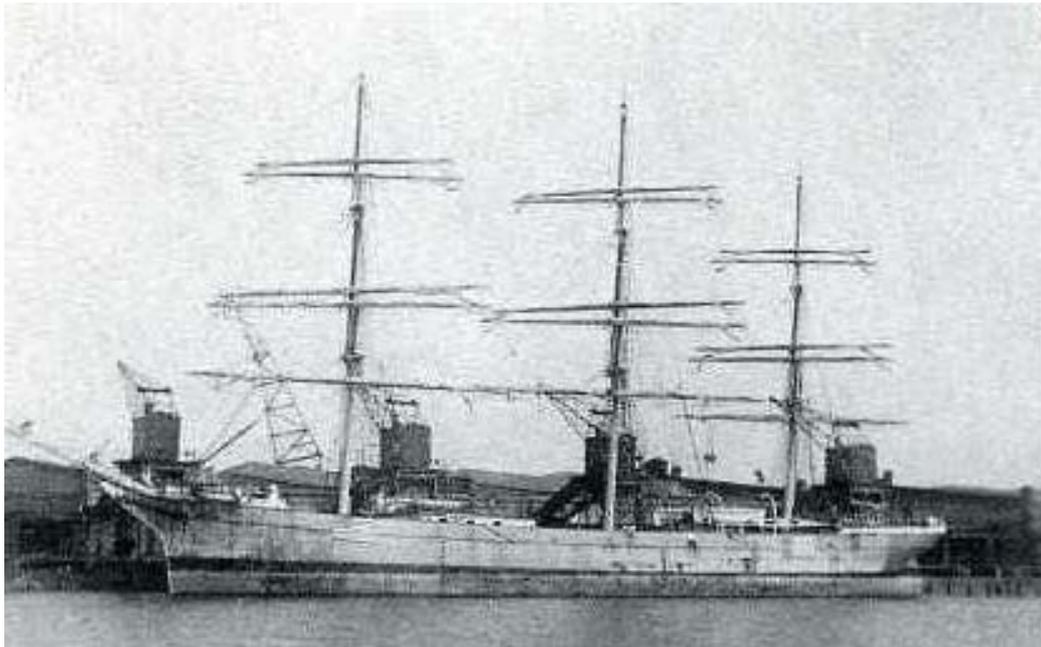
# Power grid example: masking

- ❖ In a cyber attack block all communication back to the control room.



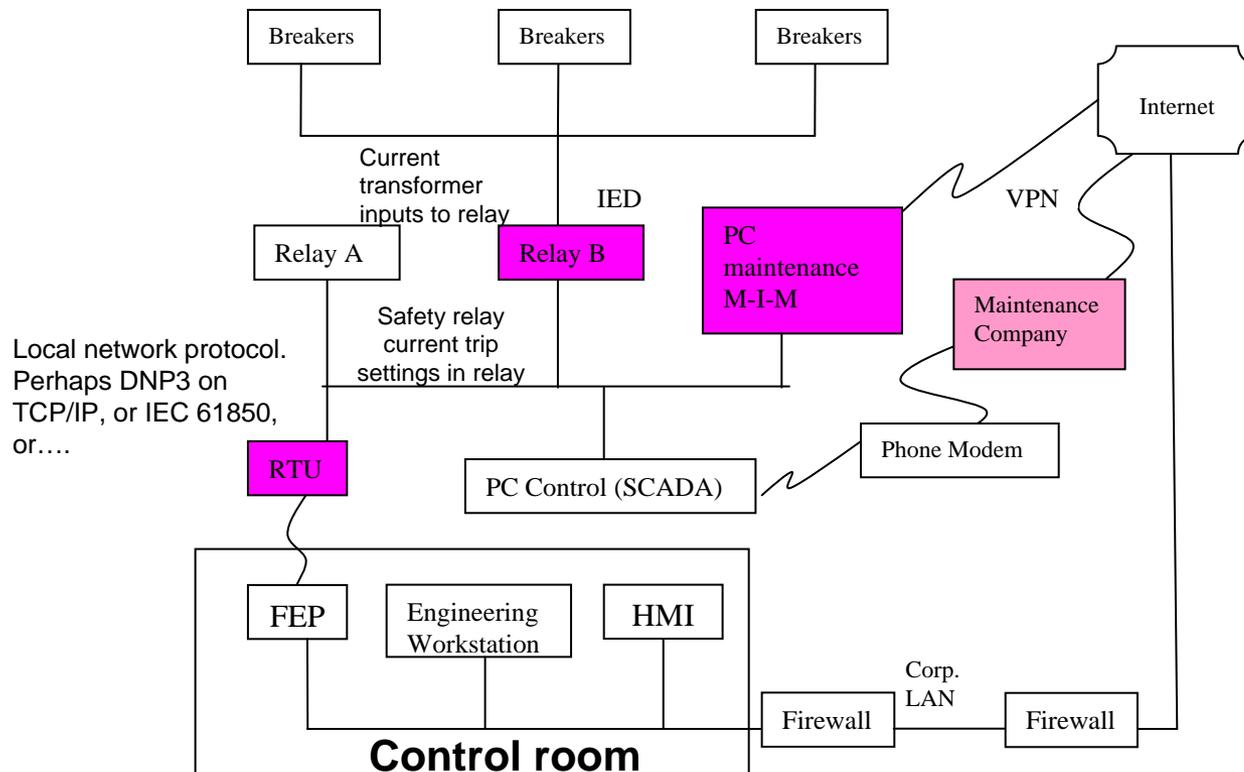
# Repackaging

- ❖ Hides the real by disguising (it is seen in this case, but seen as something falsely irrelevant)



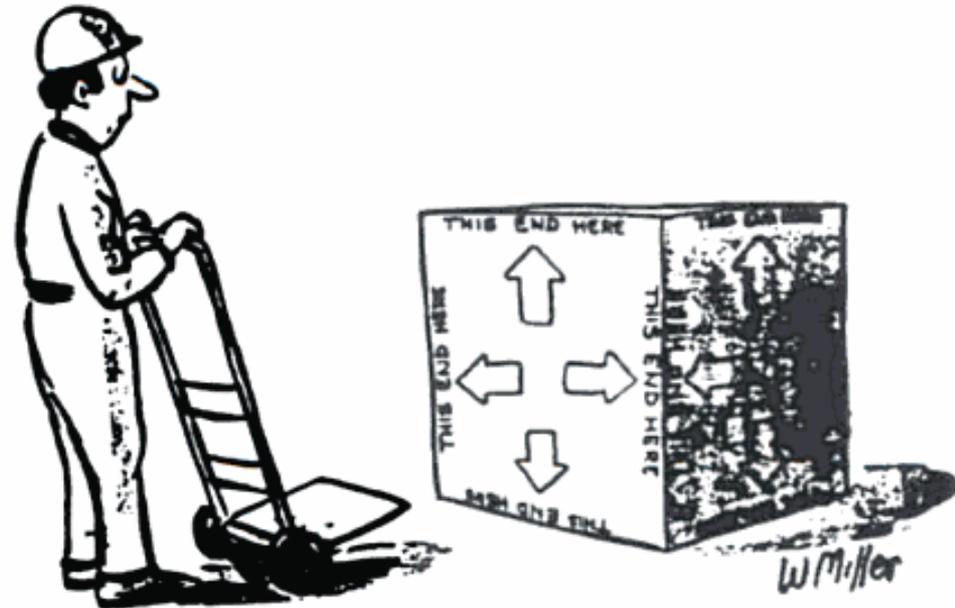
# Power grid example: repackaging

- ❖ In a cyber attack open some breakers to take a line out of service and change (lower) the power values on a parallel line reported back to the control room.



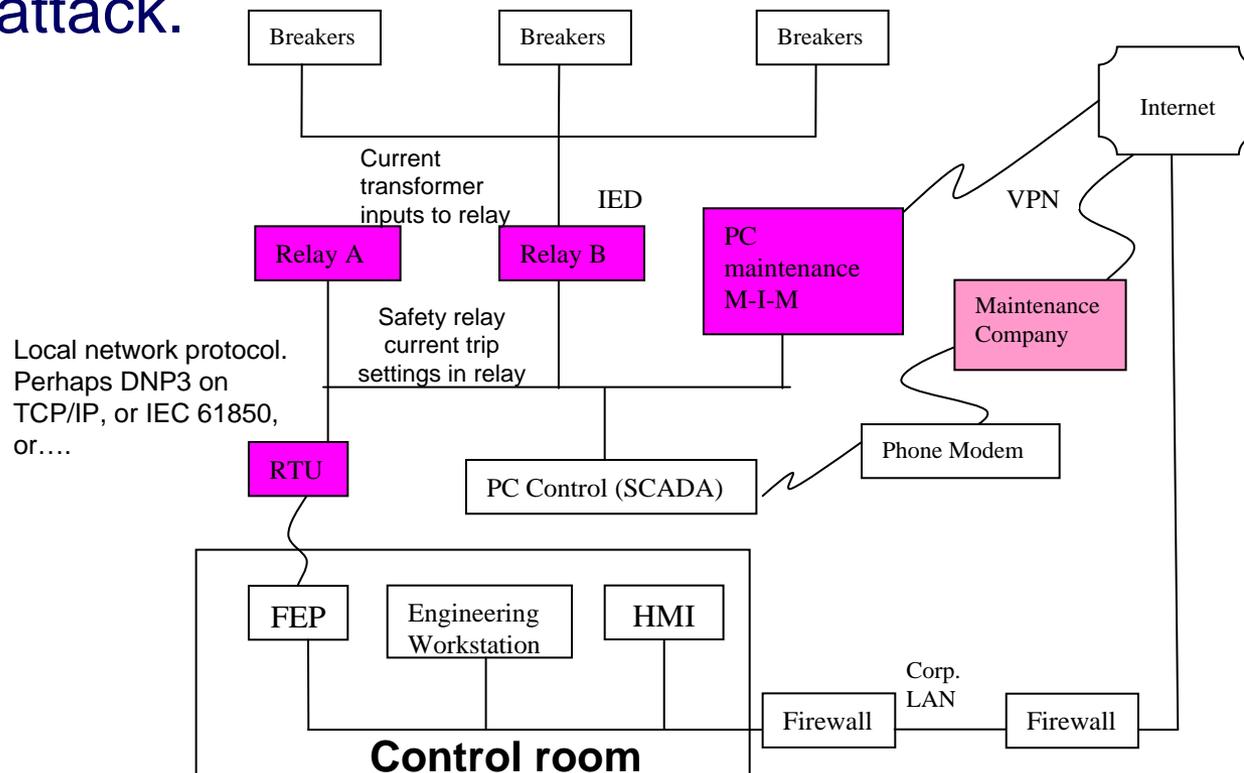
# Dazzling

- ❖ Hides the real by confusing



# Power grid example: dazzling

- ❖ In a cyber attack send randomized false breaker open and close messages back to the control room. Maybe do this for a few minutes each day for awhile to accustom the operator to intermittent system/communication problems. Then continue but also open the chosen breakers involved in the attack.



# Three ways to simulate

## ❖ Mimicking

- Shows the false by modifying its features to appear as a falsely relevant object.

## ❖ Inventing

- Shows the false by displaying a new reality. A new set of features.

## ❖ Decoying

- Shows the false by diverting attention with something which has more interesting features



# Mimicking

- ❖ Shows the false by modifying its features to appear as a falsely relevant object.





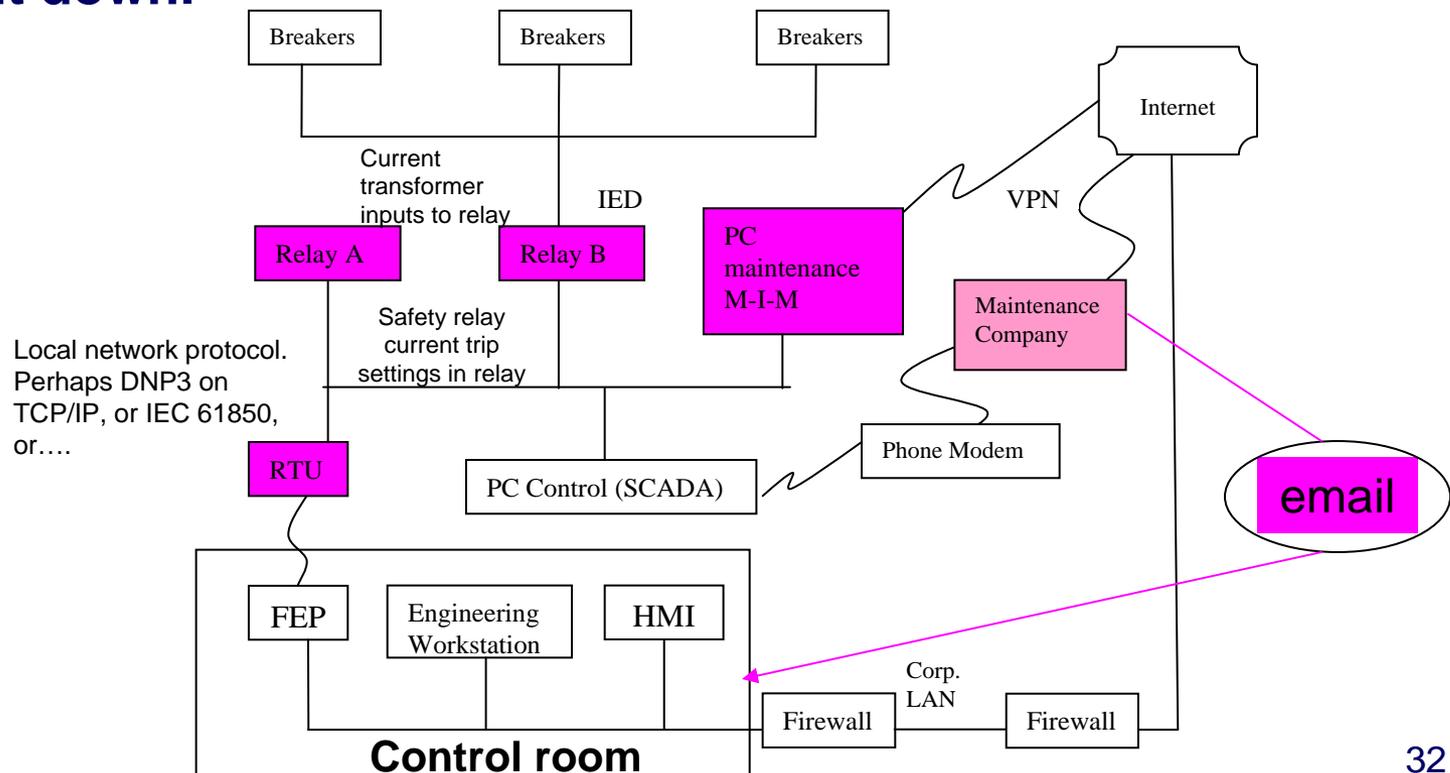
# Inventing

❖ Shows the false by displaying a new reality



# Power grid example: inventing

- ❖ In a cyber attack open some breakers to take a line out of service and lower the power values on a parallel line reported back to the control room (so far this is the repackaging scenario). **A little beforehand, spoof an email to the operators as though it is from the maintenance department letting them know that they are going to be doing maintenance on the line and will be taking it down.**



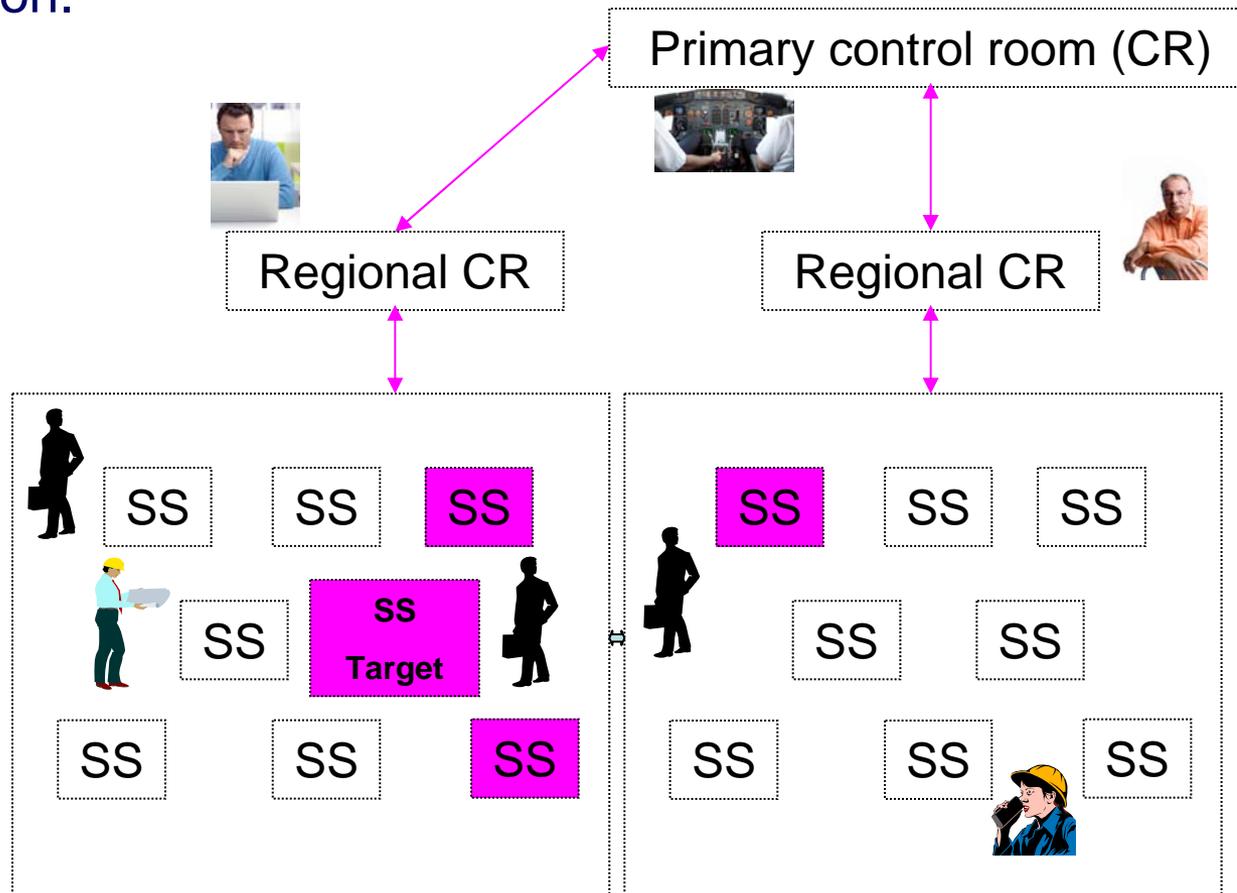
# Decoying

- ❖ Shows the false by diverting attention with something which has more interesting features



# Power grid example: decoying

- ❖ In a cyber attack trip some breakers at a potentially important set of substations--Perhaps in a set of substations supplying power to a nuclear plant. In parallel trip the breakers in the targeted substation.

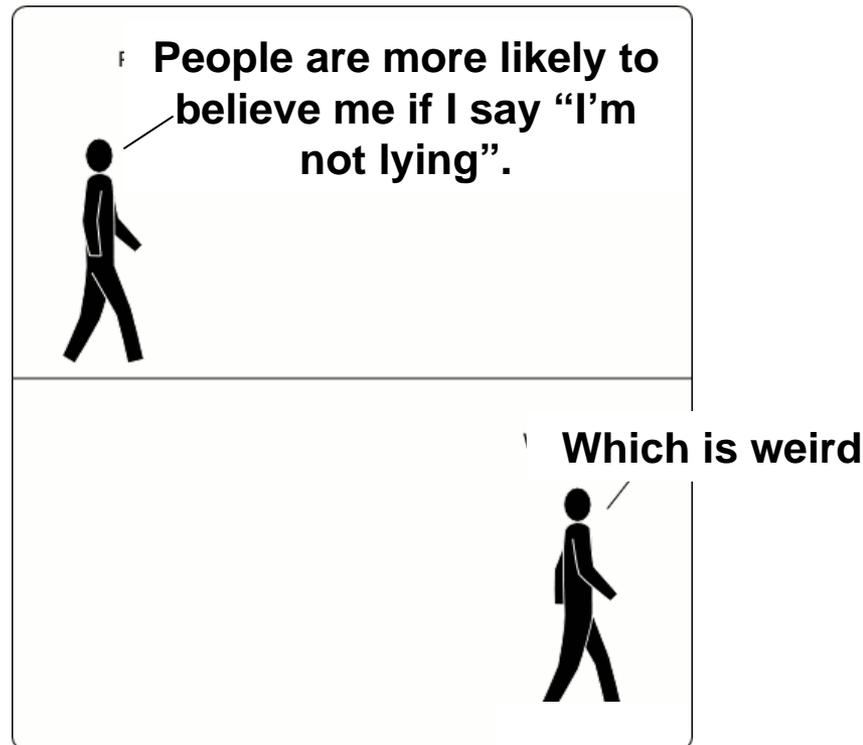


# Recap: Deception methods

- ❖ Every deception is comprised of two basic parts
  - Dissimulation
    - Masking, repackaging, dazzling
  - Simulation
    - Mimicking, inventing, decoying
  - Both are together in every deception

# A bit about lying (a special case of deception)

- ❖ To **make a believed-false statement** to another person, with the intention that that other person believe that statement to be true, violating that person's right of liberty of judgment, with the intention to **harm that other person**.





# Pan-cultural belief cues about lying

- ❖ 71.5 % Liars avoid eye contact
- ❖ 64.8% Liars touch and scratch themselves
- ❖ 62.2% Liars tell longer stories than usual
- ❖ All of this would be less puzzling if we had more reason to imagine that these cues actually work
  - Large body of work calls these cues into question
  - Judgments of deception are frequently wrong

# Accuracy in detecting lies

- ❖ Judgments about lying are associated with stereotypes
- ❖ Stereotypes focus on behavioral cues
- ❖ People are generally not very accurate in detecting lies from behavioral cues

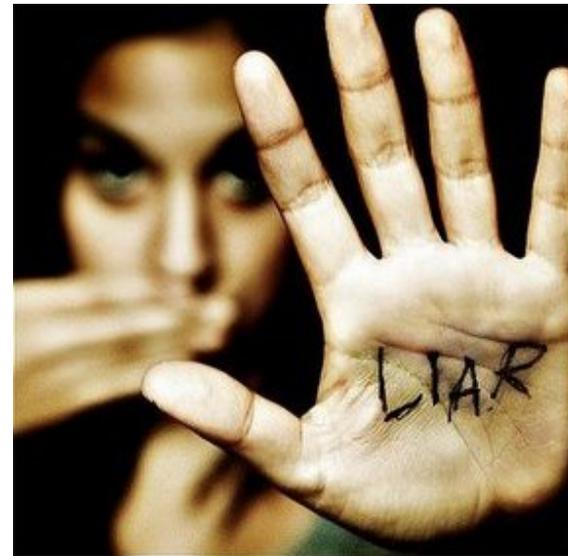
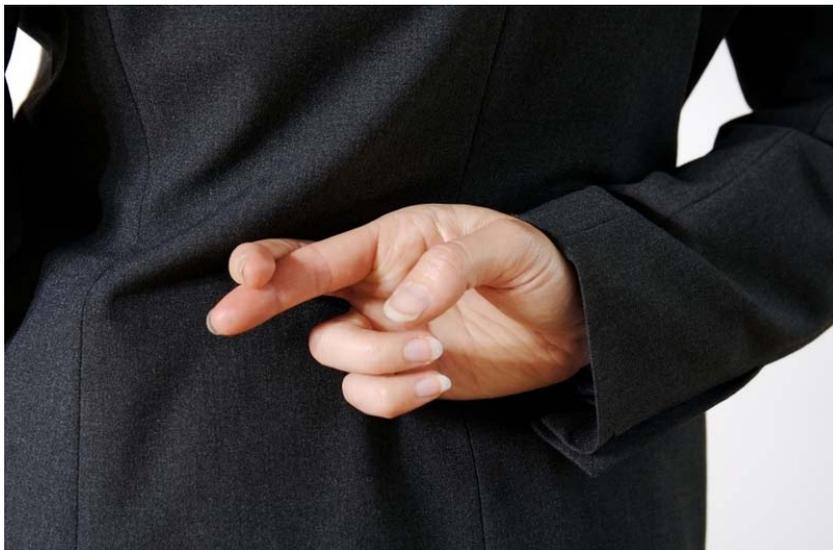


- ❖ So how is lying ever accurately detected?
  - Third party information
  - Confessions
  - Physical evidence



# Does lie detection training help?

- ❖ With training, knowledge test results improve.
  - Understanding of deception has improved
- ❖ Actual detection results do not appear to improve much, if at all.
- ❖ Although, with more at stake the results may improve.



# Social engineering

❖ **Social Engineering** is **attacking or penetrating a system by tricking or subverting operators or users**, rather than by means of a technical attack. More generally, the use of fraud, spoofing, or other **social or psychological measures** to get legitimate users to break security policy.  
Handbook of Information security by Hossein Bidgoli

❖ **Social engineering** is the act of **manipulating people into performing actions or divulging confidential information**. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.  
[http://en.wikipedia.org/wiki/Social\\_engineering\\_%28security%29](http://en.wikipedia.org/wiki/Social_engineering_%28security%29)

# Humans are integral to system function

## Power grid example



Business proposition



Operations and maintenance

Primary control room (CR)

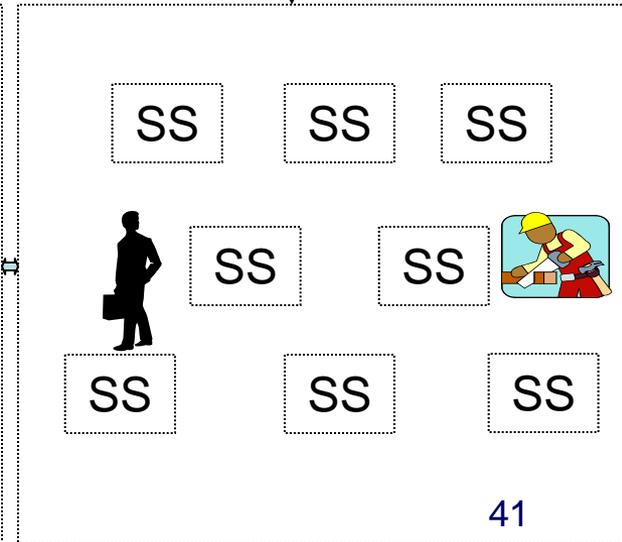
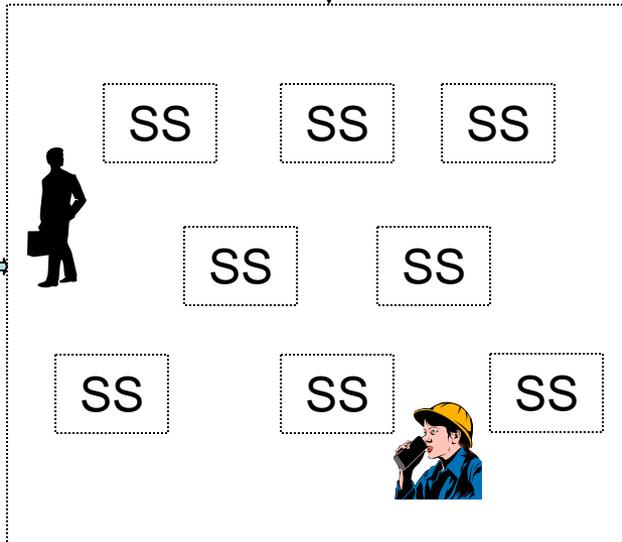
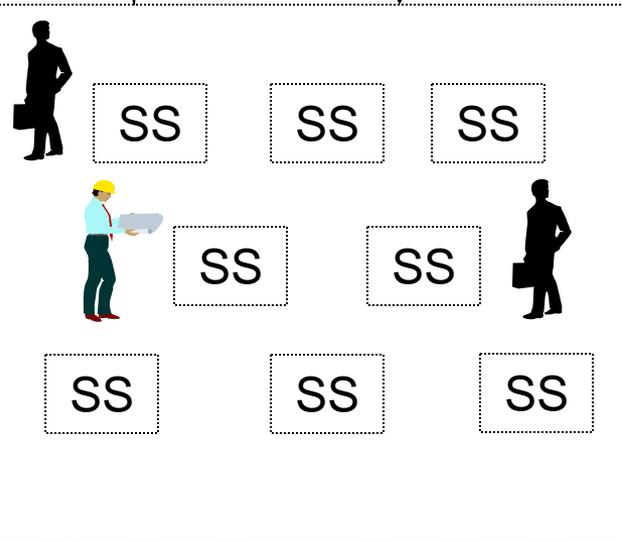


Regional CR

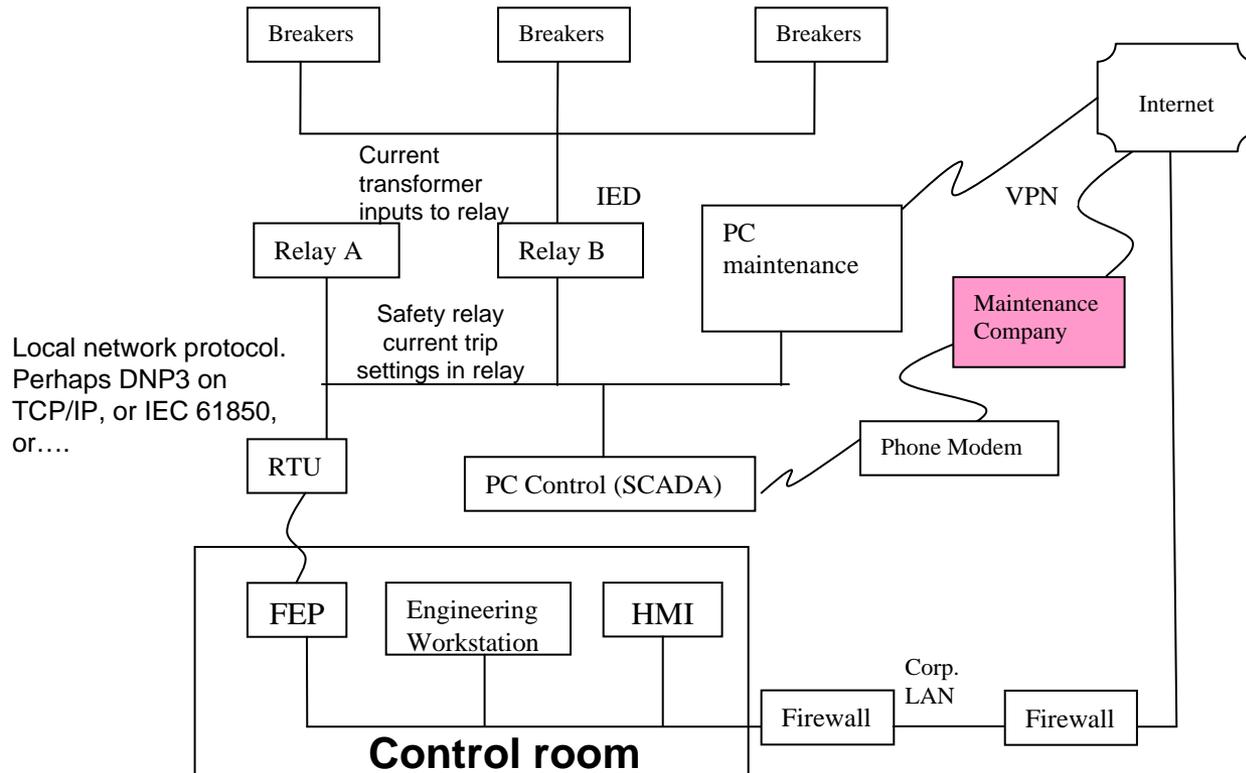
Regional CR



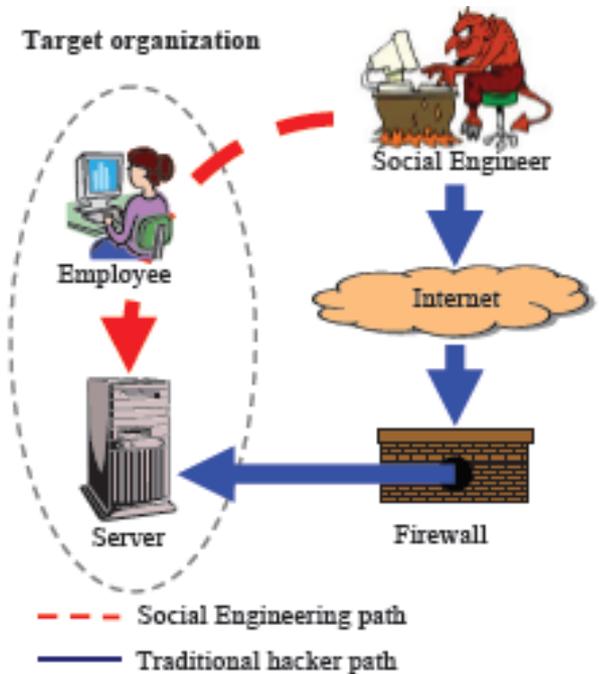
Regional CR



# Notional communications



Local network protocol. Perhaps DNP3 on TCP/IP, or IEC 61850, or....



M. Hermansson, R. Ravne, "Fighting Social Engineering", University of Stockholm / Royal Institute of Technology, March 2005

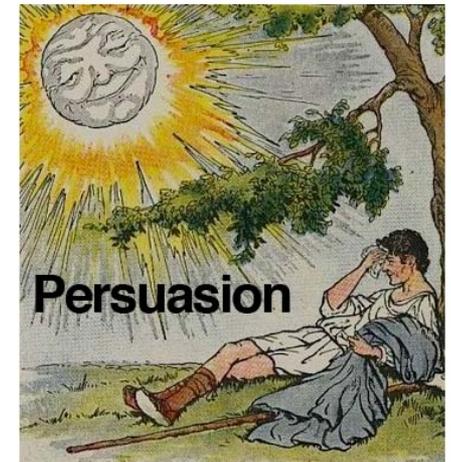


# People influencing principles to support a deception

## ❖ A few influencing mechanisms

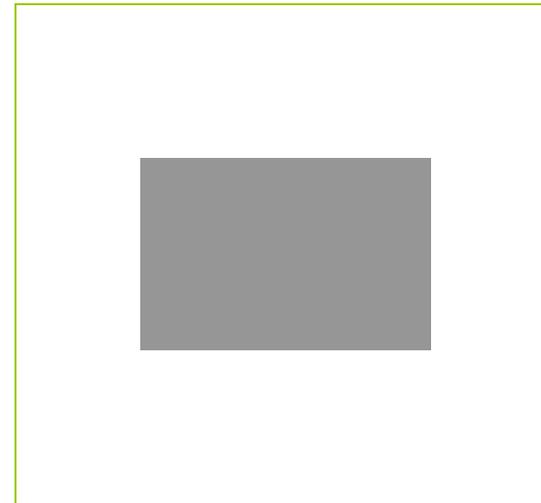
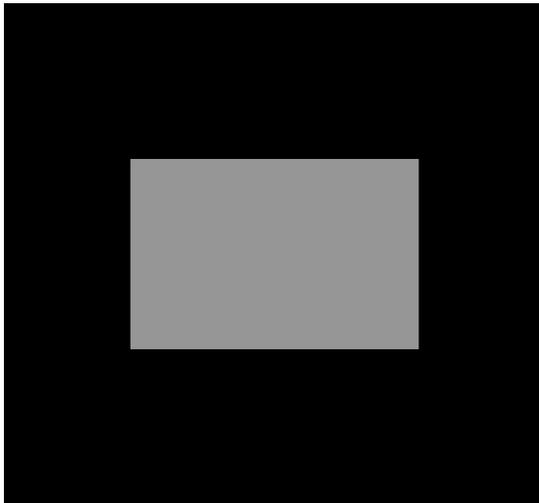
- Perceptual contrast
- Reciprocation
- Consistency and Commitment
- Social proof
- Liking
- Authority
- Scarcity

A Question Of Influence



# Perceptual contrast

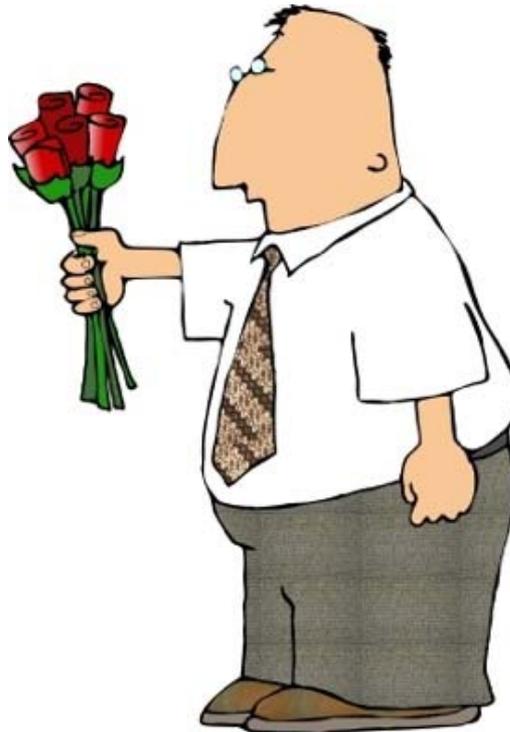
- ❖ There is a principle in human perception that effects the way we see the difference between two things that are presented one after another.
  - If the second item is fairly different from the first, we will tend to see it as more different than it actually is. E.g. if we lift a light object first and then lift a heavy object, we will estimate the second object to be heavier than if we had lifted it without first trying the light one.





# Reciprocity

- ❖ We are human because our ancestors learned to share their food and their skills in an honored network of obligation (Richard Leakey).
  - As a result there is a lowering of the natural inhibitions against transactions that must be begun by one person providing personal resources to another.



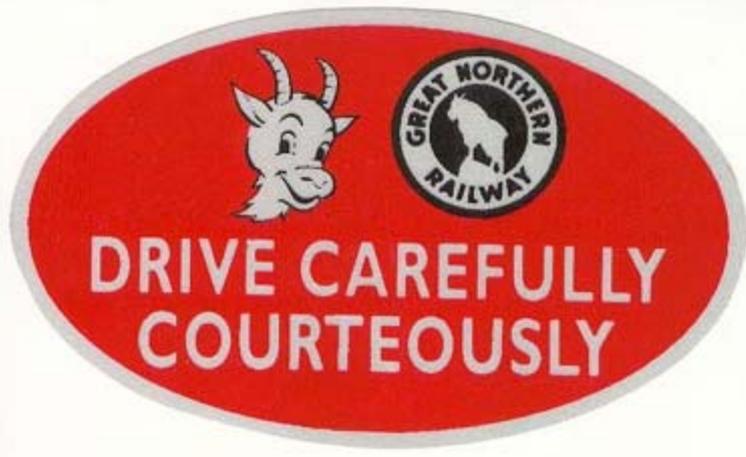
# Perceptual contrast and reciprocity (rejection-then-retreat)

- ❖ Make a larger request of someone that they most likely will turn down, then if they turn you down make a smaller request which you were interested in all along.
- ❖ If you have structured the requests skillfully, the second request should come across as a concession and they should feel inclined to respond with a concession of their own.



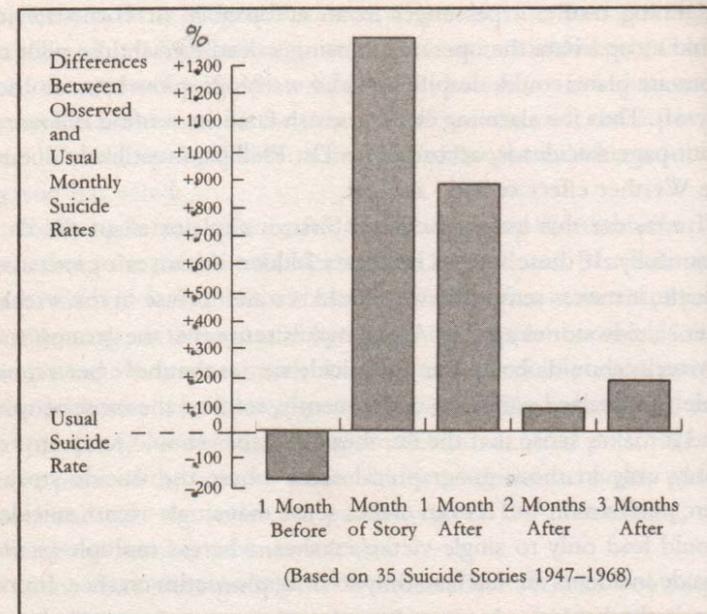
# Consistency in commitment

- ❖ Once a person has made a choice or taken a stand, they will encounter personal and interpersonal pressures to behave consistently with that commitment.
  - Start with a little request and gain the commitment. Later, go for the larger request.



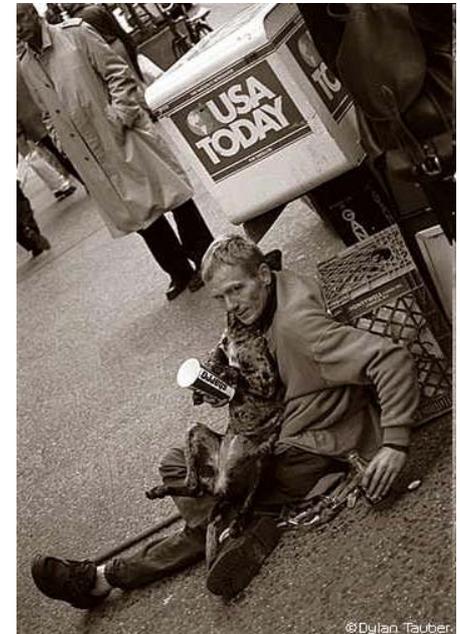
# Social proof

- ❖ People tend to believe that an action is more appropriate if one or more others have previously or are currently doing it.



# Liking

- ❖ People prefer to say yes to the requests of people they like.
  - Good looking people have an advantage in social interaction
  - We like people who are similar to us.
  - We tend to like people and products associated with things we like.



# Authority

- ❖ To varying degrees, people demonstrate a tendency towards obedience to authority.



# Scarcity

- ❖ Opportunities seem more valuable to us when their availability seems limited.
  - Employees time
  - Product availability
  - Information

**LIMITED-TIME OFFER:**  
DELUXE ROOM & SHOW TICKET PACKAGES



**INCLUDES:**

- **2 NIGHTS** AT MANDALAY BAY
- **2 TICKETS** TO DISNEY'S **THE LION KING** AT THE MANDALAY BAY THEATRE
- **\$100** CABANA CREDIT
- **COMPLIMENTARY CHILD ADMISSION** TO SHARK REEF AQUARIUM FOR EACH PAID ADULT

PRICES INDICATED ARE COLOR-CODED TO REFLECT PLACEMENT IN THEATER SEATING CHART



# People influencing principles to support a deception

## ❖ A few influencing mechanisms

- Perceptual contrast
- Reciprocation
- Consistency and Commitment
- Social proof
- Liking
- Authority
- Scarcity



## Social engineering training and awareness

- ❖ Concern for increasing efficiency of INL's social engineering training and awareness program.
- ❖ Continuously evolving process.
- ❖ Focus on evolving the training programs to enhance reduction of employee susceptibility to social engineering attacks.

“The only thing constant in life is change”



# March-08 -- phone based phishing

- ❖ Attacker: **Female**, field services, with **nice voice** calls from her personal cell phone
- ❖ 45 employees contacted

## Conversation (Rough cut):

- John? This is Julia from the opscenter. **Management is having us** deploy a new system to **help employees** recover their passwords if forgotten. **To get this working for you**, we need your password so if **you just give it to me now I will enter it and you will be all set up for Monday.**
- Yes, we could reset and **force you** to change the password yourself but **it is just easier for you**, and me, if I put it in for you—that's what **everyone else has been doing**. We don't want you **not being able to login on Monday** (You know how it is, things do go wrong!).

•Perceptual contrast

•**Reciprocation**

•Consistency and  
Commitment

•**Social proof**

•Liking

•**Authority**

•Scarcity



# March-08 -- phone based phishing

## Result Summary:

- 18 out of 45 (40%) employees provided their password to the fake ops center employee.
- 4 employees did realize the mistake and contacted the OpsCenter to get their passwords immediately changed.
- 17 out of 45 (38%) employees called and reported the incident to the OpsCenter.
- The first call to the OpsCenter was placed 45 minutes into the exercise.

# July-08 -- Road apples

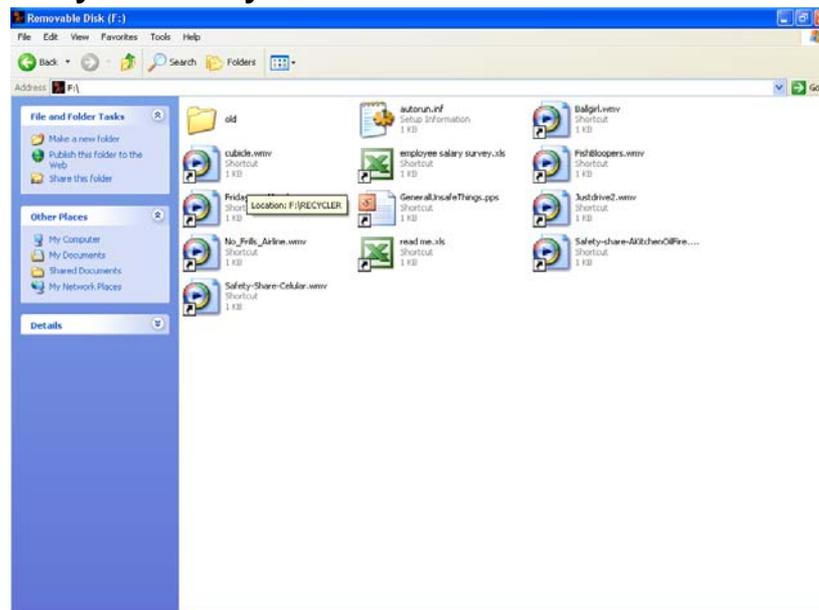
- ❖ 50 thumb drives were distributed in parking lots, around picnic tables, sidewalks, benches, ...
- ❖ Thumb drive included an autorun.inf file and an executable.

Autorun.inf:

```
[autorun]
```

```
icon=lilguy.ico
```

```
shell\open\command=old\salary_survey.xls.exe
```



# July-08 -- Road apples

## Result Summary:

- 34 out of 50 (68%) employees turned in the thumb drives.
- 10 out of 50 (20%) employees placed the thumb drive into their computer.
- 6 out of 50 (12%) are unaccounted for.

# December-08 -- Phishing E-mail

"hm Moore@security.gov" <hm Moore@security.gov> 07/10/2009 02:52 PM

To "miles.mcqueen@inl.gov" <miles.mcqueen@inl.gov>  
Cc

Subject: Oregon woman loses 400,000 to Nigerian E-Mail scam

Security Alert- New wave of targeted Nigerian E-Mail scams!!

Fox News reports:

Oregon Woman Loses \$400,000 to Nigerian E-Mail Scam

SWEET HOME, Ore. An Oregon woman who is out \$400,000 after falling for a well-known Internet scam says she wasn't a sucker or an easy mark.

Janella Spears of Sweet Home says she simply became curious when she received an e-mail promising her \$20.5 million if she would only help out a long-lost relative identified as J.B. Spears with a little money up front.

*Please read the attached complete story.*

Security wants to remind you to always be vigilant.

H. M. Moore

CSO

hm Moore@security.gov

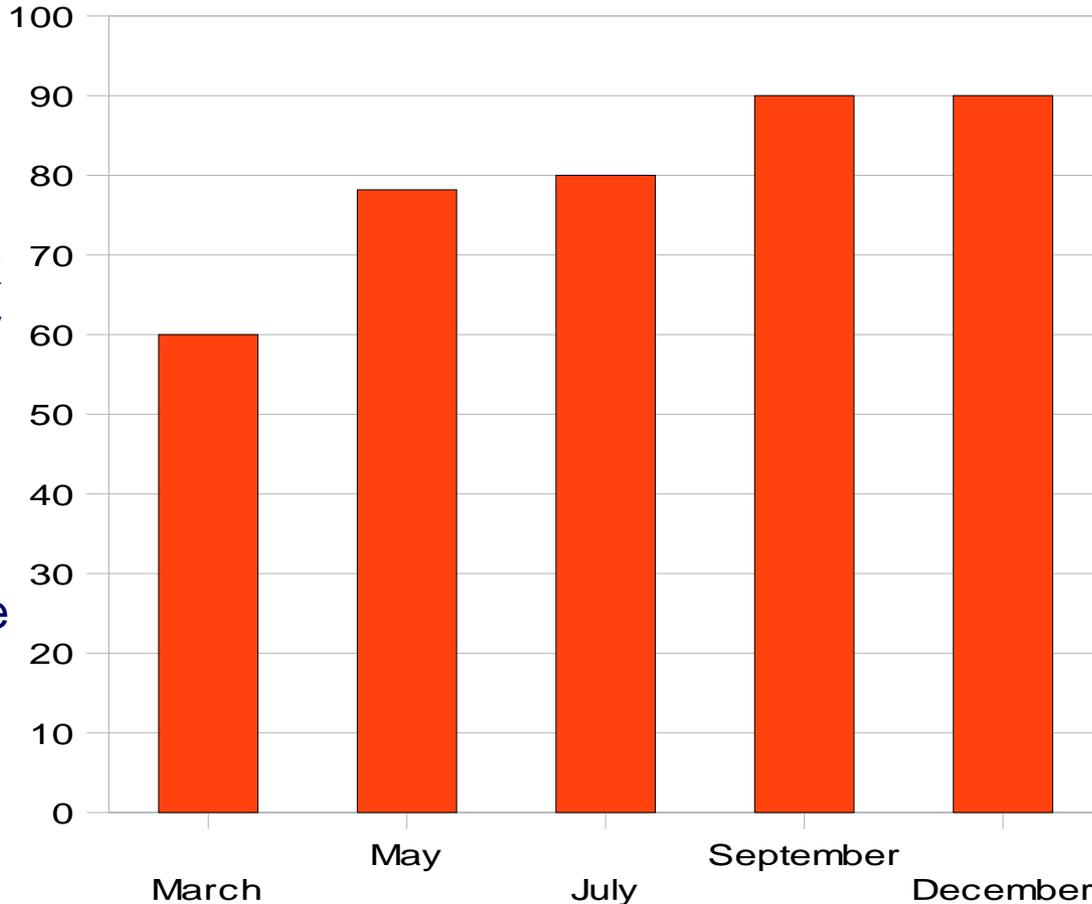
# December-08 -- Phishing E-mail

---

## Result Summary:

- 201 out of 1934 (10%) employees opened the attachment.

# Has the INL social engineering training and awareness program helped?



Perhaps...But think of the experimenter being evaluated on performance.

Is it possible we are being deceived?

% Correct Responses to INL Tests

# Human vulnerabilities: Strength and weakness

- ❖ It would be wrong simply to equate human vulnerabilities with “undesirable behavior.”
- ❖ A characteristic or behavior that leads to a security breach in a specific context may be highly desirable in another (for instance, being helpful to customers, or trusting a colleague).



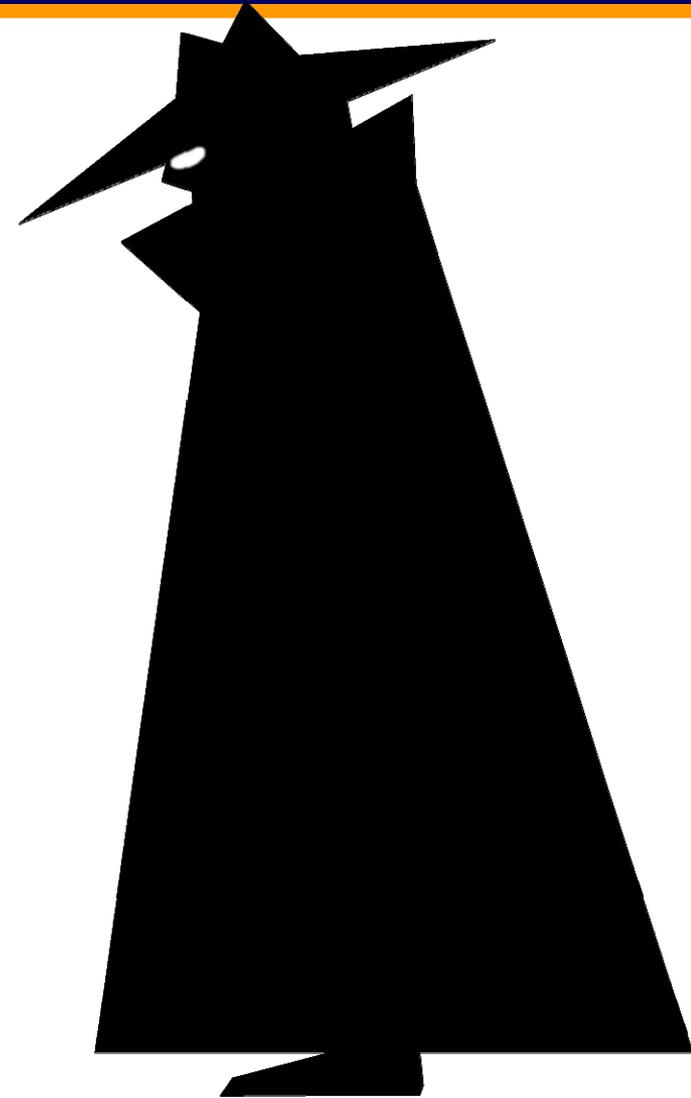
# Managing human vulnerabilities and their impacts

- ❖ To effectively manage human vulnerabilities, all stakeholders need to be involved in the design and operation of secure systems.
  - Effective security must acknowledge that every human within an organization has the capability to become, or aid, an attacker.
  - Unacknowledged vulnerabilities may cause systemic failures. Human vulnerabilities need to be identified and managed before they lead to an actual breach of security.
  - The potential impact of human vulnerabilities on systems is due to ineffective design of systems and management of people.

# Social engineering summary

Technical systems have vulnerabilities, and so do humans.

Attackers may focus on social engineering attacks – if we could effectively train the stakeholders then the attack is less likely to work

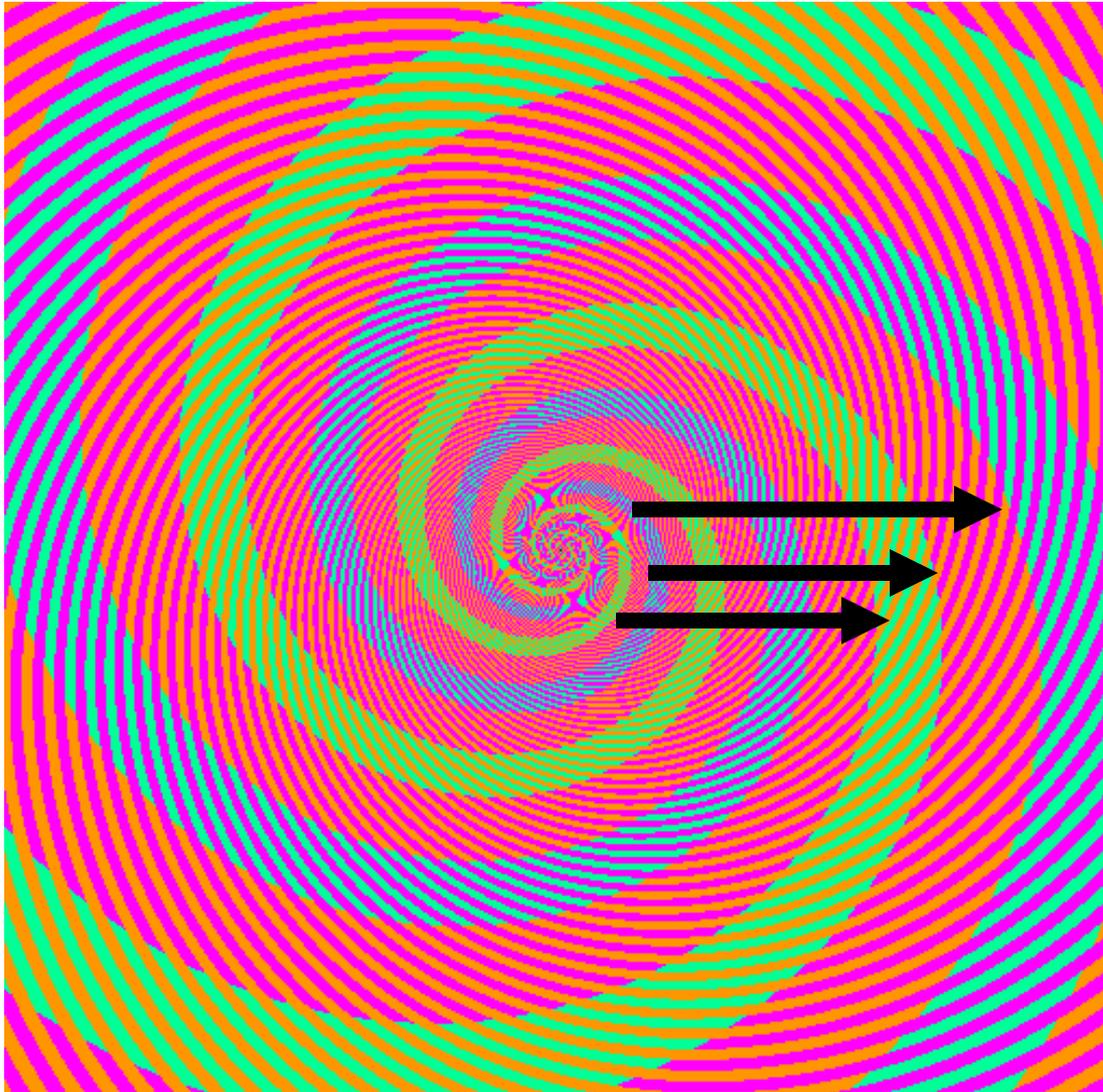




# Secure and resilient control systems?

- ❖ **How do we design, build, and operate infrastructure systems to be secure and resilient given that they, their operators, and users have vulnerabilities which may be exploited by an adversary?**
  
  - ❖ **What is the appropriate role of humans?**
    - Users themselves are often perceived as being the “weak link” in the security chain, as many neglect to adopt or correctly use the most basic security measures.
- Bruce Schneier, *Secrets and Lies*, John Wiley and Sons, 2000

# Discussion: After lunch gentle wakeup



Invent an algorithm.

How many spirals of each color? **Number crossed + 1**

Blue: 2?

Green: 2?

Pink: 4?

The above answers are **incorrect**. The correct answers are:

Blue: 0

Green: 0

Green-Blue: 4

Pink: 4

See handout for **explanation**.

# Break time

## Discussion?

Break time: 2:30pm – 3:00pm

Session 4: Human Systems

# ISRCS 2009

## Contact

Miles McQueen	amm@if.uidaho.edu or Miles.McQueen@inl.gov	( 208) 526-5872
---------------	--	--------------------

## Heuristics and Biases Addendum

# Attackers view

- ❖ The heuristics and biases research suggests that ordinary people are cognitive misers who use little information and little cognition, and thus are largely unable to estimate probabilities, risks, or maximize their happiness.
- ❖ Attackers may actively position their adversary to make errors in judgment.
  - Position the defender's heuristics to yield bad results (Takes imagination and effort but what more could an attacker want...)

# Examples of heuristics

- ❖ Representativeness
- ❖ Availability
- ❖ Anchoring and adjustments
- ❖ Recognition
- ❖ One good reason
  - Many heuristics here...
  
- ❖ Many other proposed heuristics and biases

# Representative heuristic

- ❖ The greater the match of some of an event or object's attributes to our image of a category the greater is our assessed likelihood of the event or object belonging to the category.
- ❖ **Experiment. Linda is thirty-one years old, single, outspoken and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in anti-nuclear demonstrations. Rank the following statements about Linda in terms of how likely each is to be true.**
  - a. Linda is a teacher in an elementary school
  - b. Linda works in a bookstore and takes yoga classes
  - c. Linda is active in the feminist movement
  - d. Linda is a psychiatric social worker
  - e. Linda is a member of the League of women voters.
  - f. Linda is a bank teller.
  - g. Linda is an insurance salesperson
  - h. Linda is a bank teller and is active in the feminist movement.

**Many people mistakenly place h above f.** People seem to average the two probabilities instead of multiplying them.

- ❖ **Note: this leads to the following type of error: When the attacker tells someone something very implausible, it is much more likely to be believed if the attacker tells the same person something very plausible.**

# Availability heuristic

- ❖ The more easily examples come to mind, the greater the assessed likelihood of the event.
- ❖ An experiment. Think of four pages in a novel with about 2,000 words. One group of students was asked “How many words would you expect to find that have the form \_ \_ \_ \_ ing?”. **Average guess: 13.4 words.**
- ❖ Another group of students was asked “How many words would you expect to have the form \_ \_ \_ \_ \_ n \_ ? “. **Average guess: 4.7 words.**

**Note:** This type of experiment has been repeated in many different forms yet the result is the same. The more easily (not the absolute number of) examples come to mind the greater the assessed likelihood.

# Anchoring and adjustment heuristic

- ❖ To answer a question or assess a likelihood you start with a number you know and then adjust. There end up being two problems. The first is that the adjustment is rarely enough. The second and more astounding is that the starting number may have no relationship to the question.
- ❖ An experiment. People were asked what percentage of African nations were in the United Nations, but before answering they were given a percentage and asked whether it was higher or lower than the actual percentage. The average estimate by subjects who were started at 10% was 25%, while those started at 65% averaged 45%.

**Note: This heuristic provides great opportunity for manipulation.**

# Recognition heuristic

- ❖ If one of the object is recognized assume the recognized object has the higher value.
  - Sometimes people benefit from ignorance
  - This heuristic is domain specific in that it only works in environments where recognition is correlated with the criterion.
    - Genetically coded
    - Learned from experience
- 1. Which English soccer team will win?
  - 50 Turkish students and 54 British students made forecasts for all 32 English FA Cup 3rd round soccer matches. (1997). The Turks knew very little about the English teams, while the Brits knew quite a lot. The Turks made predictions that were nearly as accurate as those of the English (63% versus 66%). English teams are usually named after English cities so people can use city recognition heuristic as a cue for soccer performance. Cities with successful soccer teams are likely to be larger and thus more likely to be recognized. Empirical evidence indicates that the Turks used the recognition heuristic: Among the pairs where one team was recognized but the other was not, the former team was chosen 627 times out of 662 cases (95% of the time).



# Just one good reason heuristic

- ❖ This is a set of heuristics that define a single reason to make a selection and then uses that reason.
  - Take the Last
    1. If applicable use the recognition heuristic
    2. Not so Random search: **Choose the cue that seemed to help on the last selection on a problem that seems similar.** Determine if that accentuates one of the objects for you. If it does then select it.
    3. Otherwise go back and select another cue.

## Heuristics and biases Sample problems

# Sample problem 1

- ❖ Assume that the following is true: 'If the 500kv breaker is open, then the 230kv breaker is closed.' Or 'If the 500kv breaker is not open then the 230kv breaker is closed. ' But not both of these if-thens are true.
- ❖ What can you infer from these assumptions?

## Sample problem 2

- ❖ Intuitively, in typical English text, are there more words that begin with *k*, or are there more that have *k* as their third letter?

## Sample problem 3

- ❖ In Milan there are two cab companies, the blue cabs, which own 85 percent of the cabs, and the green cabs which own the other 15 percent. A cab is involved in a hit-and-run accident and a witness says she thought it was a green one. Tests were made and it was found she could correctly identify the color of the cab 80 percent of the time in the lighting condition under which the accident took place; the rest of the time she mistakenly thought a blue cab was green, or vice versa. Is the Milan cab that was involved in the crash more likely to have been blue or green?



## Sample problem 4

- ❖ Order the cities by population
  - Dhaka
  - Hanoi
  - Milan
  - Santiago

## Heuristics and biases Sample problem solutions

# Discussion: sample problem 1

- ❖ Assume that the following is true: 'If there is a king in the hand, then there is an ace in the hand.' Or 'If there is not a king in the hand, then there is an ace in the hand.' But not both of these if-thens are true. What can you infer from these assumptions?

Answer:

- ❖ To be false an implication must have the predicate be TRUE and the consequence be FALSE.
- ❖ We know that at least one of the implications must be false. This implies that exactly one implication is true and one is false (to be false the predicate must be true and we can't have both a king in the hand and a king not in the hand).
- ❖ Whichever implication is false will have the predicate true and the consequence false. Since the consequence is the same for each implication we know that there ISN'T an ace in the hand.

## Discussion: sample problem 2

- ❖ Intuitively, in typical English text, are there more words that begin with *k*, or are there more that have *k* as their third letter?

### Answer

- ❖ More have *k* as the third letter.
- ❖ For all length words, about twice as many have *k* in the third position as opposed to the first position.
- ❖ Looking at the relevant paper in cognitive psychology by Tversky and Kahneman they indicated that this is true for all words found in typical English text (Investigating a bit further, the study by Mayzner et al indicated 200 words from each of 100 different sources—newspapers, magazines, books—for a total sample of 20000 words).
- ❖ In general most people state that there are more words that have *k* as the first letter than as the third letter. The reason is that it is easier to recall (i.e. lookup) words in our memory that begin with *k* (or any other letter for that matter) than words which have *k* as their third letter. We naturally assume that things that come more easily to mind are things we have more frequently encountered—an assumption which ignores how we store and process information.

## Discussion: sample problem 3

- ❖ In Milan there are two cab companies, the blue cabs, which own 85 percent of the cabs, and the green cabs which own the other 15 percent. A cab is involved in a hit-and-run accident and a witness says she thought it was a green one. Tests were made and it was found she could correctly identify the color of the cab 80 percent of the time in the lighting condition under which the accident took place; the rest of the time she mistakenly thought a blue cab was green, or vice versa. Is the Milan cab that was involved in the crash more likely to have been blue or green?

Answer:

- ❖ The percent of cabs identified as green is  $.2 \times 85\% + .8 \times 15\% \rightarrow 29\%$
- ❖ Of the 29% identified as green,  $12\%/29\%$  are green and  $17\%/29\%$  are blue so the cab is more likely to be blue.

# Discussion: sample problem 4

- ❖ Order the cities by population (largest to smallest)
  - Dhaka
  - Hanoi
  - Milan
  - Santiago

## Answer

1. Dhaka 10.9 million
2. Santiago 5.2 million
3. Milan 4.2 million
4. Hanoi 3.6 million

Most people will not choose Dhaka because they have never heard of the city. Instead they choose one of the other three cities as the most populous because they recognize the names of those cities. This is true even when the selector has little or no idea about any of the cities populations. This is known as the recognition heuristic—we are most likely to select based on recognition (i.e. not select because of ignorance!).

# ISRCS 2009

ISRCS 2009

## Contact

Miles McQueen	amm@if.uidaho.edu or Miles.McQueen@inl.gov	( 208) 526-5872
---------------	--	-----------------