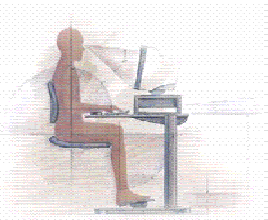# CMPE 233: Human Factors

The Future of Human Factors

The Old Human Factors (1940-2000)

► Domains:
- Military systems
- Aviation and space systems
- Human-computer interaction
- Other transportation systems (driving, etc.)

► Methods
- Time and motion study
- Task analysis
- Human-in-the-loop simulation
- Usability analysis

The New Human Factors (2000-50)

► Domains:
- Military systems (unfortunately…..)
- Space systems
- Robotics
- Medicine and health care
- Home and personal automation
- Neuroergonomics (the study of brain and behavior at work)

► Methods
- Human-in-the-loop simulation
- Usability analysis
- Neuroscience methods
- Reverse engineering methods
- Genetics
- Nano-technology
- Biotechnology

Failed Predictions of the Future

► "The Americans have need of the telephone, but we do not. We have plenty of messenger boys." - Sir William Preece, Chief Engineer, British Post Office, 1878.

► "Flight by machines heavier than air is unpractical (sic) and insignificant, if not utterly impossible." - Simon Newcomb; The Wright Brothers flew at Kittyhawk 18 months later.

► "Television won't last because people will soon get tired of staring at a plywood box every night." - Darryl Zanuck, movie producer, 20th Century Fox, 1946

► "There is nothing new to be discovered in physics now; All that remains is more and more precise measurement." - Lord Kelvin, speaking to the British Association for the Advancement of Science, 1900.

► "The concept is interesting and well-formed, but in order to earn better than a C, the idea must be feasible." - A Yale University management professor in response to a college assignment by Fred Smith proposing a reliable overnight delivery service, in 1966. Smith founded Fedex.

The Fitts' List (1951)

► Machines are better at:
- Speed (Human time delay: 0.5 - 1 s)
- Power (Human maximum output: 0.2 hp/day)
- Consistency of application (Machine: constant; Human: variable, susceptible to fatigue)

► Humans are better at:
- Reasoning (Human: Inductive and deductive; Machine: deductive only)
- Intelligence (Human: Adaptive, flexibl;: Machine: limited)
- Fine motor skills (Human: Versatile, flexible; Machine: limited)

► Mixed
- Computation (Human: slow, error prone but good at error correction; Machine: Fast, accurate, poor at error correction)
- Memory (Human: Large store, random access; Machine: Very large, poor access)


Does the Fitt's List still apply?

► Increasing machine intelligence
- Moore's Law
- Kurzweil's predictions: "Within a few decades, machine intelligence will surpass human intelligence, allowing nonbiological intelligence to combine the subtleties of human intelligence with the speed and knowledge sharing ability of machines"

► Human-machine symbiosis ("joint cognitive systems")

► Augmented human cognition

http://www.kurzweilAI.net/

ARE WE SPIRITUAL
MACHINES?

Ray Kurzweil
vs. the Critics of Strong A.I.
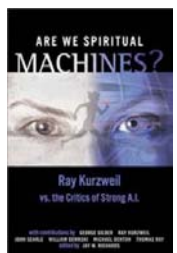
Down the slippery slope…..?

▶ Adaptive automation: systems in which both the user and the system can initiate changes in the level of automation, using neuroergonomics approach and psychophysiological measures

▶ Augmented cognition: using computational technology to enhance human performance in various tasks by overcoming the bottlenecks in processes such as attention and memory

▶ Brain-computer interfaces

▶ Wearable computing

▶ Permanently on line humans

▶ Personal robots

Down the slippery slope…..?

▶ Neurophones: transmitting acoustic information to the brain by means of radio waves into the skin
  ▪ Developed in 1958 by Flanagan, patented in 1968

▶ Implanted cognitive chips: useful for stroke and spinal-cord injuries patients

▶ Wireless brain-to-brain communication

▶ Biological robots
  ▪ imitate the structure or physiology of a biological organism
  ▪ connect and integrate biological and mechanical components in its operation

▶ Digital people and intelligent robots

▶ Everything nano

Terms, terms, terms…..

▶ Bionic humans: humans enhanced by electronic or electromechanical devices

▶ Augmented humans: using technology to increase significantly the intellectual effectiveness of human beings

▶ Cyborgs: machines that are controlled by a sentient brain, but with bodies made of inorganic mechanical parts

▶ Androids: automatons that resembles a human being

▶ Digital life: initiated by MIT Media Lab, three focuses:
  ▪ Organic Networks: viral communications systems with the intelligence at the ends
  ▪ 10X, technologies that can improve human activity by 10x, including bionics, robotic and cognitive assistants
  ▪ Common-Sense Computing, reinvigorating AI by developing a cognitive architecture that can support many features of "human intelligent thinking."

Augmented Human

▶ Physical prosthetics (limbs, heart, kidneys……)
▶ Physical augmentation (exoskeleton, high-force hands…..)
▶ Cochlear implants
▶ Retinal implants
▶ Cortical implants
▶ Deep brain stimulation: a surgical treatment involving the implantation of a medical device called a brain pacemaker
▶ Thalamic stimulation
▶ Hippocampal (memory) stimulation
▶ Neurochips (bi-directional neuron to silicon communication)

Augmentation: Smart fabric

▶ An integration of fabric or human tissue with 'micro' technology

▶ Early 70s → fibre optics, luminous fibres, unsuccessful

▶ The changes
  ▪ Low power (by parent device, human movement, solar, etc)
  ▪ Light & durable (micro) devices
  ▪ Affordable, flexible, washable

▶ Application domains
  ▪ Construction & mines
  ▪ Military & police
  ▪ Harsh weather conditions: mountain rescue, polar expeditions
  ▪ Health: blood pressure/heart rate monitor, BCI

Augmentation: Interactive fabric

▶ Fabric that intelligently responds to stimulus
  ▪ sense and react (e.g., color change, oscillate, swell)
  ▪ conduct electricity
  ▪ perform computational operations
  ▪ collect/store energy

▶ Primary application domain: military
  ▪ Motion, pressure & physiological status sensors embedded in fabrics.
  ▪ Acoustic arrays in large area textiles.
  ▪ Flexible antenna arrays in garments.
  ▪ Body heat-generated power.
  ▪ Fabric-based batteries

Trends

"He who can see three days ahead will be rich for 3,000 years" – Japanese proverb

IS and networking	Science & Technology	Personal & Business Impact	Impact on Society
Speed & scale	Bits & atoms converge	Anonymity & privacy	Religion, philosophy, politics
Miniaturization	Genetics & medicine	Identity & access management	War & peace
Virtualization	Robotics	Pervasive computing & connectivity	Globalization & trade

Scale & Speed

► Moore's law: Processor speed doubles every 18 months
► Build memory, storage, bandwidth, address space, they will fill it
► Supercomputers handle more cps than a mouse's brain today, human within decade, all humans within a generation
► Internet grows from 3 billion to 3 trillion devices in next decade
  ▪ Mobile devices (including cars)
  ▪ Networked homes
  ▪ Sensors

Effects on Internetworking

► New protocols:
  ▪ IP v6 deployments
  ▪ "Internet 0" basic functionality for simple devices interoperable with Internet 1 or Internet 2
  ▪ Delay tolerant networking protocols
  ▪ Device to device conversations will vastly outnumber human:client:server interactions
► Administrative/security consequences:
  ▪ Unified management vital
  ▪ Be careful with transitive trusts in access controls
  ▪ Intelligent event parsing and notification, report aggregation necessary
  ▪ Outsourced operations and incident response
  ▪ People may reach your data faster than you become aware of their access

Miniaturization

Symbol	Prefix	Multiplication Factor	
E	exa	10^{18}	1,000,000,000,000,000,000
P	peta	10^{15}	1,000,000,000,000,000
T	tera	10^{12}	1,000,000,000,000
G	giga	10^{9}	1,000,000,000
M	mega	10^{6}	1,000,000
k	kilo	10^{3}	1,000
h	hecto	10^{2}	100
da	deka	10^{1}	10
d	deci	10^{-1}	0.1
c	centi	10^{-2}	0.01
m	milli	10^{-3}	0.001
μ	micro	10^{-6}	0.000,001
n	nano	10^{-9}	0.000,000,001
p	pico	10^{-12}	0.000,000,000,001
f	femto	10^{-15}	0.000,000,000,000,001
a	atto	10^{-18}	0.000,000,000,000,000,001

► Mainframes
► Microcomputers
► PC's
► Handhelds
► Wearables
► Implants
► Motes
► Nanytes
► Quantum dots

Handhelds

► Applications for:
  ▪ Law Enforcement
  ▪ Military personnel
  ▪ Health care providers
  ▪ Field engineers
  ▪ Nomadic employees
► Personal uses:
  ▪ E-currency, e-commerce, browsing
  ▪ Mobile TV, video conferencing emerging
  ▪ Follow me anywhere connectivity
► Security concerns:
  ▪ Need authentication, dynamic authorization, encryption, A-V, HIDS
  ▪ Subject to adware, viruses, worms via game & music downloads or bluetooth & infrared driveby's

Scenario: Destructive cell phones

► Worms/viruses propagate via infrared, bluetooth, CDMA, GSM or file downloads
  ▪ Relatively benign events in 2000, increasingly malicious since
  ▪ Symbian OS upgrade "fixed" vulnerabilities in February, 2005, 52 more trojans by April
► Phones can:
  ▪ trigger explosions
  ▪ destroy or steal data (pod slurping)
  ▪ disable applications
  ▪ empty bank accounts
  ▪ Eavesdrop
  ▪ disclose user's location
  ▪ deny 911 service, or
  ▪ cause Mario Brothers to fail

Wearables

- Wear your computers
- People don't want to sit where it's convenient for the PC
- Link via PAN's and WLAN's
- Voodoo inputs, plain conversation queries
- The media environment will reach out to wearers: Drifting through drivel vs. dredging dramatic discoveries
- Personal software agents - can they be turned?

Scenario: Hacker assassins?

- Medical implants
  - Pharmaceutical dispensers
  - Insulin pumps
  - Implanted defibrillators
  - Prosthetics
- Wireless interfaces are justified:
  - For emergency responders to quickly diagnose a crisis
  - To fully-inform other practitioners under normal conditions
  - To re-program obsolete devices or de-bug defects
- Interfaces offer potential exposure to hacker with deadly motives

Motes

- Tiny computers with sensors in ad hoc mesh networks
  - Smart bricks
  - Smart gravel
  - Smart dust / utility fog
  - Smart paint
- Applications:
  - Bridge maintenance
  - Utility meters
  - Oil production
  - Crop conditions
  - Earthquake predictions
  - Border patrol
  - Weather monitoring and control
  - Forest/endangered species management
- Issues:
  - Privacy
  - Physical security
  - Encryption

Genetics & Medicine
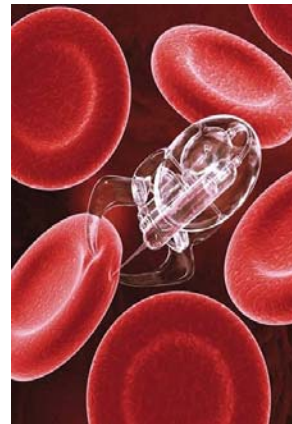
- DNA, an information system as old as life itself
- Genetic sequencing progressing rapidly
- Genetic engineering common in crops, increasing in animals
- DNA replication processes can be harnessed to create designer proteins, microelectromechanical systems (MEMS), and information storage devices
- Humans are designing machines that resemble those found in nature
- Security implications of biology/technology hybrids

Robotics & Artificial Intelligence

- Robots in use now in:
  - Manufacturing
  - Exploration
  - Homes
  - Millions today
  - Billions one day
- AI applied to business:
  - Language
  - Data mining/searches
  - Engineering design
  - NBAD's
  - SIM's

Virtualization

- Virtual SANS
- MSSP's & ASP's
- Software as a service
- Search engines and highly distributed databases
- Common interface for disparate devices may ease administration: intuitive?
- Security implications:
  - Redundancy may improve availability
  - Virtualization requires a complex web of trust
- Grid computing
  - 10, 20, 40 gbs links
  - Data & CPU's distributed among hundreds of participants or more
 - Who cares where data is processed as long as it's billed correctly?

Scenario: Grid computing

How many transitive trust relationships must you accept to participate in grids?

Blurring borders between binary and tangible worlds

- ► Merger of physical security and infosec is underway on a macro scale
- ► Biological virus now digitized, digital virus now carried by living creatures
- ► Quantum computing, Qbits
- ► Artificial atoms & molecules
- ► PF's: personal fabricators

THERE ARE ONLY 1 0 TYPES OF PEOPLE WHO UNDERSTAND BINARY THOSE WHO DO AND THOSE WHO DO NOT.
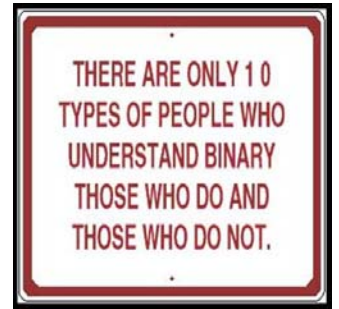
Privacy & Anonymity

- ► Cross-linked databases
- ► Ease of correlation among unrelated databases
- ► Mountains of data and content require both search engines and anti-search technologies
- ► http://www.aclu.org/pizza/
- ► Anonymizers, avatars, and agents…can they be "turned"?
- ► Next wave of regulation? personal genetic information
- ► Pervasive surveillance

Pervasive Surveillance

Who will be better informed about security events as they happen, the "white hat communities" or the "black hat communities"?

Scenario: Encrypt sensitive data wherever it goes

Assume that anything you create, manipulate, transmit, store, or even delete may find it's way "out in the open". Does it matter?

- Personally-identifiable information
- Medical records
- Account balances
- Credit histories
- Trade secrets
- Business transaction histories
- Offsite backups
- Guard vs. data theft and/or corruption

Quantum Computing

- ► Much faster for certain types of calculations by solving all outcomes at once - e.g. prime factors or airline/shipping schedule optimization
- ► Unbreakable (?) Quantum Key Distribution
- ► Man-in-the-middle measuring wrong variable or choosing wrong method can completely randomize results, defeating own efforts

Pervasive Computing & Connectivity

► "The future is here. It's just not evenly distributed yet."- William Gibson
► Computing and communications embedded in nearly everything
► Network-enabled environment
► Ad hoc nets
  ▪ self organizing
  ▪ self powering scavengers
  ▪ self administering
► Not just global, interplanetary nets
► "Follow me" services
► "Discover your habits" services
► Only for the elite "digirati", or for all people?

Scenario – the Singularity
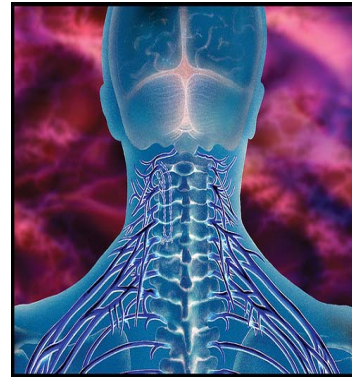
► "Transcendent" humanity, enhanced or uploaded
► Merged with technology, including AI greater than all minds in previous history combined
► Becomes "one" with the intelligent Universe

Identity & Access Management

► Interoperable directories
► Access controls integrated in infrastructure and applications
► Biometric and RFID trends

RFID tags for humans

► For identification and authentication
► Easily implanted and used:
  ▪ data center access
  ▪ PC login
  ▪ unlocking car/house
► Combine RFID with phone or key fob for cashless transactions

RFID & biometric passports

► Passport/VISA enforcement
► Scanned involuntarily within 30-60', so modified with metal covers and magnetic strips
► Biometrics inside – face photo and 2 fingerprints
► Safeguards to prevent forgeries?
► Some people oppose biometric databases
► Security benefit > risk?

Globalization & Trade

► Interaction trumps isolation
► "No nation was ever ruined by trade." – Ben Franklin
► "No nation with a McDonald's has ever attacked another with a McDonald's" – Tom Friedman
► Intertwined data infrastructures, economies, currencies, and fates
► Instant leaps from agricultural societies to information age cultures
► Individuals, small businesses, and small villages are enabled in the global economy
► Specialization, separation of duties on a global scale

Worldwide regulatory environment

Technological change continues to outpace government's ability to create new regulations, or fix obsolete or inadequate laws that overburden businesses and individuals. Contradictory mandates exist today for global businesses, but international standards are emerging through professional associations, industry associations, and leading government organizations.

War & Peace

► Corroborate multiple sources of intelligence
  ▪ Remotely operated vehicles
  ▪ Ruggedized, delay-tolerant systems
  ▪ Networked troops and HUMINT
  ▪ Surveillance at the border
  ▪ Satellites and sensors
► Vision2020
  ▪ Info superiority
  ▪ Precision engagements
  ▪ Focused logistics
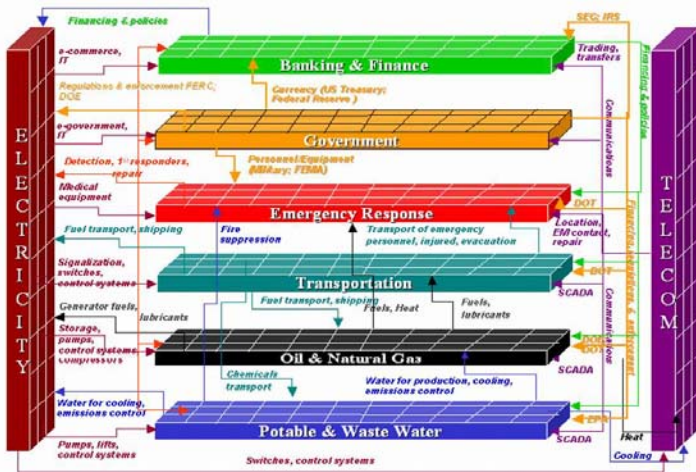► Peace/aid workers must apply security practices, too
  ▪ Caution in transmitting even the most mundane data
  ▪ Lives are at stake
► Critical Infrastructure Protection

Interconnected Infrastructure

Future scenario: SCADA breaches

► Factors have contributed to the escalation of risk to System Control and Data Acquisition (SCADA) systems:
  ▪ the adoption of standardized technologies with known vulnerabilities
  ▪ connecting control systems to other networks, including insecure remote connections
  ▪ the widespread availability of technical information about control systems
  ▪ lack of awareness of problems, solutions, and events
  ▪ Intruders from China had 17 days of access to California power provider's SCADA systems before detection
  ▪ Ex-contractor sabotaged Maroochyshire, Queensland, AU sewer plant

Enduring Principles

► Methods change, motives don't
► Confidentiality, Integrity, Availability
► Obscurity ≠ security
► Ease of use vs. strength of security
► Don't build $1,000 fence for $100 horse
► Don't bring a free horse inside a $M fence
► "The trouble with worrying so much about your security in the future is that you feel so insecure in the present." - Harlan Miller