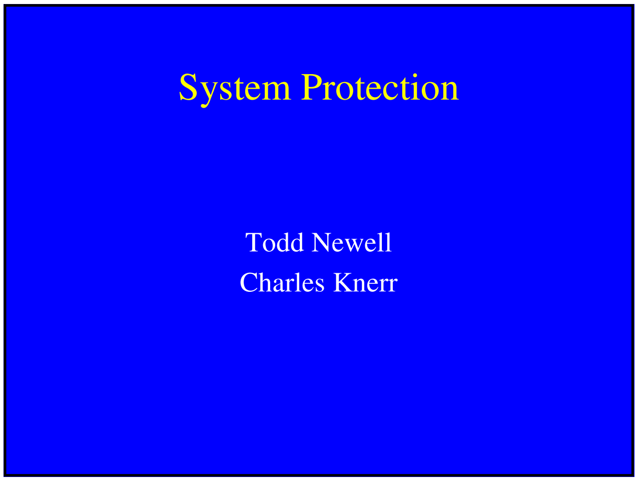
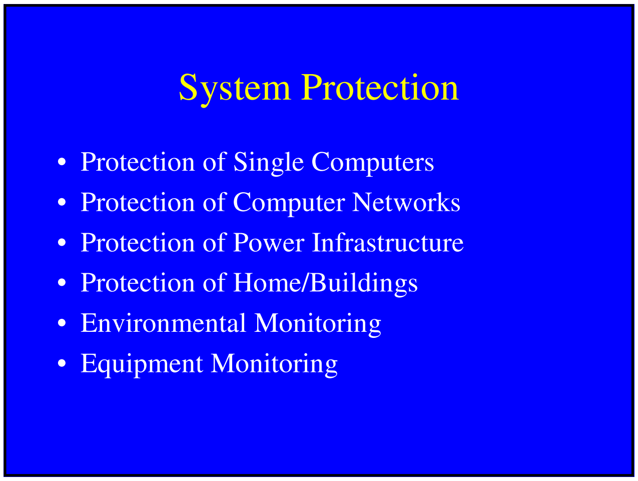


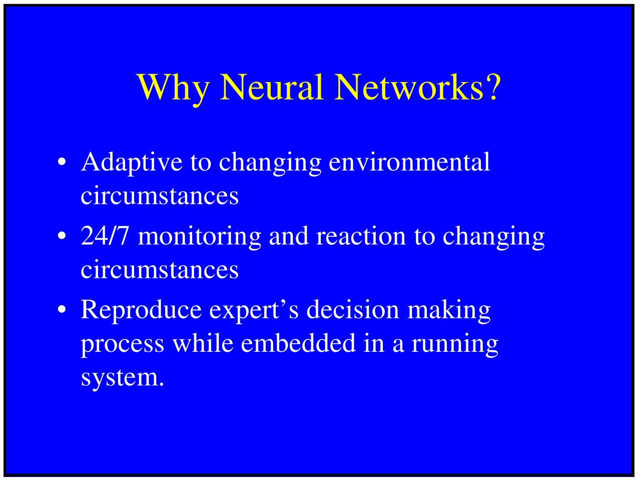
System Protection

Todd Newell
Charles Knerr



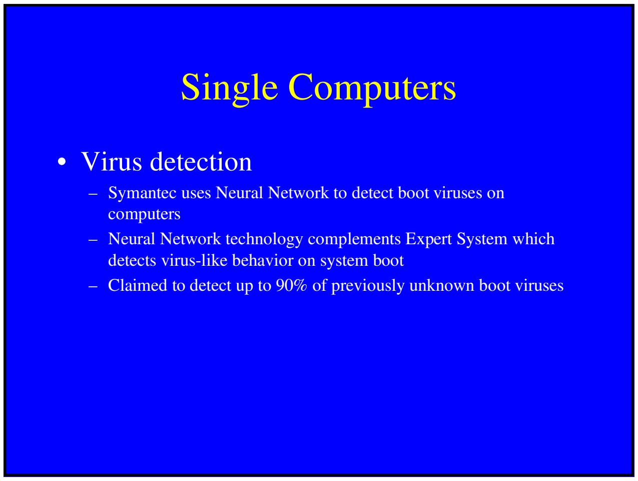
System Protection

- Protection of Single Computers
- Protection of Computer Networks
- Protection of Power Infrastructure
- Protection of Home/Buildings
- Environmental Monitoring
- Equipment Monitoring



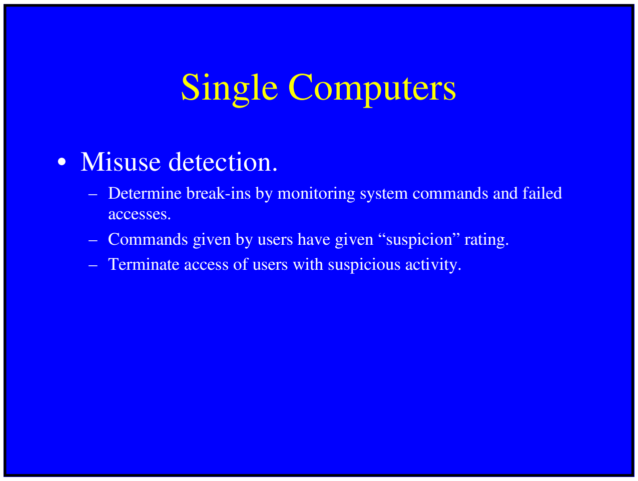
Why Neural Networks?

- Adaptive to changing environmental circumstances
- 24/7 monitoring and reaction to changing circumstances
- Reproduce expert's decision making process while embedded in a running system.



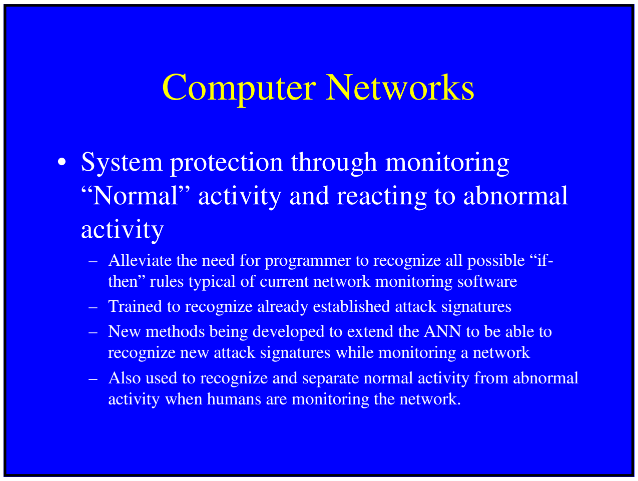
Single Computers

- Virus detection
  - Symantec uses Neural Network to detect boot viruses on computers
  - Neural Network technology complements Expert System which detects virus-like behavior on system boot
  - Claimed to detect up to 90% of previously unknown boot viruses



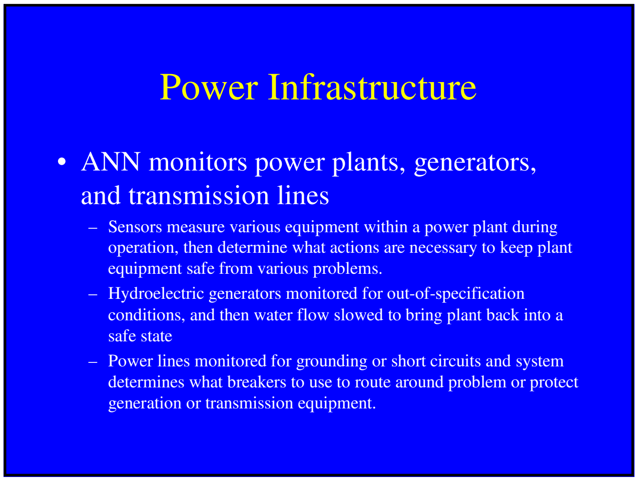
Single Computers

- Misuse detection.
  - Determine break-ins by monitoring system commands and failed accesses.
  - Commands given by users have given “suspicion” rating.
  - Terminate access of users with suspicious activity.



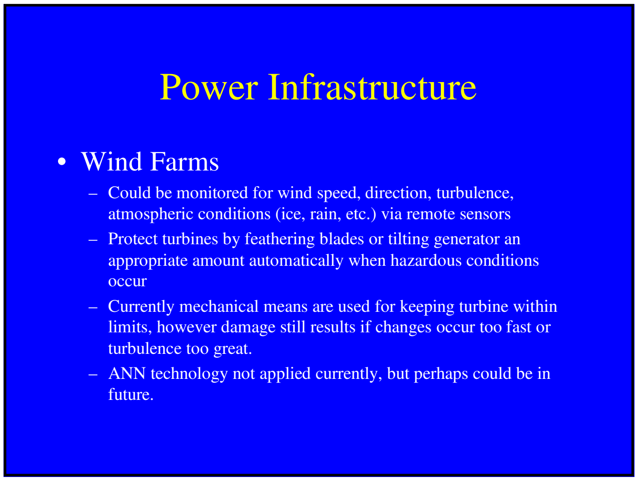
Computer Networks

- System protection through monitoring “Normal” activity and reacting to abnormal activity
  - Alleviate the need for programmer to recognize all possible “if-then” rules typical of current network monitoring software
  - Trained to recognize already established attack signatures
  - New methods being developed to extend the ANN to be able to recognize new attack signatures while monitoring a network
  - Also used to recognize and separate normal activity from abnormal activity when humans are monitoring the network.



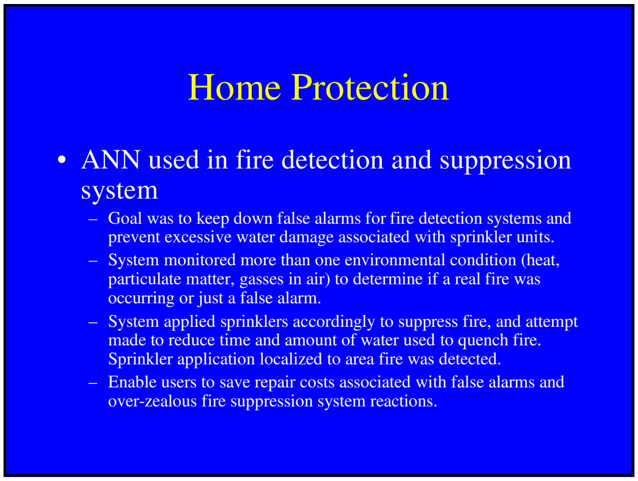
Power Infrastructure

- ANN monitors power plants, generators, and transmission lines
  - Sensors measure various equipment within a power plant during operation, then determine what actions are necessary to keep plant equipment safe from various problems.
  - Hydroelectric generators monitored for out-of-specification conditions, and then water flow slowed to bring plant back into a safe state
  - Power lines monitored for grounding or short circuits and system determines what breakers to use to route around problem or protect generation or transmission equipment.



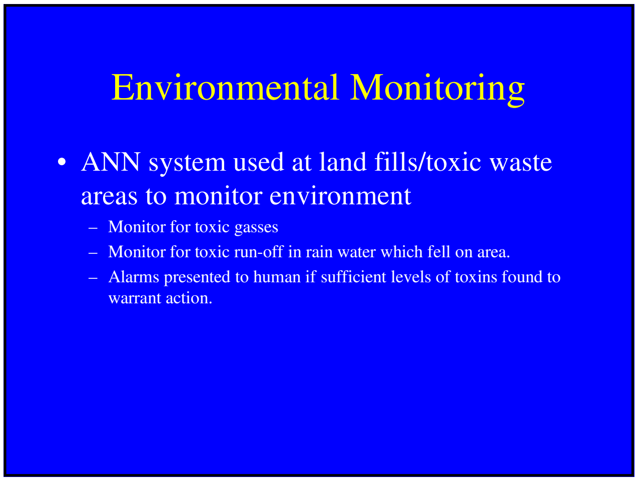
Power Infrastructure

- Wind Farms
  - Could be monitored for wind speed, direction, turbulence, atmospheric conditions (ice, rain, etc.) via remote sensors
  - Protect turbines by feathering blades or tilting generator an appropriate amount automatically when hazardous conditions occur
  - Currently mechanical means are used for keeping turbine within limits, however damage still results if changes occur too fast or turbulence too great.
  - ANN technology not applied currently, but perhaps could be in future.



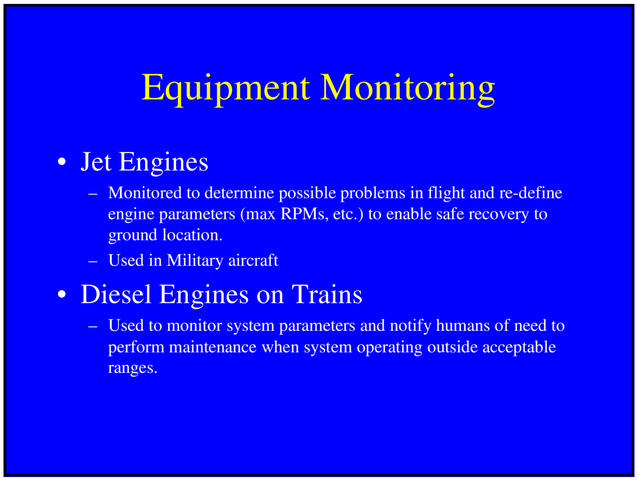
Home Protection

- ANN used in fire detection and suppression system
  - Goal was to keep down false alarms for fire detection systems and prevent excessive water damage associated with sprinkler units.
  - System monitored more than one environmental condition (heat, particulate matter, gasses in air) to determine if a real fire was occurring or just a false alarm.
  - System applied sprinklers accordingly to suppress fire, and attempt made to reduce time and amount of water used to quench fire. Sprinkler application localized to area fire was detected.
  - Enable users to save repair costs associated with false alarms and over-zealous fire suppression system reactions.



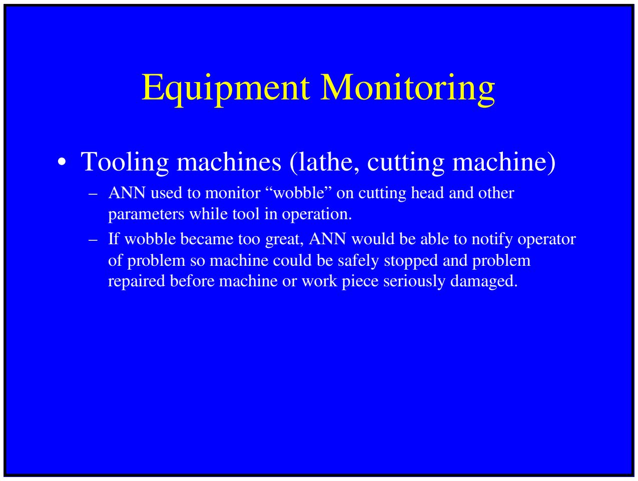
Environmental Monitoring

- ANN system used at land fills/toxic waste areas to monitor environment
  - Monitor for toxic gasses
  - Monitor for toxic run-off in rain water which fell on area.
  - Alarms presented to human if sufficient levels of toxins found to warrant action.



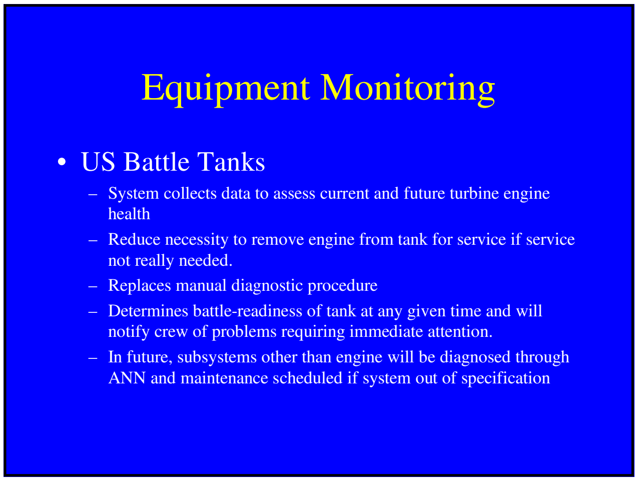
Equipment Monitoring

- Jet Engines
  - Monitored to determine possible problems in flight and re-define engine parameters (max RPMs, etc.) to enable safe recovery to ground location.
  - Used in Military aircraft
- Diesel Engines on Trains
  - Used to monitor system parameters and notify humans of need to perform maintenance when system operating outside acceptable ranges.



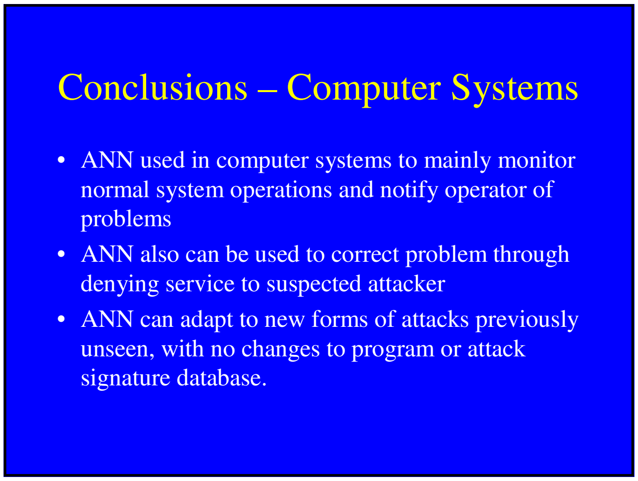
Equipment Monitoring

- Tooling machines (lathe, cutting machine)
  - ANN used to monitor “wobble” on cutting head and other parameters while tool in operation.
  - If wobble became too great, ANN would be able to notify operator of problem so machine could be safely stopped and problem repaired before machine or work piece seriously damaged.



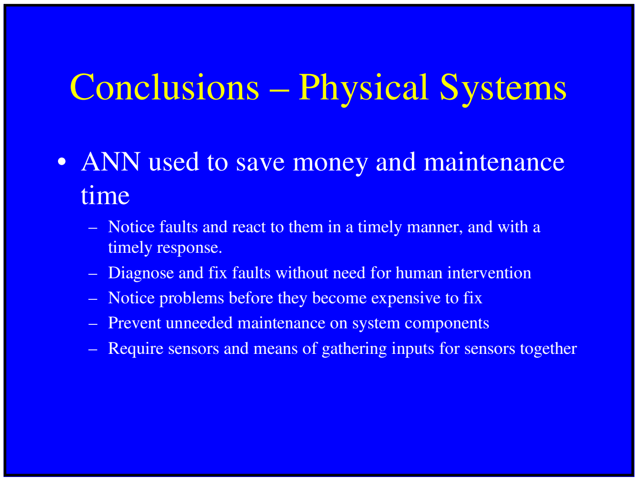
Equipment Monitoring

- US Battle Tanks
  - System collects data to assess current and future turbine engine health
  - Reduce necessity to remove engine from tank for service if service not really needed.
  - Replaces manual diagnostic procedure
  - Determines battle-readiness of tank at any given time and will notify crew of problems requiring immediate attention.
  - In future, subsystems other than engine will be diagnosed through ANN and maintenance scheduled if system out of specification



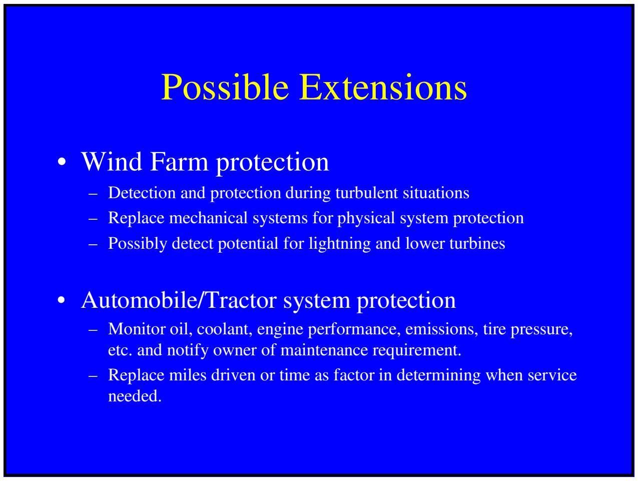
Conclusions – Computer Systems

- ANN used in computer systems to mainly monitor normal system operations and notify operator of problems
- ANN also can be used to correct problem through denying service to suspected attacker
- ANN can adapt to new forms of attacks previously unseen, with no changes to program or attack signature database.



Conclusions – Physical Systems

- ANN used to save money and maintenance time
  - Notice faults and react to them in a timely manner, and with a timely response.
  - Diagnose and fix faults without need for human intervention
  - Notice problems before they become expensive to fix
  - Prevent unneeded maintenance on system components
  - Require sensors and means of gathering inputs for sensors together



Possible Extensions

- Wind Farm protection
  - Detection and protection during turbulent situations
  - Replace mechanical systems for physical system protection
  - Possibly detect potential for lightning and lower turbines
- Automobile/Tractor system protection
  - Monitor oil, coolant, engine performance, emissions, tire pressure, etc. and notify owner of maintenance requirement.
  - Replace miles driven or time as factor in determining when service needed.