# Embedded Virtualization for Reliable Redundancy

Robert Gifford, Alexander Maloney
{robertgif, maloneya}@gwu.edu
Computer Science, The George Washington University

## Motivation

**Critical Dependence on Embedded Devices**

Cars, power plants, hospitals, and other critical infrastructure all depend on embedded devices

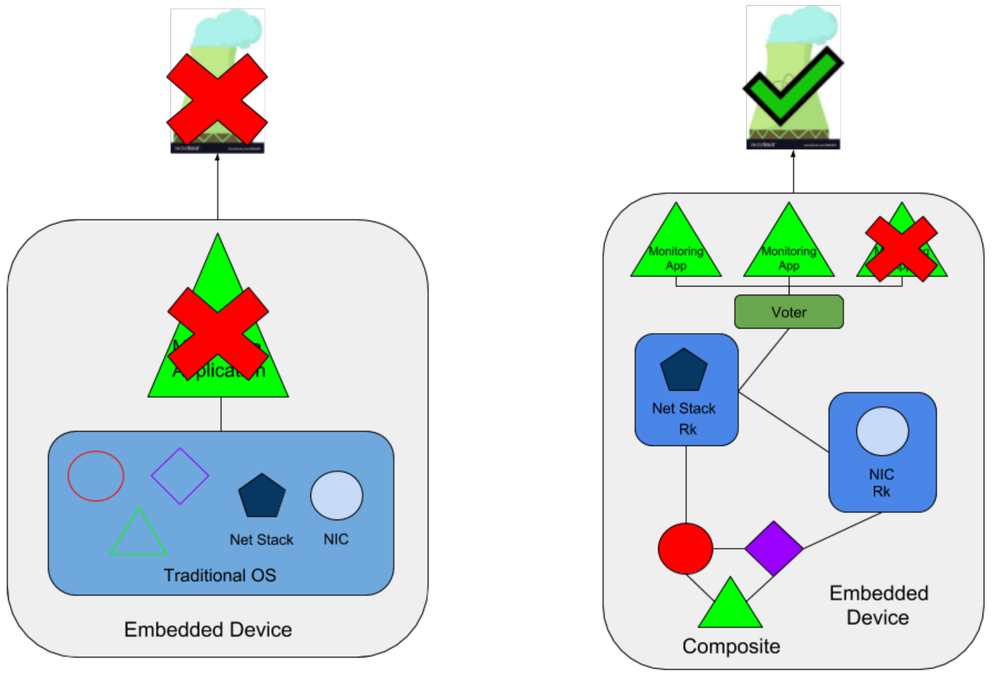
**Problem: Fault propagation**

- **Example case: 2003 Northeast Blackout**
- **55 million people effected**
- **6.4 billion dollars in commercial losses**
- **Approximately 100 deaths**
- **All due to a failure in monitoring software with no fault recovery**

## Project Goals

- **Build a fault tolerant system to protect applications from crashes and malicious attacks**
- Create virtual redundant applications
- Minimize single points of failure
- Enable crash detection

## Our Solution




## Results

**Created an experiment in which a power plant monitoring dashboard was served from a buggy web server.**

**With our framework we are able to run redundant copies of the server, catch the fault and continue to provide service**

## Design

### Composite

- Micro Kernel architecture creates isolation between resource providers
- Fault tolerance at operating system level

### Voter

- Component that replicates running applications, monitors their state, and detects faults
- Continued application service even after fault occurs

### Rump Kernel

- NetBSD Unikernel provides support for legacy software
- Isolate resource providers increasing system isolation