worldcast Research Report

E-SUPER DOMINO

A report on the needs & methods for developing defenses against electromagnetic pulse weapons & magnetic storms,
&
the role of hardened point-to-multipoint IP communications using SMART(p) technology.

By Ian A. Stewart

Table of Contents

List of Figures

Foreword

Worldcast proposes research into E-SUPER DOMINO

Using the analogy of falling dominos, a "super domino" is one that is linked to others and is impervious to single point failure. E-SUPER DOMINO stands for ***Enhanced*** **Security Utilizing Public and Emergent Reliable Distribution of Multipoint Inter-domain Networking Objects**, with reliability added to *base* level *point-to-multipoint* communications infrastructure with Worldcast's **SMART** technology. Worldcast's technology layers security, reliability and provides for multipoint feedback from mass audiences.

Fiber is impervious to the electromagnetic pulses created by nuclear detonations and magnetic storms (EMP/S)

Because fiber optical communications use light to transmit signals rather then electrons over wire, a hardened national fiber backbone could be used for expanded capacity and to provide *point-to-multipoint* communications in the event of an EMP attack or magnetic storm, referred to hereafter as EMP/S. (Note: common name for an electromagnetic storm is a sunspot). However, a separate system is required to add the security and reliability to *base* (unreliable) *point-to-multipoint* IP connections. Worldcast has developed such a system and has called it SMART - Secure Multipoint for Advanced Repeating of Television. Also, to be efficient, a mechanism is required to analyze the *base* multipoint protocols available and use the best possible multipoint link. Worldcast has also developed this system, andhas called it SIMPLE - Self Implementing Multipoint Protocol Level Escalation.

A fiber optics backbone could also be connected to key infrastructure such as the monitoring and control of remote devices (also called SCADA). For example, hardened solar power stations in the southwest cold use point-to-multipoint technology for monitoring and remote switching. Wind power generators, hardened against EMP/S, could have the capability to be controlled by SMART fiber technology allowing them to generate an EMP/S tolerant transmission medium, such as hydrogen.

Our research shows that Worldcast is the first, and currently the only, developer of technology that provides the add-on to point-to-multipoint IP communications which adds security, reliability and a bi-directional reporting mechanism designed for mass audiences. The use of SMART point-to-multipoint technology could be tested with the installed base of dark fiber or newly installed fiber that could be routed along railroads or roadways. It should be noted that many of the current fiber routing stations are already in Faraday cages (wire mesh surrounding the building that is tied to ground) making them suitable candidates for conversion to fully hardened fiber stations.

Worldcast proposes the E-SUPER-DOMINO project to test multipoint connectivity

We propose to test the operation of SMART technology to overcome the United States' vulnerability to EMP and magnetic storms. This document provides a look at the related infrastructures and their vulnerability to EMP/S and shows how SMART technology overcomes those vulnerabilities in the most efficient way possible.

Worldcast proposes research that connects point-to-multipoint Internet infrastructure to create large scale transmissions of control data, media and distributed data, in order to provide redundancy not found in the current infrastructure. This proposed research project, E-SUPER DOMINO, will investigate the use of the base point-to-multipoint infrastructures for the application of Secure Reliable point-to-multipoint systems that have bi-directional capabilities.

E-SUPER DOMINO project proposes to test the use of existing infrastructure

Test elements include routers network, switching for broadcast of multipoint data, control information, and emergency systems. E-SUPER DOMINO uses the super domino effect to distribute data by bridging over missing point-to-multipoint elements using networking objects.

The Problem

Infrastructure's vulnerability to EMP/S

The infrastructure in the United States is highly vulnerable to EMP/S. Solar activity peaks its 11 year cycle again in 2012, posing a potential threat. Another example: Some rouge states have developed the ability to launch a missile at sufficient altitude and range to mount a catastrophic attack. If a missile were equipped with an EMP nuclear device, the footprint of the attack area would be nation consuming. If such a rouge nation were to create a weapon with the intent to cripple the U.S., the most effective defense, for the least amount of money and the least potential for self infliction (as with germ warfare), would be an EMP weapon. From a position in space, the EMP weapon could be detonated by remote or pre-programmed control, wiping out most electronics in the entire United States mainland. Of particular interest to Worldcast is the effect the EMP attack or solar storm would have on the point-to-multipoint communications infrastructures, such as broadcast television, radio, cable television and satellite television. EMP/S damage to command and device control (SCADA) would create unparalleled catastrophic events. The United States infrastructure is most highly vulnerable to EMP/S. For example, all high power broadcast equipment has little or no off the shelf replacement capability.

Areas of infrastructure that are highly vulnerable to EMP/S:

Electronic monitoring systems (SCADAs)

Figure 1 - Example of SCAD device

- SCADA systems are heavily used in critical infrastructure components, such as the U.S. power grid, drinking water management, and oil and gas pipeline distribution. In November of 1999, ships' radar was able to block the electronic control of the San Diego Aqueduct system. A crew was dispatched to manually control the flood gates averting a "catastrophic failure" of the aqueduct. Most importantly, monitoring of the status of these devices is not distributed. Even if some command centers survived the EMP attack or storm the status of those centers are unknown to others.

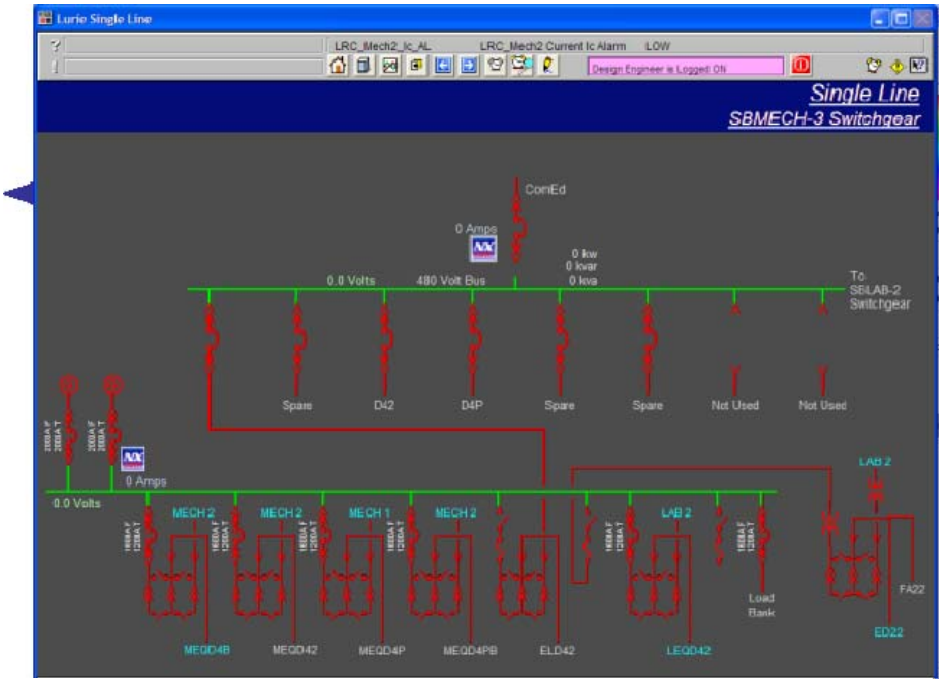

Figure 2 - Example of a SCADA computer based command center

Multipoint-infrastructure related to power

- ### The grid

  The electrical system in the U.S. requires management of a power grid that is currently run at peak times close to the point of failure. The national power grid is operated by a maze of contributors where a problem of a small contributor can mushroom into a catastrophic failure. Upsetting this grid by EMP/S would cause widespread failure of the system. As we have seen in the massive and deadly power failures of 2003, 1977 and 1965, the balance of the grid requires the control and energy output reporting of every grid participant, in order to enable the system operator to maintain the delicate balance between energy consumption and energy use.

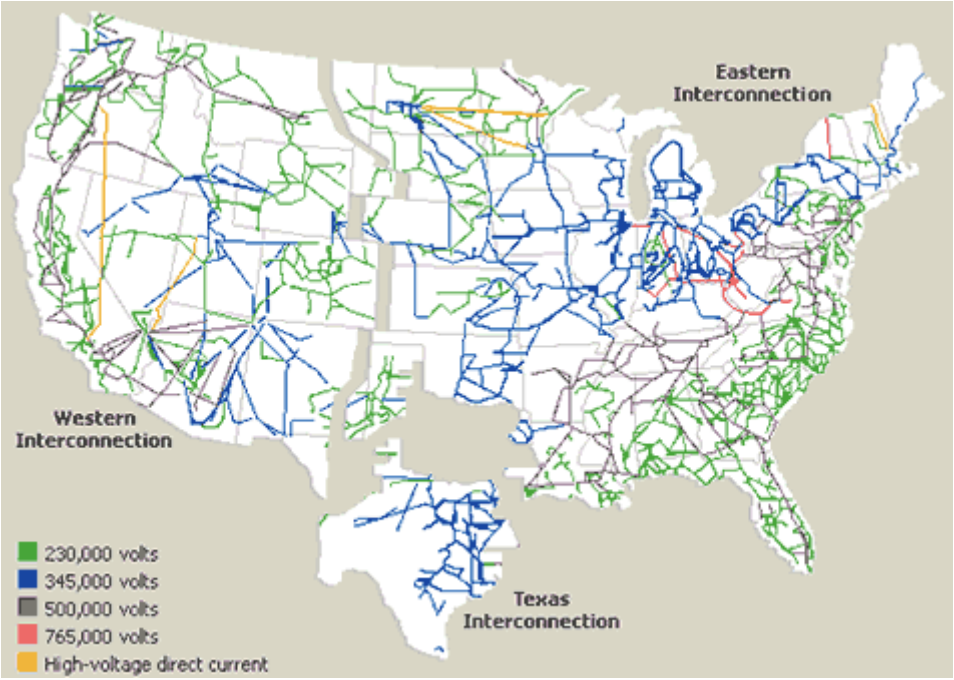

Figure 3 - Even after the massive blackouts of 2003, 1977 and 1965, the national power grid remains in fragile, vulnerable condition. Energy spokespeople state investments of $56 to $450 billion is needed to fix this antiquated system.

- ### Centralized control system

  Currently this control system is centralized at a small number of command stations. The use of point-to-multipoint communications could allow a decentralized command structure thus increasing survivability to EMP attack or electromagnetic storm.

- ### The role of point-to-multipoint communications in power generation

  Using point-to-multipoint communications in power grid stations and components will allow a nationwide awareness of power generation status and capability. This reduces the power grids' vulnerability to attack from conventional sources, as well as EMP/S. Using a secure reliable point-to-multipoint system with bi-directional feedback would allow a distributed command and control, and would provide the ability to create redundancy for power grid, command, and control stations.

- **Concentration of power grid command centers**
  Currently, the concentration of the command centers for the power grid makes them a target for terrorists. The concentration of these power command and control centers creates vulnerability for a 9/11 style attack. The consequences of a nationwide power failure resulting from an attack on these few control facilities would have a far greater effect for the average American than did the 9/11 attack.

- **How point-to-multipoint technology can increase power survivability and reliability**
  Using EMP/S hardened secure reliable point-to-multipoint technology for these command and control facilities would allow for distributed command and control. Essentially, any point with access to a multipoint enabled facility could, providing the access level and authority, function as a command point. Using multipoint technology, command points could be mobile and standby computers (laptops or otherwise) and could be stored for immediate interconnection in the event of attack. SCADA devices could then be controlled using a hardened point-to-multipoint system.

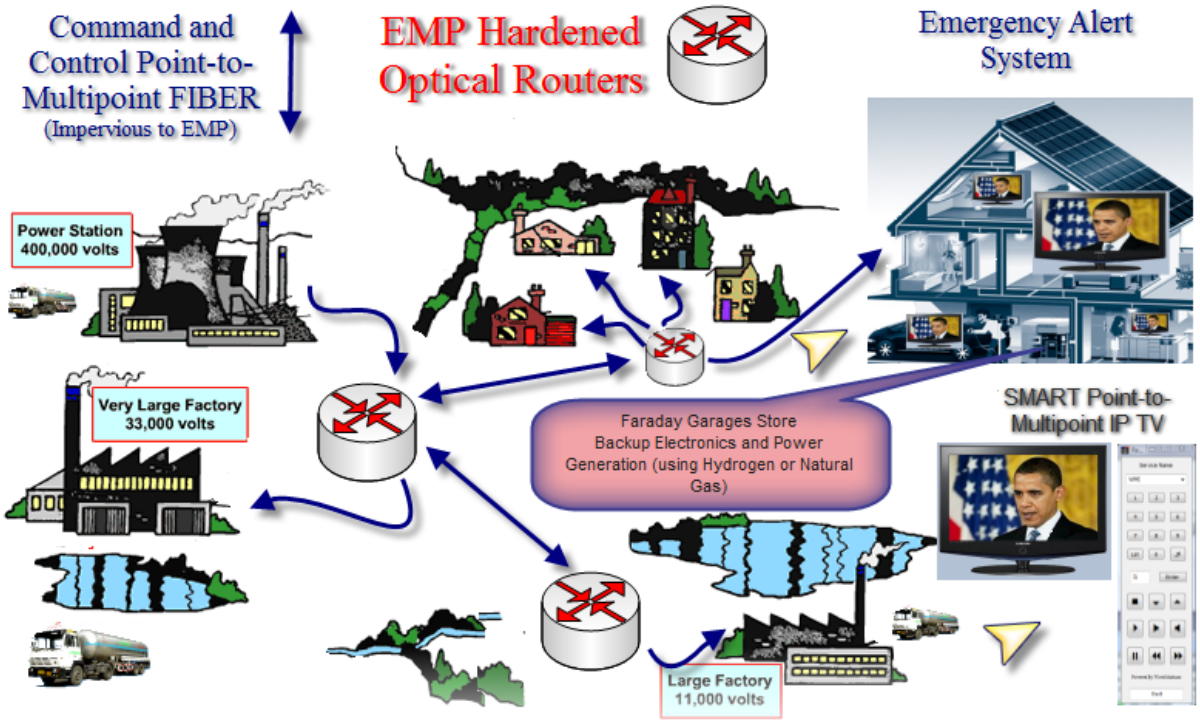

Figure 4 EMP/S impervious FIBER carries command and control and Emergency Alert Services

Multipoint telecommunications vulnerabilities to EMP/S

- **The broadcast stations**

  Broadcast television uses satellite to pull network feeds. Satellites are highly prone to damage by EMP/S, and can be damaged at a great distance by gamma rays from the detonation of a nuclear device in space. Furthermore, the antennae of broadcast television stations are perfect receptors of the EMP/S radiation. Failure of these broadcast stations would be close to 100% in the affected areas.

  To answer the threat, SMART IP protocol transmission can be broadcast to massive scale audiences in much the same way as television, but SMART uses fiber as its transmission medium; hence, if used with hardened routing stations, a SMART television system would be impervious to EMP/S attack.

- **The cable systems**

  Cable systems use copper wire to move the television signals into the home. Such wires would carry off-scale voltages in the event of an EMP/S attack. These voltages would damage any devices that are connected, and possibly injure people who might be close. There is, however, some good news about cable systems in relation to EMP/S. Cable systems use fiber to the neighborhood and this fiber, as well as telecommunications fiber to the home (FTTH), could be modified and hardened to carry EMP/S-proof SMART transmissions.

Virtual cable using SMART point-to-multipoint technology

Virtual cable is a term to describe the use of public IP infrastructure to provide cable-like service simultaneously to massive numbers of homes and businesses. Although we've all seen television-like service on the internet with video-on-demand companies like "You Tube" and "Hulu," such services lack the capability to accommodate the numbers of users that tune into major events, such as sporting events, first run movies, popular network television programming, or major news.

On 9/11, television usage skyrocketed. Because broadcast and cable television is point-to-multipoint in nature, live viewers were able to see the events as they unfolded. The same can not be said for Internet transmissions on 9/11. All the major Internet news sites crashed due to oversaturation. This is because current web sites like YouTube.com or CNN.com are transmitting their signals from point-to-point rather than point-to-multipoint. One complete signal is needed for each user, and because the demand was so great on 9/11, the capacity was quickly exceeded and did not fully recover for days.

Because of the Internet's usage of bandwidth for point-to-point connections, the current point-to-point Internet is rendered useless in any type of emergency.

SMART virtual cable technology solves this problem by using the unreliable multipoint base protocols currently available and adding to them the security, reliability and bi-directionality to maintain full functionality during any emergency situation.

SMART technology creates a cable facsimile that is impervious to EMP/S

Because SMART works like broadcast television, but can use fiber as its base transport, it can be used to create a broadcast system that shares fibers' immunity to EMP/S. To the end-user, SMART works just like cable, but SMART uses IP infrastructure to accomplish the same goals as cable. Under the hood SMART is completely different than current cable infrastructure and SMART TV can be used with public infrastructure. Cable has no mechanism to accomplish this ubiquity.

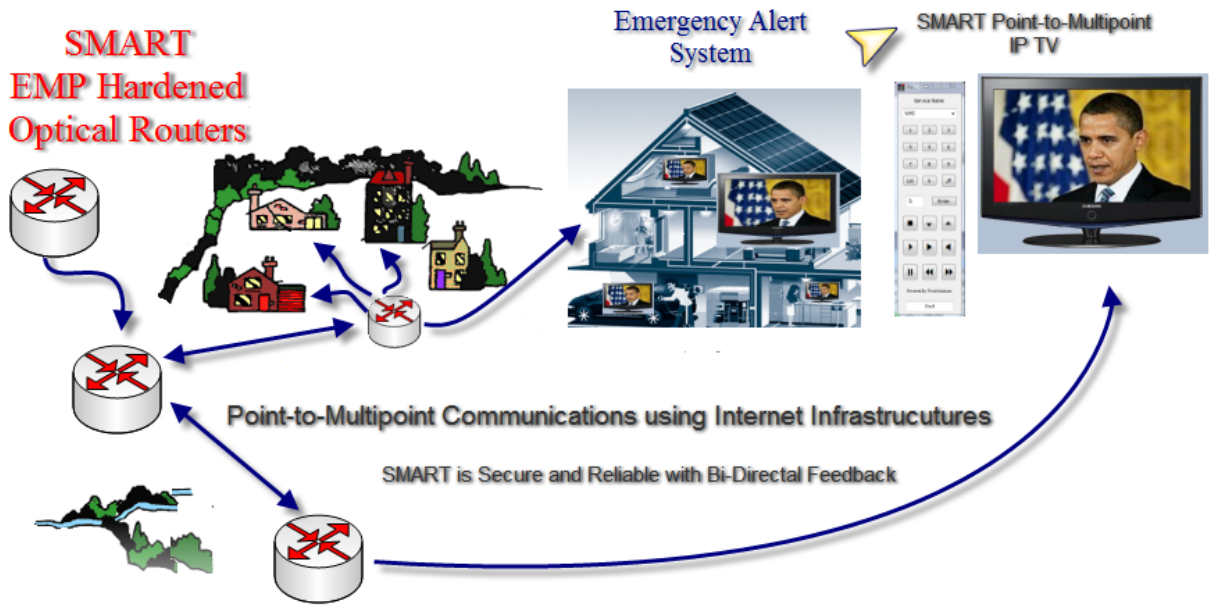

Figure 5 - EMP/S-proof Virtual Cable using SMART Technology

EMP/S's Effect on Banking and Finance

There are several areas of vulnerability in the U.S. banking system.

- Centralized record keeping is vulnerable to EMP/S
- The banking system is reliant on the Internet
- Electricity is needed to power computers
- Banking is reliant on computing

The areas that SMART point-to-multipoint communications can contribute to the EMP/S survivability are:

- Decentralize the banking system. Bank records are maintained in mirrored databases
- Reduce traffic levels on the Internet -- decentralized access of financial data
- Increase reliability of the electrical system - (see Multipoint Infrastructure Power)

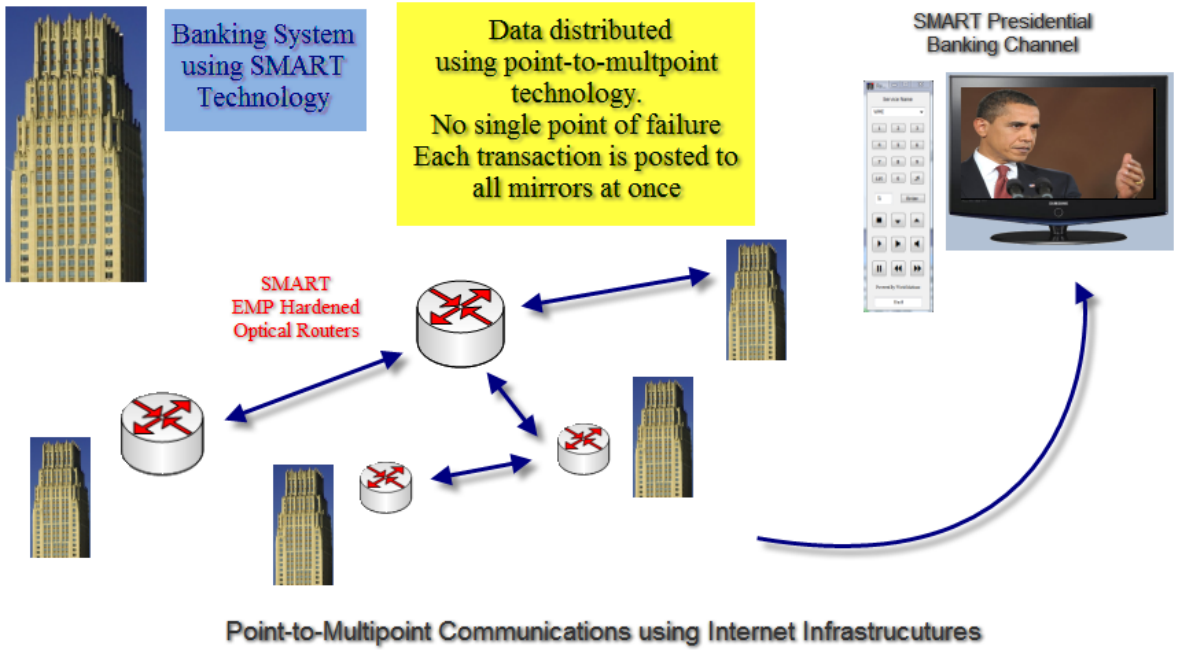

Figure 6 - Point-to-multipoint distributed banking system

Controlling Distribution of Petroleum and Natural Gas

Petroleum and natural gas are distributed using pipelines and trucks. The trucks rely on schedules generated by computers. Control devices used to maintain the pipelines could use SMART to prevent catastrophic failures of remote-controlled system devices.

Interrelated Transportation Infrastructure

Air traffic systems benefit by SMART multipoint communications

Airplanes are fortunate to have natural EMP/S resistance, but the infrastructure they depend on, such as air traffic control and airport management, would be decimated by EMP attack or magnetic storm. The airport control systems are concentrated at each airport, and traffic control is handled by a central facility. (See picture of Palmdale air traffic control below.)

Figure 7 - All California air traffic control is centralized and is vulnerable to attack

Survivability would be augmented by de-centralization of the flight traffic systems. Using SMART point-to-multipoint data, any authorized point could contribute to flight control order. Hardened airplane transponder receivers could relay point-to-multipoint information to be received by interested parties. Using distributed command and control, redundancy would be built in by the nature of multipoint communications.

Trains, trucks, busses and planes all move on schedules. These schedules could easily be communicated using SMART point-to-multipoint messages.

Food distribution in the post EMP/S attack world

Food distribution relies on a trucking system that would be crippled by EMP/S. Supermarket inventories are stored in central databases that would be affected.

Using SMART point-to-multipoint technology the databases of truck status and inventories could be de-centralized which would improve their survivability in the event of an attack. Because all inventories would be available to any network point, the governmental agencies involved in emergency management services would know where any shortages occur. All food distribution command centers would be aware of the entire status of any area at any time.

Figure 8 - Food monitoring and command and control

Control Systems Loss Due to EMP/S and the Effect on Water Supply

Water systems are highly automated with remote-controlled floodgates and water level monitoring. The control stations for this monitoring are centralized within regions and are at risk of catastrophic failure if an EMP attack or serious magnetic storm were to take place.

Using distributed multipoint command and control, and using SMART-enabled multipoint commands to control and monitor floodgates, water level monitoring systems could be upgraded to a high degree of reliability and far greater resistance to EMP/S.

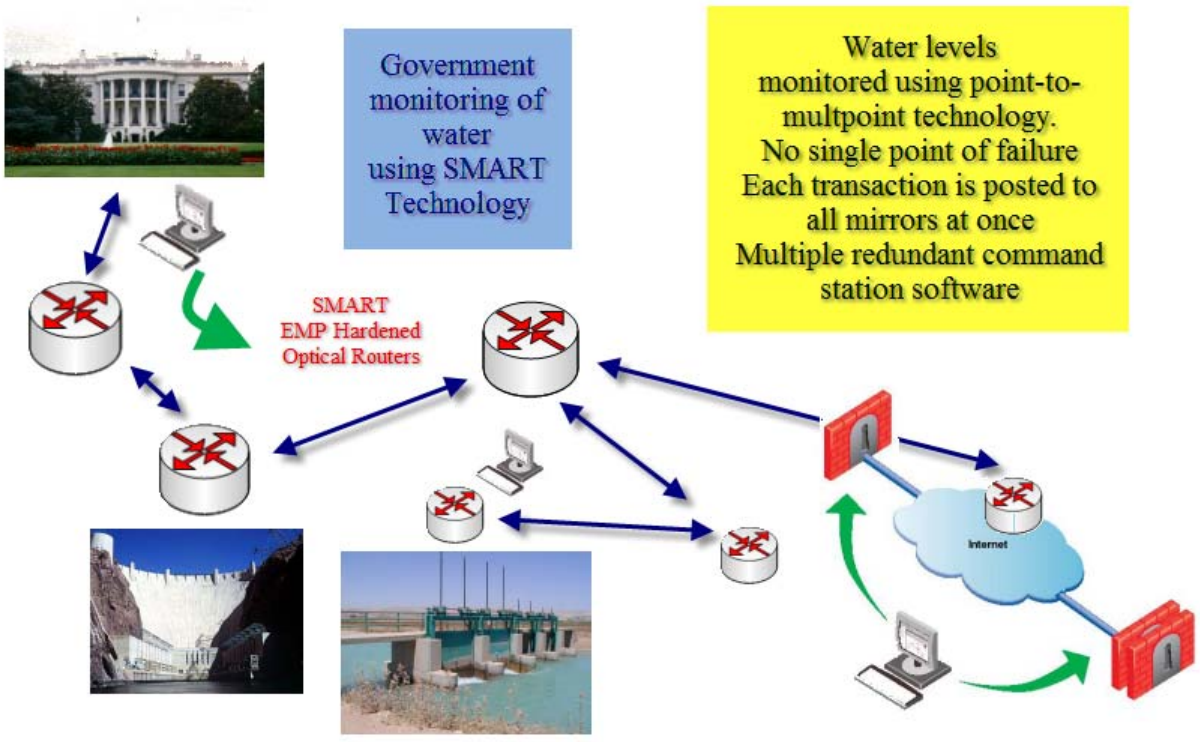

Figure 9 - SMART command and control of water resources

Contemporary Emergency Alert System Failure Due to EMP/S

An EMP attack or serious magnetic storm would knock out broadcast antennae and TVs connected to cable or over the air reception antennae. This would completely disable the Emergency Alert System.

By using SMART point-to-multipoint fiber based technology, a system could be created that would be impervious to EMP/S. Homes powered by natural gas or hydrogen could easily be made EMP/S resistive with screening.

The point-to-multipoint base infrastructure that SMART technology is built upon provides the ability to have Secure Reliable point-to-multipoint communications that also contain a feedback mechanism. The feedback mechanism provides the operator a method to discover the end-user quality of service. With this feature, the total numbers hearing the emergency transmission can be known. Monitoring traffic for SMART systems will allow government agencies to identify the hardest hit areas. SMART security is a plug-in module that is currently set to use Advanced Encryption Standard (AES). AES is currently the mechanism for "top secret" documents used by the U.S. government.

The SMART distribution system for television or data

Why point-to-multipoint can support mass scale

Worldcast has developed an Internet software solution for worldwide television to mass audiences bringing economic opportunities and consumer benefits.

SMART sends one signal to millions simultaneously. It is exponentially cost- and bandwidth-efficient when compared to Unicast transmission. Unicast bandwidth cost is per customer with no economy of scale (in fact, it doesn't scale). SMART's efficiency increases with each customer added and the cost approaches zero-per-user in mass media application.

With SMART, worldwide "cable" companies are now possible. SMART is another step in the convergence of communication technology, bringing the power of the computer and the Internet to the living room television and more. SMART is ubiquitous, able to transport video across all systems (cable/copper, fiber and wireless) to all devices (living room television, computers and all types of mobile devices).

SMART has been lab tested and is in operation now.

The need:

The quantity of data traveling across the Internet is growing at an almost exponential rate. For Internet service providers (ISPs), bandwidth, or the lack thereof, is becoming a critical issue. In order for video or data to be received with acceptable frame rate or clarity and speed, Internet congestion must be managed. Current technology – commonly called Unicast – requires sending a separate signal for each end-user; therefore, audiences larger than a few hundred thousand are not possible without causing congestion and loss of quality. These systems can easily consume more bandwidth than is available. Simply put, current streaming media systems are complex, capital-intensive bandwidth hogs.

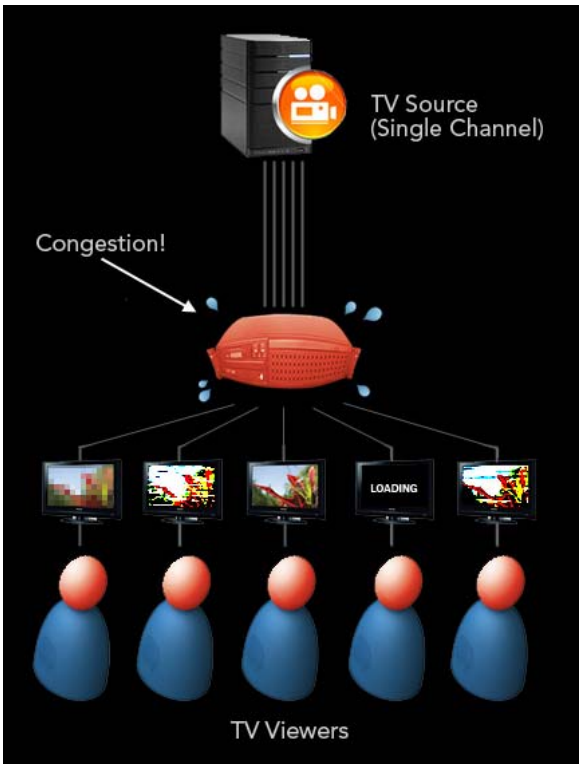

Figure 10 - SMART technology as is relates to television

By comparison, SMART is an elegant software system that is far less expensive to operate and far easier to implement. With Worldcast's patented, secure, reliable SMART technology, one signal can be sent to millions simultaneously, with a cable-like quality picture, making it possible to launch a television system over the Internet. SMART combines television with the power of the computer, making full interaction with the viewer possible, all at exponentially reduced costs. Applications extend far beyond just television and include: video movie rental, video conferencing, military applications, broadcast to portable/mobile devices and command and control.

The solution:

SMART makes use of existing Internet protocols, and then adds the point-to-multipoint functionality that hereto has been missing. A protocol is a set of rules used by all Internet communications. Protocols in use today are well established, e.g., Transmission Control/Internet Protocol or TCP/IP. SMART technology has been through rigorous testing in the University systems.

Worldcast holds the key to multipoint infrastructure network solutions, for which it holds five patents (three issued and two published/pending). Worldcast's technical staff has over eleven years experience in SMART research and development.

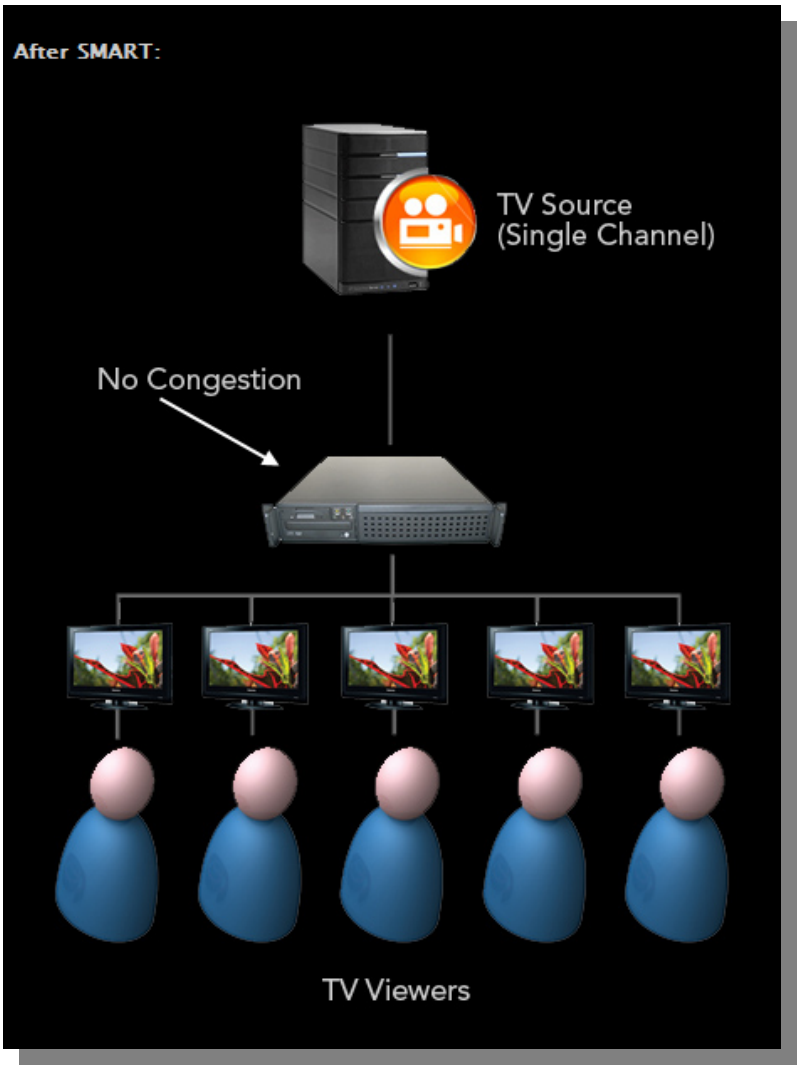

Figure 11 - SMART allows for large audiences

Base Infrastructure Compatibility

Internet 6 IPV6 and multipoint communications

As we move to the next level on the Internet2, there are some missing elements in the model for "any source" point to multipoint connectivity. "Any source" connectivity is required to provide redundant sources for point-to-multipoint connectivity. The missing link in the multipoint model for IPV6 is the lack of support for a Multipoint Discovery Protocol. Worldcast has assembled a team of distinguished individuals to affect a permanent fix for this problem.

Proposal from Vint Cerf, Ian Stewart, Kevin Almeroth and Paul Vixie provides source discovery for IPV6

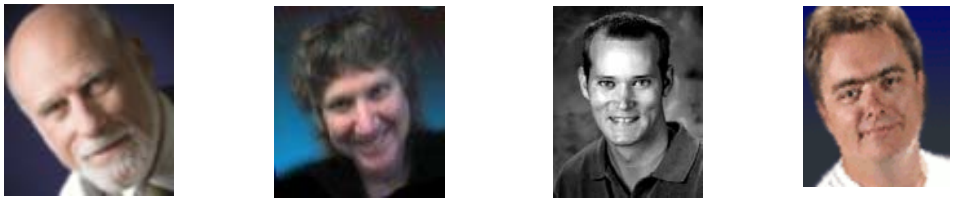

Figure 12 - Vint Cerf, Ian Stewart, Kevin Almeroth and Paul Vixie

The DP-DPO project

The E-SUPER DOMINO's sub project, DP-DPO, has the distinguished members Vint Cerf, Ian Stewart, Kevin Almeroth and Paul Vixie. The DP-DPO project was created to patch Internet 6 multipoint connectivity hole. A multipoint discovery mechanism is currently not available for Internet 6.

The DP-DPO is an IRTF draft in progress.

For more information please contact:

Worldcast

Jucival Dos Santos, MBA - COO - Board Advisory Member

Office: 213-787-6682 • Cell: 310-869-1634 • jdossantos@worldcast.tv

4125 Market St., Suite 18, Ventura, CA 93003

www.worldcast.tv