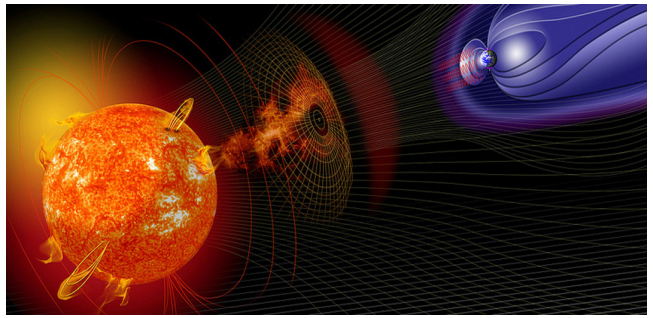
RISKs TO THE HYPERLOOP

There are numerous risks that could cause damage to the development and operation of the hyperloop

A few will be discussed including risks to the US electrical infrastructure that Hyperloop depends on for operation



Al Florence – Lakewood, Colorado
Multidiscipline Systems Engineer
Colorado Electromagnetic Pulse (EMP) Task Force
Retired from a Washington D. C. Think Tank
alflorence123@gmail.com

REAL RISKS to the HYPERLOOP

The following are some project areas and activities that require attention to prevent them from becoming risks to projects

- **Project Planning** – Project planning starts early during the concept phases and continues all the way through product retirement; plans are developed for all aspects of management, engineering, production, operation and retirement
- **Procurement** – Many activities during procurement can cause risks during development and operation; request for proposals (RFPs), contractor selection, technology selection, development schedules, budgets, etc.
- **Project Management** – Project managers needs to have project management skills especially in the process and technical areas of the project
- **Requirements/Capabilities** – Requirements and capabilities need to be vetted, and approved by all stakeholders, they need to specify what is required and must be achievable within cost and schedule
- **Design** – Design needs to be traceable and satisfy all requirements and must be testable to insure all requirements have been satisified
- **Interfaces** – Interfaces that connect various system entities need to be identified and properly implemented (an Itnerface Control Group needs to be established)

REAL RISKS to the HYPERLOOP

Project areas and activities that require attention to prevent them from becoming risks to projects (Continued)

- **Tests** – Tests that validate all requirements and design need to be developed and executed to ensure end products are developed to specifications
- **Configuration Management (CM)** – CM that baselines and manages changes to plans, requirements, design, test cases, budgets, schedules, hardware, software, etc. has to be planned and implemented
- **Quality Assurance (QA)** – QA that assures the quality of all management and engineering activities, specifications, design, construction, test cases and test results, etc. needs to be implemented
- **Earned Value Management** – Earned Value for measuring project performance and progress in an objective manner needs to be implemented
- **Change** – Change happens, it happens all the time especially in our modern changing world, it happens on anything and everything. Organizations that do not plan for, manage and mitigate, change quickly disappear, this is demonstrated all the time. Changes to hyperloop may be: technology, design, capabilities, funding, schedules, interest, laws and regulations, key personnel, and many others.

RISKS to the HYPERLOOP

Project areas and activities that require attention to prevent them from becoming risks to projects (Continued)

- **Measurement and Analysis** – Collects and analyzes engineering, management, cost, schedule, etc. data and makes appropriate corrections as required
- **Project Milestone Reviews** – Reviews at specific stages of development that reviews technical, management, schedule and budget items/issues and makes corrections as necessary
- **Independent Verification and Validation (IV&V)** – Independent oversight of critical aspects of programs: management, engineering, and development activities
- **Redundancy** – Redundant system applications for critical actions and activities of the systems; double redundancy for critical ones and triple redundancy for the most critical
- **Risk Management** – Identifies management and technical risks and attempts to mitigate them before they are realized and may cause major harm to the project

REAL and DANGEROUS RISKS to the HYPERLOOP

Hyperloop Depends on Electricity for Operation

The threat of the U.S. power grid crashing is a very real and the severity of vulnerability under which we live. Experts say our power grid, or portions of it, can be destroyed by an electromagnetic pulse (EMP). Experts also say it is not a mere possibility but a near certainty that the grid will be hit and it could happen at any time.

An EMP can be caused by a nuclear detonation above our atmosphere in low earth orbit (LEO)
or by a solar storm, a coronal mass ejection (CME)

- **An EMP or CME can destroy transformers of the electric power grid and other portions of the US electrical infrastructure**
- **Once transformers are destroyed, due to EMPs or CMEs, they do not come back and have to be replaced which may take months if not years**
- **Other threats to the power grid are major physical and cyber attacks**
- **Without electricity the nation or regional areas would be effected including the hyperloop**
- **The hyperloop, dependent on electric power, would come to a complete halt**
- **Passengers in the hyperloop without electrical power would not be able to escape and may not survive**

These are MAJOR risks to the hyperloop which requires major attention

Search: Nuclear electromagnetic pulse: How it works

Reference

GRID SECURITY THREATS 2013-2015

Dr. Peter Vincent Pry
EMP Task Force on National and Homeland Security

Coronal Mass Ejection (CME) capable of generating catastrophic geomagnetic super-storm narrowly missed Earth on July 22, 2012. NASA estimates the likelihood of such a storm hitting Earth to be 12 percent over the next decade--which virtually guarantees a natural EMP catastrophe will happen in our lifetimes or that of our children.

EMP field coverage increases with increasing height-of-burst. A balloon or jet aircraft could loft a nuclear warhead to an altitude of 30 kilometers would cause an EMP which, targeted over New York City, would also cover Washington, D.C., New York State, New Jersey, Pennsylvania, Virginia, Maryland, Delaware, and most of New England.

North Korea has tested nuclear weapons, including reportedly a 'super EMP' design obtained from Russia, has repeatedly threatened the U.S. with nuclear attack with an orbited satellite that could be used in an EMP strike and has collaborated closely with Iran on nuclear.

North Korea's KMS 3-2 satellite is compatible with the size and weight of a small nuclear weapon – particularly one optimized for EMP effects – and is orbiting at an altitude suited for such use. It also approaches the U.S. from the south, a direction which lacks early warning or missile defenses.

Reference

guilty knowledge

What the US Government Knows about the Vulnerability of the Electric Grid, But Refuses to Fix

Introduced by Frank Gaffney, Jr. - President and CEO, Center for Security Policy

FOWARD On January 21, 2014, Fox News aired a segment describing the vulnerability of the U.S. bulk power distribution system, popularly known as the electric "grid." The report described various dangers that could cause the grid to fail, possibly catastrophically. These range from physical and cyber attacks on its subsystems to space weather and a high-altitude nuclear detonation unleashing intense electromagnetic pulses (EMP) that could afflict the grid across vast areas. Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication. The electromagnetic fields produced by weapons designed and deployed with the intent to produce EMP have a high likelihood of damaging electrical power systems, electronics, and information systems upon which American society depends. Their effects on dependent systems and infrastructures could be sufficient to qualify as catastrophic to the Nation.

EXECUTIVE SUMMARY The last few years have seen the threat of a crippling cyber-attack against the U.S. electric grid increase significantly. Secretary of Defense Leon Panetta identified a "cyber-attack perpetrated by nation states or extremist groups" as capable of being "as destructive as the terrorist attack on 9/11. A five-year old National Academy of Sciences report declassified and released in November 2012 found that physical damage by terrorists to large transformers could disrupt power to large regions of the country and could take months to repair, and that "such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction." On May 16, 2013, the Department of Homeland Security testified that in 2012, it had processed 68% more cyber-incidents involving Federal agencies, critical infrastructure, and other select industrial entities than in 2011. It also recently warned industry of a heightened risk of cyber-attack, and reportedly noted increased cyber-activity that seemed to be based in the Middle East, including Iran.

Reference

EMP Task Force on National and Homeland Security 501(c)(3)
Dwight L. Echert - Colorado State Director

What is Electromagnetic Pulse (EMP)?
A Transient Electromagnet Disturbance, a burst of Electromagnet Energy
Sources Include: Natural Sources, Meteoric EMP, Solar Weather, Man Made Sources, Non-Nuclear EMP, Nuclear Weapon

Some Solar Weather Events:

Google: Carrington event probability

- **Carrington Event Sept 1, 1859**
  - **Auroras Borealis visible in Hawaii, Cuba, Jamaica, El Salvador and the Bahamas**
  - **Telegraph capabilities destroyed, this was the advanced technology of the time**
  - **Messages transmitted with batteries disconnected**
  - **It was a 150 year event (or was It?)**
- **Significant events also occurred on Nov 18,1882**
  - **All telegraph transactions east of the Mississippi & north of Washington D. C. came to a halt**
- **Aug 4, 1972: destroyed telephone communications in Illinois**
- **March 13, 1989: Hydro Quebec (6 million people for 9 hours in blackout) melted power transformers in NJ**
- **Halloween 2003: power outage in Sweden, satellites damaged, Aurora Borealis seen in Texas**
- **Dec 5, 2006: disrupted satellite communications for 10 minutes including GPS**
- **July 23, 2012: CME nearly missed Earth by 9 days (may have exceeded Carrington event)**

Satellite Systems Are Typically Designed to the 1989 Event
If Events Closer to the Carrington Event Were to Occur….. (Scientifically Speaking: "WOW!")

Reference

Colorado Electromagnetic Pulse (EMP) Task Force

Glenn Rhoades, Director National Operations EMP Task Force on National and Homeland Security;

Dwight L. Eckert, Director State of Colorado EMP Task Force on National and Homeland Security;

Al Florence, Multidiscipline Systems Engineer, Colorado EMP Task Force

Without a functioning electric grid our modern civilization could not survive. The U.S. Electric Grid is susceptible to the effects of Electromagnetic Pulse (EMP) from either natural or manmade causes. Although the complexity of the grid and the physics from the effects on the grid make the exact outcomes of an event highly unpredictable, it is not beyond careful extrapolation that Coloradans will be affected. Based on scientific analysis from at least five national reports, including the US Congressional EMP Commission and the National Academies of Science the electrical power grid could experience irreplaceable destruction due to an EMP event. Within the first few months of an EMP or Geomagnetic Disturbance (GMD) event, as few as a million to a few hundreds of millions could be at risk of dying or being injured through 1) societal chaos, 2) disease, especially water borne illnesses like cholera, diphtheria, and typhoid, and 3) starvation.

Although this is of national concern, the Colorado EMP Task Force has been established to work Colorado specific concerns as well as to support the national interests. There currently exist various groups operating in Colorado that are raising public awareness to these threats including The EMP Task Force on National and Homeland Security, The InfraGard EMP SIG, The Secure the Grid Coalition, The Foundation for Resilient Societies, National Oceanic and Atmospheric Administration (NOAA), The Colorado Department of Public Safety and Homeland Security and the Electric Infrastructure Security (EIS) Council. The Colorado Task Force will work to prepare our state and our civilization for such an event through efforts to educate, prepare for, prevent or recover from the threats caused by either an EMP or GMD event.

Reference

Idaho National Laboratory (INL) a U.S. Department of Energy National Laboratory

Strategies, Protections, and Mitigations for the Electric Grid from Electromagnetic Pulse Effects

The mission of the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) is to lead national efforts to modernize the electricity delivery system, enhance the security and reliability of America's energy infrastructure, and facilitate recovery from disruptions to the energy supply. One of the threats OE is concerned about is a high-altitude electromagnetic pulse (HEMP) from a nuclear explosion and electromagnetic pulse (EMP) or an early time E1 pulse (a very fast component of a nuclear EMP) which can be generated by EMP weapons. INL was chosen to conduct the EMP study for DOE-OE due to its capabilities and experience in setting up EMP experiments on the electric grid, conducting vulnerability assessments, and developing innovative technologies to increase infrastructure resiliency. Strategies for applying EMP mitigations to the electric grid include characterizing the threat based on current and expected (nuclear and EMP) weapons in the inventory of potential adversaries (not on U.S. or Soviet nuclear weapons from the 1960s or 1970s), baselining the impact of EMP on modern grid technologies, baselining the mitigations, and sharing results to inform methods and toolsets for utilities to do their own trade-off analyses for protecting against the EMP threat. Among the greatest challenges is a lack of knowledge or strategy to mitigate new risks that emerge as a result of an exponential rise in complexity of modern control systems.

- **Growth of networks and communication protocols used throughout ICS networks pose vulnerabilities**
- **Threat actors on multiple fronts continue to seek to exploit cyber vulnerabilities in the U.S. electrical grid**
- **Utilities often lack full scope perspective of their cyber security posture**
- **The assortment of regulatory standards and guidelines applicable to utilities regarding cyber security practice produces varied methods of adoption**
- **Utilities expect more qualitative, timely threat intelligence from existing federal information sharing programs**

Reference

Powering Through – From Fragile Infrastructures to Community Resilience

InfraGard

We take electric power for granted. Threats to our electric grid are real, how to prepare. Powering Through is an action guide and contains, for the first time, a comparison of critical infrastructures that can suffer long duration outages caused by five high impact threats: high altitude Electromagnetic Pulse (HEMP); solar geomagnetic storms; cyber-attacks; physical attacks; and Radio Frequency (RF) weapons. We are accustomed to short duration power failures. However, disruptions of weeks, months, or over a year are more and more possible, yet this risk is largely unrecognized. The book examines the interdependent, and critical, infrastructures that would be threatened by a sustained electric grid failure, such as our water and wastewater systems, communications, transportation, emergency and healthcare services, government and military defense, to name only a few. Importantly, the book concentrates on consequence management, starting at the individual, household, and community levels of preparedness. If we are better prepared at home, we can better assist the organizations that will lead recovery, whatever the challenges. In addition, the book sets out a plan for forming resilient community islands which can ultimately aid in recovery. Ultimately, Powering Through offers hope, via thorough and concrete expert advice, not just to individuals, but to local, state and federal government, emergency organizations, and others, that they can prepare for this very real threat to our electric grid. And what's more, this book heralds a call to action for these same groups to begin preparing NOW.

Reference

SPACE WEATHER PREDICTION CENTER NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION (BOULDER COLORADO)

About Space Weather
- Impacts
  - Earth's Climate
  - Electric Power Transmission
  - GPS Systems
  - HF Radio Communications
  - Satellite Communications
  - Satellite Drag
- Partners and Stakeholders
  - Commercial Service Providers
  - Federal Agencies
  - International Organizations
  - International Service Providers
  - Space Weather Research
- Phenomena
  - Aurora
  - Coronal Holes
  - Cots/Solar Cycle
  - Total Electron Content
- Additional Info
  - NOAA Space Weather Scales
  - ronal Mass Ejections
  - Earth's Magnetosphere
  - F10.7 cm Radio Emissions
  - Galactic Cosmic Rays
  - Geomagnetic Storms
  - Ionosphere
  - Ionospheric Scintillation
  - Radiation Belts
  - Solar EUV Irradiance
  - Solar Flares (Radio Blackouts)
  - Solar Radiation Storm
  - Solar Wind
  - Sunspo**Products and Data**

- Forecasts
  - 27-Day Outlook of 10.7 cm Radio Flux and Geomagnetic Indices
  - 3-Day Forecast
  - 3-Day Geomagnetic Forecast
  - Forecast Discussion
  - Predicted Sunspot Numbers and Radio Flux
  - Report and Forecast of Solar and Geophysical Activity
  - Solar Cycle Progression
  - Space Weather Advisory Outlook
  - USAF 45-Day Ap and F10.7cm Flux Forecast
  - Weekly Highlights and 27-Day Forecast
- Reports
  - Forecast Verification
  - Geoalert - Alerts, Analysis and Forecast Codes
  - Geophysical Alert
  - Solar and Geophysical Event Reports
  - USAF Magnetometer Analysis Report
- Models
  - Aurora - 30 Minute Forecast
  - D Region Absorption Predictions (D-RAP)
  - Geospace Geomagnetic Activity Plot
  - Geospace Ground Magnetic Perturbation Maps
  - Geospace Magnetosphere Movies
  - North American (US Region) Total Electron Content
  - North American Total Electron Content
  - Relativistic Electron Forecast Model
  - SEAESRT
  - STORM Time Empirical Ionospheric Correction
  - WSA-Enlil Solar Wind Prediction

- Observations
  - Boulder Magnetometer
  - GOES Electron Flux
  - GOES Magnetometer
  - GOES Proton Flux
  - GOES Solar X-ray Imager
  - GOES X-ray Flux
  - LASCO Coronagraph
  - Planetary K-index
  - Real Time Solar Wind
  - Satellite Environment
  - Solar Synoptic Map
  - Space Weather Overview
  - Station K and A Indices
- Summaries
  - Solar & Geophysical Activity Summary
  - Solar Region Summary
  - Summary of Space Weather Observations
- Alerts, Watches and Warnings
  - Alerts, Watches and Warnings
  - Notifications Timeline
- Experimental
  - ACE Real-Time Solar Wind
  - Aurora - 3 Day Forecast
  - Current Total Electron Content

Dashboards
- Aviation
- Electric Power
- Emergency Management
- Global Positioning System
- Radio
- Satellites
- Space Weather Enthusiasts

References

Blackout Wars

Peter Pry. State Initiatives To Achieve Preparedness Against An Electromagnetic Pulse (EMP). Blackout Wars is about the historically unprecedented threat to our electronic civilization from its dependence on the electric power grid. Most Americans have experienced temporary blackouts, and regard them as merely an inconvenience. Some Americans have experienced more protracted local and regional blackouts, as in the aftermaths of Hurricanes Sandy and Katrina, and may be better able to imagine the consequences of a nationwide blackout lasting months or years, that plunges the entire United States into the dark. In such a nightmare blackout, the entire population of the United States could be at risk. There would be no food. No water, Communications, transportation, industry, business and finance--all of the critical infrastructures that support modern civilization and the lives of the American people would be paralyzed by collapse of the electric power grid.

Cyber War

Richard A. Clarke and Robert K. Knake, 2010 novel. Few understand the devastation cyber weapons can wreak or how the United States will use them in a crisis. Security expert Richard A. Clarke goes beyond 'geek talk' to succinctly explain how cyber weapons work and how vulnerable America is to the new world of nearly untraceable cyber criminals and spies. Clarke reveals how successful foreign cyber espionage has already penetrated the Pentagon, the control systems for U.S. electric power grids, and the defense industry. While the U.S. has not yet been attacked in a full-scale cyber war, petabytes of information have already been stolen, including advanced research in aerospace, weapons systems, biotechnology, and engineering.

One Second After

William R. Forstchen, 2009 novel. The novel deals with an unexpected electromagnetic pulse (EMP) attack on the United States as it affects the people living in and around the small American town Black Mountain, North Carolina. *One Second After* was ranked as number 11 on of the New Your Times Best Seller list New Your in fiction, in May 2009

Patriarch Run

Benjamin Dancer, 2016 novel. "The description of the vulnerabilities of our infrastructures, especially that of the often neglected-to-mention vulnerability of our food supply system due to its dependency on the long term availability of electricity, seems to me both accurate and thought provoking. Or at least, it ought to be. Works such as this may serve a larger purpose than 'mere' entertainment by alerting the public, and even some government agencies, to the dangers that lurk out there while there is still opportunity to do something about them in a way that often obscure official reports and studies are unable to accomplish." *Dt. Michael. J Frankel, former Executive Director of the EMP Commission.*

Final Thoughts

These are critical risks to the Hyperloop during development and operation

These are critical but they are not alone, risks, risks, risks are all around us all the time!

- ***Risk Management Programs need to be established early during concept stages***
- ***Potential risks identified early and throughout development and operations***
- ***Mitigations strategies established to prevent them from occurring***
- ***Contingency strategies need to be developed and executed when risks are realized and become issues to the program***