Surface Transportation Moves Into the World of the Internet of Things and Data-Driven Decision Making – A Practical Guide to Getting There…

Author:
Bryan Mulligan – President, Applied Information, NEMA 3TS Transportation Section chair
bmulligan@appinfoinc.com
678-429-0379

Summary

The world is rapidly moving towards "connected everything", and the surface transportation network is no different. The idea of dedicated DSRC networks for connected vehicles is rapidly being swamped by ubiquitous shared 4G/LTE/5G/Wi-Fi networks that are being rolled out for the Internet of Things. At the same time, the long-held basis of systems engineering of user requirements being developed from user needs ("opinion engineering") is being challenged by the concept of Data-Driven Decision Making. This paper describes a practical process for achieving the benefits of the Internet of Things and Data-Driver Decision Making, and some of the challenges in implementing this new way of thinking. Some practical examples of successful implementations are also provided.

Step 1: Getting Connected to the Internet of Things (IoT)…

"The **Internet of Things** (**IoT**) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data."

It is happening on a massive scale right now, with home air-conditioning control; remote meter reading; industrial SCADA system and vehicle AVL systems among some of the technologies leading the way. Transportation systems are following this trend, and are making more use of cellular and Internet technologies for connectivity.

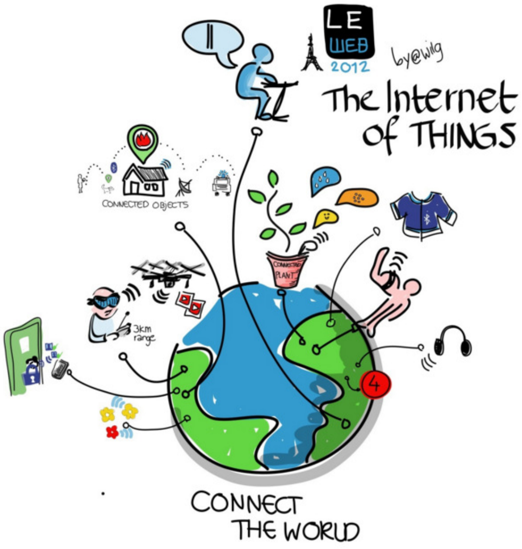


Fig 1: The Internet of Things

https://en.wikipedia.org/wiki/Internet_of_Things

However, this adoption of Internet of Things technologies is meeting resistance in the surface transportation arena because:

1) State, City and County Departments of Transportation are used to "dedicated infrastructure". This includes the history of dedicated copper wires and fiber optic systems that have been installed over the past decades. There is a great deal of institutional history of being "asset managers" and procurement, maintenance and operational procedures lend themselves to asset management of dedicated systems.
2) There is huge suspicion of the "security of the Internet…" and so this topic is dealt with separately in Step 2 below.
3) Budgeting and procurement processes are geared towards purchasing assets. It is difficult for Federal, State and City transportation funds to be applied to multi-year "software-as-a-service" and data contracts, which often require monthly payment commitments.

The vendor market is responding to these resistance factors as follows:

1) The costs of Internet of Things based systems, with its fundamental premise of reduced cost due to savings made possible by shared computing and communications infrastructure, is proving to be much, much lower than the cost of bespoke, custom, dedicated systems. The multi-million dollar systems, with huge dollar and organizational cost of entry, are becoming less frequent. Systems which minimize the cost and complexity of ownership, due to savings by using shared infrastructure, are becoming the only affordable way of deploying ITS systems for smaller agencies.
2) Vendors are bundling cell connection costs, maintenance cost, software-as-a-service (SaaS) costs into up front capital costs. This means that agencies can purchase these new services using their traditional asset purchase procurement procedures, without the difficulty of budgeting for monthly expenditure.
3) Security for the Internet of Things has largely been addressed by the financial services sector (Internet banking). Government departments are doing all sorts of business (including financial transactions) over the Internet. This move towards a 'trusted Internet' has made it more acceptable to bring transportation system onto the Internet, subject to similar security process being used. More on this in Step 2 below…

Traditional systems engineering in surface transportation has been based for several decades on the concept of knowing 'some of the things about some of the things for some of the time'. For example, it would be typical to do a traffic study for traffic volume for a couple of roads for a couple of weeks, and then extend the results of the study to all roads in a network. However, this approach tended to be single purpose. The planning traffic data (based on volume) gave no insight into speed enforcement and traffic safety. Each data sampling process was designed to answer a specific question in the systems engineering process.

The Internet of Things is changing this fundamental premise. The goal of ‘big data’ is to have the data about ‘everything about everything all the time’. This means that you can collect all the traffic parameters from all the roads all the time. The resulting large data set can then be mined to provide information for planning, traffic safety, speed enforcement, with seasonal and long term trending and any other queries that come up for improvement in the surface transportation network. This move away from ‘opinion engineering’ to ‘data-driven decision making’, with the resultant improvement in the quality of decision making, is one of the key benefits of the Internet of Things approach.

Step 2: Security

Often the initial reaction to the idea of shared Internet infrastructure is “surely it can’t be safe?” This response is entirely appropriate given the stories one hears on the news about hacking and data breaches. However, when analyzed, these security events are largely database access issues, or user access issues such as phishing. The actual communications over the Internet is remarkably secure. The HTTPS standard has proved very resilient and reliable in providing security to the communications at the core of the Internet.

The NEMA 3TS Transportation Section (the developer of the TS2, TS4 and other standards) is currently in the process of developing the NEMA TS8 Cybersecurity Standard for Transportation System. This standard addresses cybersecurity concerns, and methods for security risk mitigation, in four areas:

1) *Physical Security*: locks, cabinets, physical access control and similar topics related to keeping the devices, networks and systems physically secure.
2) *Local Access Security*: Topics related to local access passwords, “back-door” passwords, and the security of the local user interface used to configure and control the device when the user is physically located at the device.
3) *Communication Security*: Topics related to the encryption of the communications between the field device and central, including legacy and NTCIP communication.
4) *Central System Security*: Topics related to the security of the central computer system and database.

This standard, when published (the target publish date is late 2016), will provide some clear guidance on implementing security for transportation systems.

The end result of this effort, along with continued improvement in Internet security, will provide agencies the confidence for transportation devices and systems to take their place in the Internet of Things.

Step 3: Turn Your Data into Actionable Information

Given that the paradigm changes to "knowing everything about everything all the time" the result is massive quantities of data becoming available for analysis. Large quantities of data come from devices connected to the Internet of Things, and by itself this data does nothing to improve transportation. The key to improving transportation by using the data is by transforming this data into information.

"Information is data, in context, made useful"

There are many resources on the topic of turning data into information, and this discussion could make up many technical papers. However, there are a few key concepts which allow data to be sensibly managed and turned into useful actionable information.

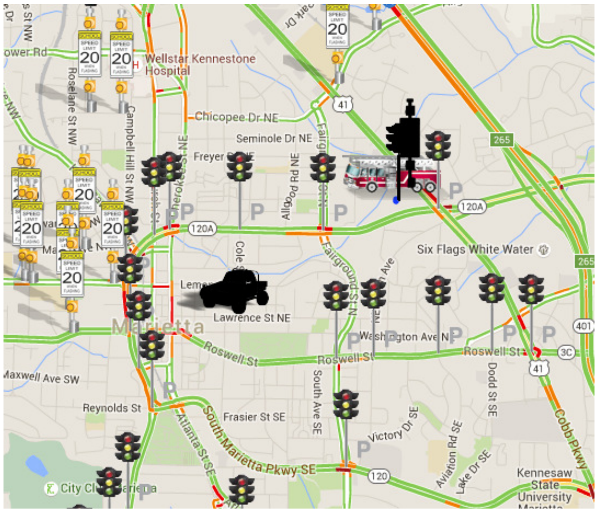


Fig 2: Integrated Web browser user interface for the City of Marietta, GA showing traffic data, intersections, school beacons, and emergency vehicles connected via the Internet of Things

1) *Abnormal situation management*: One of the keys to using data effectively is the ability to extract and highlight abnormal situations that require actionable response in near real time. The Internet of Things approach of devices being continuously connected, allows the data to be pushed out when change in the device data/sensors occurs. The central/cloud system can then apply business rules and threshold to determine whether an abnormal situation has occurred. This in turn can create an alert on a text or email to the responder, whose response to the abnormal situation can then be measured.
2) *High Performance HMI (Human Machine Interface)*: Many industries, including the industrial process control industry, have experience in man-machine (computer) interfaces, and have published "lessons learned". These lessons in interface implementation are equally applicable to the transportation industry.

   "A picture is worth a thousand words. An interface is worth a thousand pictures." – Ben Shneiderman

“No matter how cool your interface is, less of it would be better.” – Alan Cooper

3) *Cloud computing and Web browser interfaces*: Modern computer system no longer require a physical infrastructure. Cloud computers can provide a scalable, secure computing infrastructure from the smallest city to the largest enterprise, without the enterprise needing physical computers or networks. Software no longer needs to be installed on client computers, as modern systems use standard Web browsers for the user interface. This has also made modern system computer platform independent, as the standard Web browsers run on Apple or Windows, and mobile, fixed and transportable platforms. The operations center of the past is being replaced by iPads and the like, which can be accessed by the responsible operators anywhere.

The following case studies are examples of early deployment of the technologies described above, and illustrate how the combination of the data retrieved via the Internet of Things when combined with visualizing the data – turning the data into information – can help answer some difficult questions.

Case Study 1: Are Your Roads Safe For Travel in Bad Weather?

A number of weather instrument manufacturers are releasing the next generation of road weather instruments. These instruments are attached to patrol vehicles and measure the road temperature, water film height, road condition and other road parameters while the vehicle is driven at highway speeds. The combination of these instruments (sensors), Internet of Things connectivity (connected vehicles) and data visualization (turning data into information) allows the road agency to make a data-driven decision in real time whether the roads are safe for travel or not.

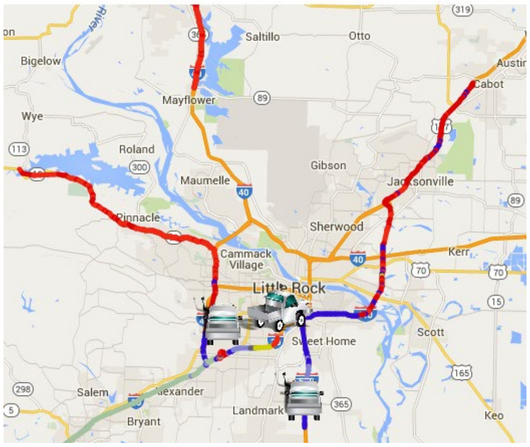


Fig 3: Little Rock, AR during the winter weather event of Jan 16, 2016 showing some roads (in the south) safe for travel, and other roads(mainly in the north) unsafe for travel

The examples provided here include:

1) *Winter road travel*: The information provided on road condition, grip level, air and road surface temperature over a wide area allows the agency to make data-driven decisions on school closings, road closings and active traffic management decisions such as reducing the speed limits using variable speed limit signs.

2) *Travel during heavy rain*: Increased water film thickness on the roadway results in a lower grip for the vehicle, and the risk of hydroplaning at highway speeds. Crash statistics show an increased risk of crash during bad weather. The water film thickness when visualized (turned into information) makes it possible for data-driven decisions on reducing the speed limit or public notification of the danger. In addition, this approach will provide a data-driven assessment of places where there is poor drainage of the roadway, resulting the increase in standing water (with the resultant increased risk to vehicle travel)

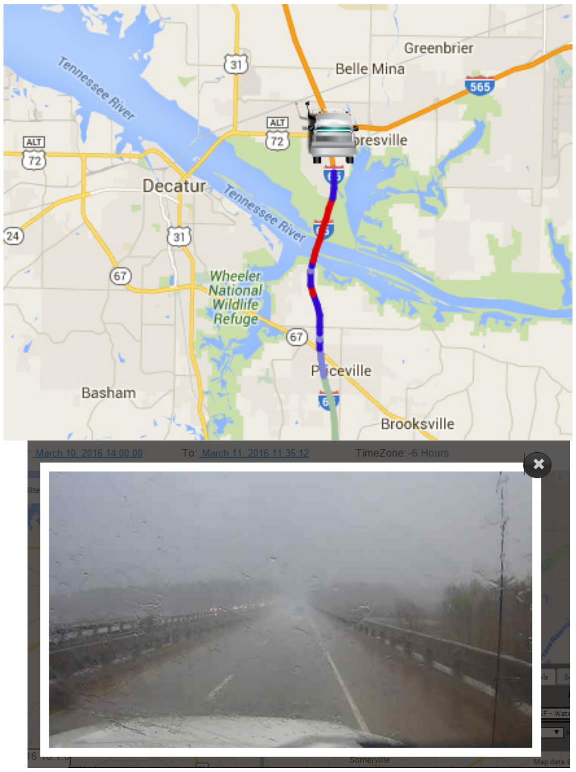


Fig 4: Crossing the Tennessee River bridge on March 10, 2016 during heavy rain. The data shows in real time the critical water film thickness, resulting in a risk of hydroplaning. Visual confirmation is provided by the dash-cam in real time.

Case Study 2: Are your School Beacons Slowing the Traffic as Intended?

There are approximately 100,000 schools in the United States. A key part of the strategy to keep the children safe during the start and end of the school day is to reduce the speed limit locally while the busses and parent vehicles are loading and offloading the children. This strategy has been in place for many decades. However, the question remains: “Are your school beacons slowing the traffic as intended?”

As school beacon systems become part of the Internet of Things with “always on” monitoring and control, the answer is provided in three sections, as described below:

1) *Are the school beacons actually working?* Many systems use solar power with batteries to power the beacon, and it is very difficult to tell by visual observation whether the beacon is working properly or not. When the technician drives by the beacon, the beacon is off most of the time. This is the normal condition for a school beacon, which is the same as being broken. Even testing during the day (when the sun is shining) does not tell the technician if the beacon will work at night/early morning, when the solar panels are not charging. However, by bringing back all the data on the solar panels and batteries (or AC supply as appropriate) the business rules engine can immediately alert the agency to any problems in the operation of the school beacon. In this way the agency can have confidence that all the devices are working properly.

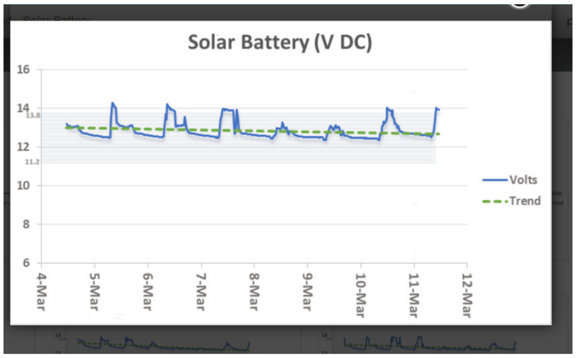


Fig 5: A typical voltage profile from a well-maintained solar school beacon in Sugarland, TX, showing the reduction in peak voltage in the cloudy/stormy days of March 9/10, 2016.

2) *Are the school beacons turning on and off at the right time?* The schedule of when to turn on/off the school beacon ends up being quite complicated in practice. The typical school has normal time (morning and afternoon, Monday to Friday); early release days (on/off at different times on some days); holidays (beacons off on some days) and delayed start (winter weather events). By having the beacons continually connected to the Internet of Things, the schedule can be downloaded and updated at any time, and the current operation of the beacon reported.

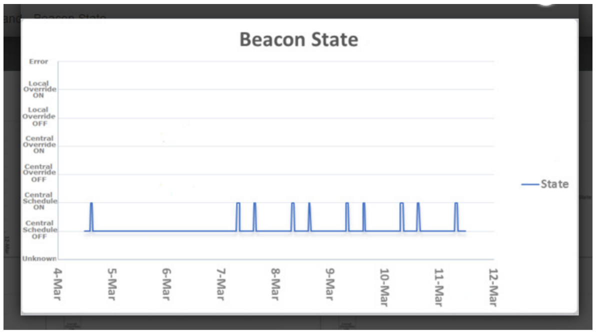


Fig 6: A typical data-visualization of confirmation of the operation of a school beacon during a typical week. Beacon goes on twice a day during the week, and off at weekends.

3) *Are the vehicles slowing down to the speed limit?* The intention is that vehicles obey the posted speed limit, and then slow down to the revised speed limit when the school beacon is flashing. However, does the traffic slow down as expected?

By adding an inexpensive radar detector to the school beacon, the data of the median speed; the 85th percentile speed and the traffic volume can be continually brought back from each school beacon location over the Internet. This data can be turned into information for analysis, and an assessment made based on the data whether additional enforcement or traffic engineering is required to slow down the traffic, and keep the children safe.

	Powers Ferry – Heards – West Bound
Median Speed with beacons ON (mph)	33.9 MPH
Median Speed with beacons OFF (mph)	41.2 MPH(+22%)
85th Percentile Speed with beacons ON (mph)	40.6 MPH
85th Percentile Speed with beacons OFF (mph)	45.9 MPH (+13%)

Fig 7: A typical speed reduction due to school beacon operation ins Sandy Springs, GA. The road is has a 35 MPH posted speed limit.

Case Study 3: Are Your Emergency Vehicles Getting There in Time to Save Heart-Attack Victims?

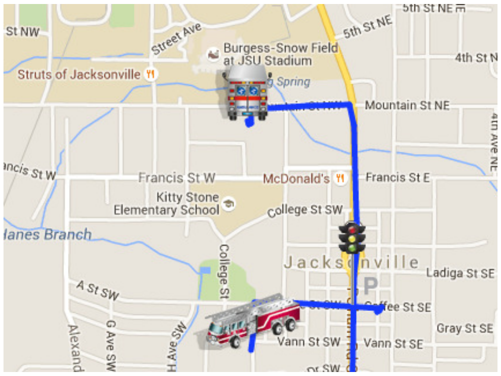
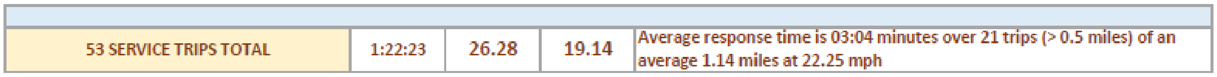


Fig 8: Typical data-visualization of the trails drawn by connected emergency vehicles and ambulance in Jacksonville, AL.

Connecting emergency response and transit vehicles can provide improved priority and preemption performance at intersections. This is the promise of "connected vehicle technology" which is being brought into practice using the Internet of Things connectivity, and not having to wait for DSRC implementation. However, as a by-product of always being connected, and knowing "everything about everything all the time" the data can be mined for the average response time of an emergency vehicle to an incident, as it is known where the vehicle is traveling, and whether the light-bar (and siren) is on or off. This average response time will tell the agency if the vehicles are getting to the emergency in the target response time; if the response time is trending shorter or longer; and whether the time saved using preemption will result in the para-medics arriving in time to save heart-attack victims (where time is of the essence).



53 SERVICE TRIPS TOTAL	1:22:23	26.28	19.14	Average response time is 03:04 minutes over 21 trips (> 0.5 miles) of an average 1.14 miles at 22.25 mph

Fig 8: Typical analysis of trip repose time for a para-medic emergency response vehicle over a period.

References

(1) Internet of Things: Wikipedia https://en.wikipedia.org/wiki/Internet_of_Things

(2) The High Performance HMI Handbook. Hollifield, Oliver, Nimmo and Habibi.

(3) National Electrical Manufacturers Association (NEMA) 3TS Transportation Section: NEMA TS8 Cybersecurity Standard (Working group documents)