Safety Analysis of a Conceptual ITS Network: Applying SODA to Guide Investment Decisions in Early Studies of Highly Vulnerable Systems

Rajiv Rai, Adam Harris, Christos Gkartzonikas, Hanyu Zhu
Purdue University, West Lafayette, IN 47906

Safety analysis was applied to an Intelligent Transportation System (ITS) System of Systems (SoS) architecture as a method of guiding prominent stakeholder investment decisions by identifying critical systems. In the research, a dependency network analysis technique was used to assess operability, reliability, and resilience in an operational network associated with ITS concept. A directed network was used where nodes represent component systems in a typical ITS and links represent functional dependencies between the systems. The research goal was to analyze effects of dependencies and their strength and criticality on the operability of target systems – Airport Administration and CyberCars. Systems operational dependency analysis (SODA) based modelling and analytic methods were also applied. While scope was limited to the concept of ITS in an airport for passengers with restricted mobility, the research team finds that the Airport Operational Database (AODB) and the Monitoring & Control Center (MCC) are the most critical systems for effective operability of Airport Administration and the CyberCars. Therefore, investments from stakeholders must be directed towards maintaining higher operability of these nodes.

1. INTRODUCTION

1.1 Operational Context

To meet increasing demands for air travel, airports have continued to expand their services since the 1960s. Larger airports mean greater distances for passengers between parking, ticketing, gates, and baggage. Existing airport transport systems to not provide seamless transportation throughout the airport. Moreover, there is difficulty incorporating appropriate infrastructure for restricted mobility passengers forcing them to rely on wheelchairs which are slow, non-personalized, and increases the psychological dependence of. A system consisting of autonomously operated cars that travel intelligently in a crowded airport will be an important step in future airport transport. With access to an airport operational database (AODB), such a system would integrate with other systems such as security, administration, and customer service. In this paper, an airport intelligent transportation system (ITS) with driverless podcars, or CyberCars, proposed and analyzed for transporting passengers with restricted mobility from parking to the post-security waiting lounge. While considering the problem through an system of systems (SoS) lens, modeling and analysis techniques are applied to determine the most critical systems affecting the behavior of the target system, airport administration. A hazard in an SoS is not attributable to one system, therefore SODA will be applied to guide stakeholder decisions (e.g., FAA, USDOT) and identify which systems are critical and require limited resource to improve critical systems resilience and articulate airport administration. An implementation strategy is proposed that is feasible from funding, coordination, and operational and maintenance perspectives based on the information and data collected throughout the course of this research endeavor. The availability of data is not a significant hurdle when compared to comprehensive management of large amount of data and coordination of dynamic data by AODB management systems for precise communication of information among participating systems.

1.2 Status Quo

Few airports have autonomous transportation systems: Morgantown Airport, West Virginia (1975, U.S.A), Rotterdam (1999, Netherlands), Masdar City (2010, UAE), Heathrow Airport, London (2011, U.K) and Suncheon Bay (2014, South Korea). The systems that do exist are called personal rapid transport (PRT) and consist of small pod-like vehicles transporting 2-6 passengers. PRTs are electrically powered, move on special tracks, and are computer automated. The PRT at Heathrow Airport Terminal 5 consists of passengers exiting their personal vehicle and inputting trip details, such as, number of passengers, luggage pieces, flight-time, and ticket code, at a nearby computer pick up station. This concept of ITS with driverless podcars would involve a similar setting where the passenger would enter requests through an interactive kiosk or mobile application. While having a close resemblance with a PRT, the CyberCar ITS would have key differences, such as the use of a charging station (CS) and internal airport travel providing point to point service.

The conceptual airport SoS architecture is promising but is not without challenges:

- Control: The development of software in such distributed systems is difficult and their certification poses a major problem due to unavailability of policies.
- Obstacle avoidance: Available technology includes: scanning laser rangefinders complemented by ultra-sound, radar, perception, and planning algorithm
- Localization & Navigation: A low cost solution to use the same architecture as the obstacle detection for localization.
- Fleet management: Optimizing the flow of cars to match the supply and demand is the key for better performance.

1.3 Barriers

PRT has existed for three decades, however, the technology is not widely applied due to some limitations. These limitations include cost effectively meeting demands of a busy airport and a lack of infrastructure to operate within an airport environment. A CyberCar ITS would overcome these limitations and as the technology is tested and proven safe for airport environment operations, it is expected that this system would be accepted by passengers with benefits of personalized user experience and on-the-spot service.

Like other transport systems, an intelligent driverless pod car system is capital intensive – the ITS Costs Database contains estimates of costs for side collision warning system, advanced emergency brake systems with pedestrian detection, lane departure warning systems, cost to vehicle manufacturers for embedded DSRC (dedicated short range communication equipment) which are high. [1]

A review of data from the West Virginia University (WVU) PRT system suggests that creating a directed automated transportation SoS is costlier than a complex system designed to fulfill one chief purpose. The 'redundancy' of information handling by elements drives cost in any directed SoS. The WVU PRT system, in operation since 1975, has been awarded for maintaining a 98.5% reliability, but required $120-million investment due to technology limitations at that time.

Another shortcoming of PRT systems discussed by academia and industry sector is the technology dilemma – driverless podcars cannot re-arrange their paths if the passenger changes the destination during transit.

2. PROBLEM CHARACTERIZATION

2.1 Rope Table

The Resources, Operation, Policy, and Economics (ROPE) in Table 1 shows different levels of a CyberCar ITS SoS. The ROPE table allows a better understanding of the SoS by defining levels of the problem that have been studied. The goal of this research is to help understand the effects dependencies of participating systems, the criticality for maintaining operability of a target system and improve returns on prominent stakeholder investment portfolios by focusing on developing robust critical systems. The focus of this research has been on the Resources, Operations and Policies at the α, β and γ levels as highlighted in the table.

Table 1 CyberCar System of Systems Resources, Operations, Policy and Economics Table

	Resources	Operation	Policy	Economics
α	CyberCars, commercial cars, charging stations, SSRP, airport passenger assistants, security person	Operation of a component system (e.g., Airport Passenger assistants)	Tactics, Techniques and Procedures used by components	Local budgets (e.g., manpower, maintenance, equipment cost, etc)
β	Monitoring & Control Center, electricity provider, airport administration, AODB.	Local assigned goals (e.g., MCC uses dynamic AODB to receive passenger requests and assign CC)	Standard Operating Procedures for a collection of components	Operations/ deployment budgets. (e.g., maintenance)
γ	FAA, Cybernetic transport system policy makers, Joint legislative committee for autonomous driving vehicles, International Air Transportation Association (IATA).	Operating collection of resource networks (e.g., DOT establishes guidelines for ITS based-on passenger acceptance)	Service Regulations, General Orders, etc. Operating Policies by lATA	Economics of a Cybernetic Transport System operating in airport
δ	Office of Secretary of State for Transportation, Environment & Regions.	Overall management of FAA and ultimate control of legislative committees, ACI-NA Cybernetic Transport system policy makers, NDRN etc.	US Airport & Ground Transportation Policies	Econ. of total national system (e.g.,Total ITS Budget for 5 years)

Table 2 A list of geographically dispersed network of semiautonomous elements

Level of Architecture	Component System
α Functioning sections	CyberCars, Charging Station, Passengers, Communication System
β For Control & Tracking	Monitoring and Control Center, Airport Operational Database
γ Chief Policy Makers	FAA, U.S. Department of Transportation
δ Ultimate Planners	Office of Secretary of State for Transportation

A taxonomic distinction based on Maier's architecting heuristic principles[2] is proposed in the Appendix. The table divides the SoS of interest into classes such that the members of each class share distinct attributes, and whose design, development, or operation poses distinct demands.

2.2 Summarizing the Problem

The important elements of the ROPE table pertaining to the basic architecture of an ITS SoS is described in Table 2

A typical ITS involves the following components[3].

1. Transportation Centers: combination of human operators and computers charged with monitoring and/or managing a transportation system- monitoring and control center (MCC) in Figure 4. It resembles: transit management, fleet and freight management.
2. Vehicles: USDOT's focus on driverless connected vehicles includes wireless communication, on-board sensors, navigation, and infrastructure to respond to threats on the vehicle roadway.
3. Field Devices: A wide range of field devices can be used to reduce congestion and improve

safety, e.g., parking guidance and count systems.

4. Travelers: Airlines identify four SSRP types:
   a. Can climb stairs and move around but still needs wheel chair
   b. Cannot climb stairs, and needs a wheelchair
   c. Disability of the lower limbs but sufficient personal autonomy
   d. Completely immobile, always needing a wheelchair and attention
5. Communication Systems: Communication is the link between all aspects of ITS. Data transmitted over high speed networks wirelessly. Technology must match requirements of the system.

From Table 2 all resources in a typical ITS belong to α level except the MCC and AODB.

Although Figure 1 points out the main systems participating in information transfer, it can be understood that as the number of components increase, a point would occur when the MCC is still processing data from one run when a second run begins. This leads to scaling problems where the network links can become clogged from the traffic i.e. inability of components to send/retrieve real time information from AODB – components may take longer to. AODB functions comprise operations scheduling and resource allocation backend support for billing to airlines and other clients. Key information is compiled and maintained in the AODB to enable accurate client invoicing[3]. This research is based on the hypothesis that safety analysis of critical systems in a directed SoS must be based on understanding the effect of interdependency between constituent systems.

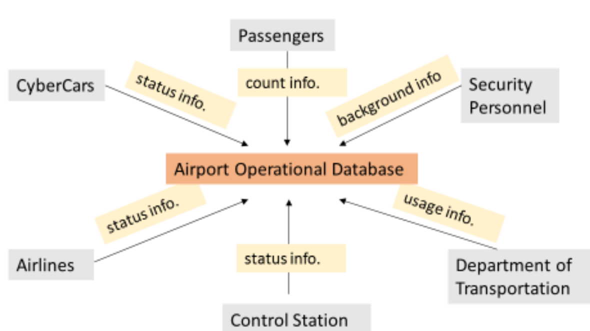


Figure 1 AODB Information Flow

According to Atkins' report on addressing security threats on ITS[4], database management systems are vulnerable to unauthorized access leading to financial theft, massive data deletion and sensitive data breaches. The malicious intent of a hacker can compromise vehicle security and security of integrated systems in the architecture that handle sensitive information. It is possible to conduct a safety analysis of a single breach in an ITS component but when we consider a SoS, the breach can affect any number of components, and thus this becomes more significant. A report on cybersecurity and resilience [5] considers two challenges for analyzing ITS components most prone to failure in a cyberattack:

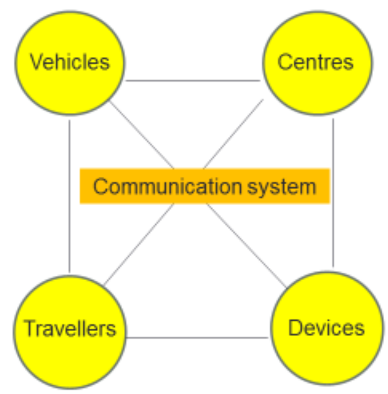


Figure 2 Interconnectivity between CyberCar ITS System of Systems[3]

Challenges are identified based on shortcomings of the status quo that were collected during the survey and the interviews with stakeholders[5]. The first challenge is difficulty integrating security due to a lack of understanding the concept of cybersecurity among Department of Transportation policy makers who require necessary measures to analyze the most critical system. The second challenge is inadequate spending on cybersecurity which is interwoven in the former challenge. This paper aims to provide a yardstick for making prominent investment decisions for improving resiliency of the most critical systems in an ITS since any hazard within a system of systems is not attributable to only one system. The research question lead to an extensive review of literature on ITS networks to understand what systems prominent investing stakeholders (e.g., FAA, USDOT) should allocate a majority of resources, before implementing ITS in future airports – should it be on infrastructure, or

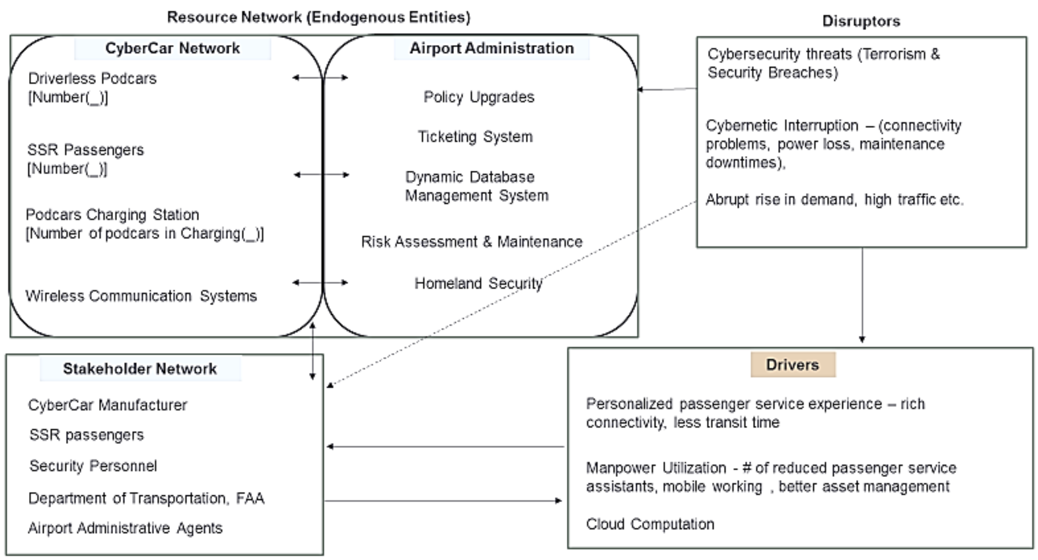


Figure 3 ITS Paper Model with Driverless Podcars – CyberCars

vehicle technology, or should it be used to improve the back-end data base management systems? This research endeavor applies Systems Operational Dependency Analysis (SODA) to answer these research questions.

2.3 Paper Model

The paper model in Figure 3 aims to depict the information flow between the stakeholders and resources, and lists the disruptors and drivers for a driverless podcar ITS. The Airport Administration is interested in the number of SSRP being moved by CyberCars at any given time. The Airport Administration also has an interest in ancillary services such as maintaining full functionality of communication and electrical power systems. The ticketing system integrated into the AODB, provides information about the passengers and is used by security personnel during screening. Due to insufficient published data on applying driverless podcars in an airport, Figure 3 represents a simplified conceptual model.

3. METHODOLOGY

The modeling approach adopted by the research team to test the hypothesis and the research question listed above is SODA. The challenge of analyzing and architecting SoS is tough due to the complexity and size of the SoS, and because of the evident dependencies between the different component systems which affect the behavior of the whole structure and network. The underlined dependencies of the functionality on linkages between the different components of the SoS, can feature emergent behavior that SODA can predict when an SoS is investigated[6].

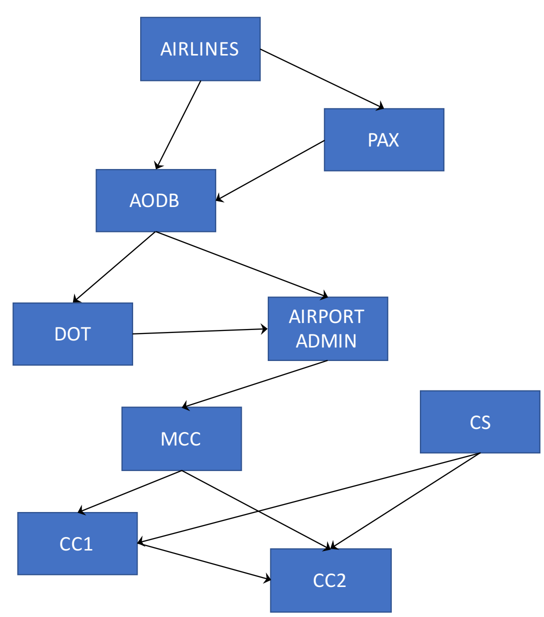


Figure 4 SoS ITS conceptual directed network

The goal of this modeling technique is to assess the impact of dependencies in the CyberCar ITS SoS and investigate where prominent investigating stakeholders can emphasize and focus limited resources, while analyzing the architecture of the SoS when a hazard occurs within it. Considering the implementations of ITS, the research team evaluated the most critical system from a functional point-of-view assuming infrastructure capabilities are ready, reliable and robust.

The SODA approach has been selected since it gives high-level information about the architecture of the system at an early stage and can identify the criticalities of the CyberCar ITS SoS, while exploiting the dependencies between components; thereby identifying emergent behavior. Furthermore, SODA provides a conceptual framework for "designing problem solving interventions and it is a decision support tool for complex systems using cognitive mapping aiding the strategic management in terms of changing "thinking and action", rather than planning".

The SoS architecture is modeled as a directed network, where the nodes represent the component systems of the CyberCar ITS. The links represent the dependencies between the components and are characterized by strength and criticality which affect the behavior of the SoS network differently. Specifically, the Strength of Dependency (SOD) represents how much the behavior of a component is dependent on the behavior of the predecessor component. Additionally, the Criticality of Dependency (COD) represents component functionality degradation when a hazard occurs in the predecessor component. The conceptual ITS SoS directed network designed by the research team is shown in the Figure 4.

For each link of the conceptual directed network two values are needed. The SOD, or α, values which must be between 0 and 1 and the COD, or β, values which must be between 0 and 100 where a lower value corresponds to a higher criticality of dependency. The research team contacted the customer representatives of the Kansas City Airport, however, but were unable to capture meaningful data. The team applied expert advice to determine the SOD and COD values which will be used for this conceptual framework approach to evaluate the critical system of the directed ITS SoS network. Table 3 and

Table 4 provide the selected values for each link of the network.

Table 3 SOD (α)Values for Each Link

	A	P	DB	D	AA	CS	MCC	CC1	CC2
A	0	0.80	0.60	0	0	0	0	0	0
P	0	0	0.80	0	0	0	0	0	0
DB	0	0	0	0.20	0.80	0	0	0	0
D	0	0	0	0	0.40	0	0	0	0
AA	0	0	0	0	0	0	0.75	0	0
CS	0	0	0	0	0	0	0	0.75	0.75
MCC	0	0	0	0	0	0	0	0.75	0.75
CC1	0	0	0	0	0	0	0	0	0.30
CC2	0	0	0	0	0	0	0	0	0

Table 4 COD (β) Values for Each Link

	A	P	DB	D	AA	CS	MCC	CC1	CC2
A	0	75	50	0	0	0	0	0	0
P	0	0	20	0	0	0	0	0	0
DB	0	0	0	10	90	0	0	0	0
D	0	0	0	0	10	0	0	0	0
AA	0	0	0	0	0	0	80	0	0
CS	0	0	0	0	0	0	0	90	90
MCC	0	0	0	0	0	0	0	60	60
CC1	0	0	0	0	0	0	0	0	10
CC2	0	0	0	0	0	0	0	0	0

For future research activities, a qualitative approach is recommended for selecting SOD and COD values. For example, identifying High, Medium or Low dependencies and relating these to appropriate ranges in the SOD and COD ranges of 0 to 1 and 100 to 0, respectively.

3.1 Deterministic Analysis

First, a deterministic analysis was adopted by the research team using a self-effectiveness (SE) of 20 to simulate degraded operability of each system; normal operations SE=100. The resulting operability of the Airport Administration, CyberCar #1 and CyberCar #2 systems were recorded. The results are recorded in Table 5.

To analyze the results of the simulation, CyberCar failure was defined as operability below 90 based on Sanou's method for satellite systems[7]. A yellow "Y" indicates a CyberCar failure and blank indicates no CyberCar failure. The results show the AODB, or DBMS, system is the most critical system for Airport Administration, and CyberCars will fail if the MCC fails. Each CyberCar also fails when their SE is reduced. Therefore, by determinist analysis MCC (Node 7) and AODB (Node 3) are the most critical systems and resources should be focused on ensuring reliable and robust operation of these systems.

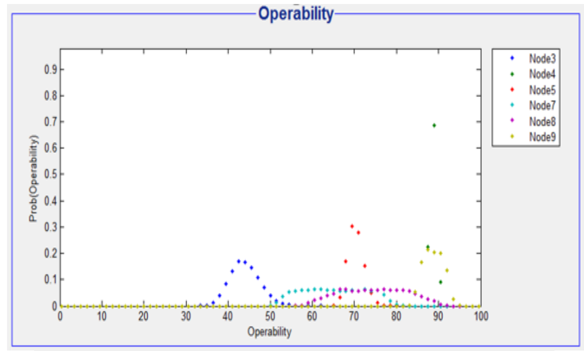
Table 5 Deterministic Results

Nodes	Airport Admin Operability	Cybercar 1	Cybercar 2	Cybercar 1	Cybercar 2
DBMS	70.44	91.65	93.6		
DOT	74	92.8	95.4		
AA	88	96.6	97.4		
A	88.98	96.9	97.6		
P	98.3	98.7	99.5		
MCC	100	70	77	Y	Y
CS	100	92.5	94.25		
CC1	100	80	98	Y	
CC2	100	98	78		Y

3.2 Stochastic Analysis

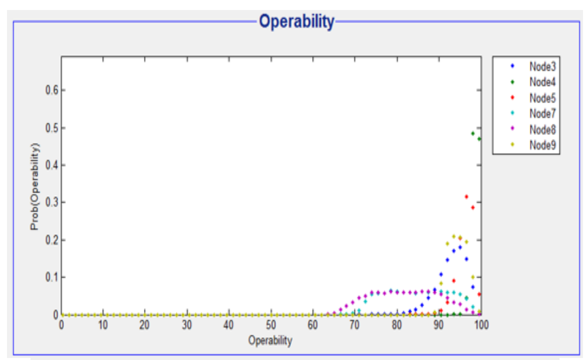
A more realistic behavior of the CyberCar ITS SoS related to the dependencies between components can be achieved using stochastic analysis in the form of probability distributions. The analysis and the calculation of expected value of the operability of a component provides a measure of resilience to failures of its predecessors and the variance can assess the sensitivity of a component. For the deterministic analysis, the assessment of the network was based on the simulation of a single instance, however for the stochastic analysis possible combinations between the values can be accounted for.

A uniform distribution was selected by the research team which means the same level of service will be provided to the airport during the different periods of the day since this distribution will serve as a base case scenario for such an ITS SoS and the dependencies of the various components can be evaluated. The results of this analysis capture behavioral patterns and features of this conceptual framework enhancing its use as a decision tool.



	-	Mean(Operability)	Std(Operability)
Node1	0	100	0
Node2	0	100	0
Node3	0	44.0131	3.4814
Node4	0	88.8026	0.6963
Node5	0	70.3269	1.8451
Node6	0	100	0
Node7	0	65.2177	7.3864
Node8	0	74.4148	7.7231
Node9	0	88.7459	2.2381

Figure 5 Stochastic Results at Lower Performance Levels



	-	Mean(Operability)	Std(Operability)
Node1	0	100	0
Node2	0	100	0
Node3	0	92.9669	3.5139
Node4	0	98.5934	0.7028
Node5	0	96.2725	1.8624
Node6	0	100	0
Node7	0	84.7316	7.3549
Node8	0	81.7643	7.6692
Node9	0	94.3593	2.2242

Figure 6 Stochastic Results at Higher Performance Levels

For the stochastic analysis two pairs of simulations were performed. First, the team analyzed when v4 operates at a lower performance level ($\mu = 20, \sigma = 5$), while the other systems run the case when v4 is at a higher performance level ($\mu = 90, \sigma = 5$). The corresponding beta distribution values are (12.6, 50.4) for lower performance, and (31.5,3.5) for high performance. After each pair of simulations, the probability distribution curve of each node in the network can be drawn according to the simulation results.

Figure 5 and Figure 6 show the shift of the probability distribution curve of Airport Administration, and the corresponding operability values. The figures show that the direct receiver node 3 (AODB) is the most sensitive node to a variety of V5 (Airport Administration) values. The more sensitive nodes are AODB, or DBMS, (from 44.4 to 92.9), followed by DOT (from 70.3.7 to 96.3). Airlines and Passengers are two robust systems showing very small variance due to their independence from Airport Administration and DBMS. The results show that failure in nodes MCC, CS, CyberCar #1 & CyberCar #2 with independent uniform distribution, and with SE of Node AODB following a beta probability distribution, and thus the Airport Administration has high resilience when the mean SE of DBMS (AODB) is higher.

4. VERIFICATION AND VALIDATION

4.1 Model Verification

The team employed inspection as the method of verification to ensure the right thing was built. First, an independent team member inspected the SoS architecture in the Excel file before it was imported to the SODA_GUI tool. Second, the "Map Network" function was used to generate a figure of the network of the model from the tool. The generated figure was compared to the network originally generated by the team.

Tool limitations allowed an eight-node network to be generated, however, Project CyberCar's network consisted of nine nodes. To work around this limitation, the network map generation was performed twice – once with the first node removed and again with the last node removed as indicated with red. The modified network and the generated network maps are shown in Figure 7 and Figure 8, respectively. Inspection of the two figures verifies the right thing was built.

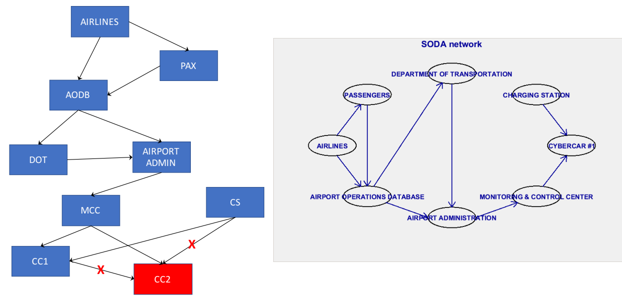


Figure 7 Modified CyberCar Network with CC2 Removed and Resulting Network Map

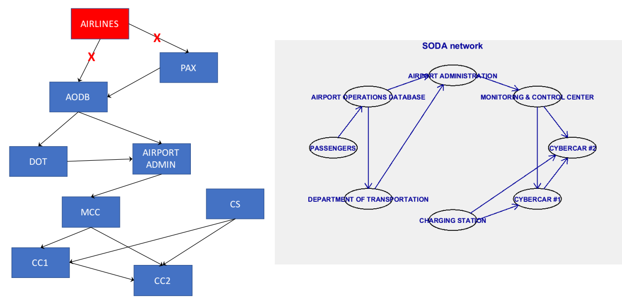


Figure 8 Modified CyberCar Network with Airlines Removed and Resulting Network Map

4.2 Model Validation

First, the model shows that AODB is the most critical system for Airport Administration. The AODB is the primary data source the administration uses to make decisions on CyberCar operations. Second, the model also shows that a reduction in the MCC system will result in a failure to the CyberCar systems. CyberCars depend on the MCC to receive information from the airport administration, therefore, the model accurately captures this relationship. Third, there is no direct information exchange from Airlines, Passengers and DOT; the model correctly shows that failure of these nodes does not affect CyberCars. And lastly, the model shows that (1) a reduction in CyberCar #1 (CC1) self-effectiveness produces a failure in CC1, (2) a reduction in CC2 produces a failure in CC2, and (3) failure of CC1 does not affect a failure of CC2. All three of these scenarios accurately reflect the expected behavior of the CyberCar ITS SoS. A combination of these results validates that we in fact built the right thing.

A couple items to note from the model. First, the DOT node has a higher impact on Airport Administration than expected. And second, CS did not produce a failure of CC1 and CC2 as expected. Further work is required to validate the SOD and COD parameters for these emergent phenomena.

5. SUMMARY AND FUTURE WORK

Summarizing the adopted modeling approach, SODA can provide a decision support tool for complex systems using cognitive mapping. This modeling approach was selected since this conceptual framework of the CyberCar ITS SoS is emerging and limited literature exists that can provide information about other case studies. In other words, this model is the first step of investigating the overall SoS. Thus, based on the results of this analysis stakeholders can achieve a deeper understanding of the directed network and emphasize their efforts on specific subcomponents of the network that are more critical or less resilient than others and conduct analysis in disaggregated level examining each critical component individually.

An alternative modeling approach is to conduct simulation scenarios using agent-based model (ABM). Such approach can analyze the SoS of interest and explore inter-system interactions for emergent behaviors. This can be achieved by conducting sensitivity analysis to the SoS by carrying out different "what-if" scenarios. These different simulation scenarios can be run by varying the initial parameters of the ABM (such as the fleet of the Cybercars in the airport, the arrival rate of special service request passengers, the arrival rate of the airport passengers overall, capacity of Cybercars, etc.). Furthermore, a significant advantage of ABMs is it can capture human factors and human behaviors which can be irrational and tend to make other modeling approaches complex. Specifically, social initial parameters can be a) how people interact with the movement of CyberCars in the airport, b) how someone's decision to ride a CyberCar can affect other decisions either related to the use of CyberCars or not. As was mentioned above, the initial parameters and conditions of a modeling approach related to CyberCars are based on assumptions and since this topic is emerging, the assumptions are based mostly on experts' opinions and less on findings from other studies. This can lead to ABMs that do not fully capture real-life conditions which may impact the results. To address this issue, stated-preference surveys can be designed and distributed in airports to target audiences such as airport passengers, people with restricted mobility and focus groups between airport administrators and other decision and policy makers (representatives of state DOT's, USDOT and FAA). The data of the surveys can be analyzed using advanced statistical or econometric models and therefore the output of these models can be utilized as input of the agent-based models capturing people's opinions and attitudes related to the concept of CyberCars and aiding people with restricted mobility within airports.

The findings of this ABM can aid the administrators of the airport, the decision and the policy makers overall, to understand the implications involved with CyberCars and better understand the benefits that CyberCars can provide to the airport.

REFERENCES

[1] "Intelligent Transportation Systems Benefits, Costs, and Lessons Learned." (2014): US Department of Transportation, June 2014. Web. 22 Apr. 2017. <http://www.itsknowledgeresources.its.dot.gov/its/bcllupdate/pdf/BCLL_2014_Combined_JPO-FINAL.pdf>.

[2] Maier, Mark W. "Architecting Principles for Systems-of-systems." Systems Engineering. John Wiley & Sons, Inc., 09 Feb. 1999. Web. 27 Apr. 2017. <http://onlinelibrary.wiley.com/doi/10.1002/(SICI)1520-6858(1998)1:4%3C267::AID-SYS3%3E3.0.CO;2-D/abstract>.

[3] Elizer, R. Marshall, Robert E. Brydia, and Curtis P. Beaty. "Guidebook for Implementing Intelligent Transportation Systems Elements to Improve Airport Traveler Access Information." (2012): n. pag. Federal Aviation Administration, 2012. Web. 28 Apr. 2017. <https://pdfs.semanticscholar.org/c0c4/d8f61c0ae8a2f0a002427f4ab738577d539c.pdf>.

[4] "Addressing Security Threats in Intelligent Transportation Systems." – Atkins. N.p., 28 Nov. 2016. Web. 24 Apr. 2017. <http://www.atkinsglobal.com/en-gb/angles/all-angles/addressing-security-threats-in-intelligent-transportation-systems>.

[5] Guariniello, Cesare, and Daniel DeLaurentis. "Dependency Analysis of System-of-Systems Operational and Development Networks." Proc. of Conference on Systems Engineering Research, Georgia Institute of Technology, Atlanta, GA. N.p., 19-22 Mar. 2013. Web. 28 Apr. 2017. <http://www.sciencedirect.com/science/article/pii/S187705091300029X>.

[6] Yang, K., Chen, Y., Lu, Y., and Zhao, Q. (2010). The study of guided emergent behavior in systems of systems requirement analysis. 5th International Conference on System of Systems Engineering, 2010.

[7] Sanou, Do Alexis, and René Jr. Landry. "Analysis of GNSS Interference Impact on Society and Evaluation of Spectrum Protection Strategies." Positioning 04 (2013): 169-82. SciRes. Web. 17 Apr. 2017.

APPENDIX

Discriminating Factor	Applicability
Managerial independence of the elements	Component systems connected via common membership in intra-Airport passenger transport structure. The CyberCars are supplied by manufacturers which receive requirements from IATA, committing to standards of Dept. of Transportation while each being run by separate operating units and sometimes different transport services.
Operational independence of the elements	Connected by Airport command and cybernetic transport control network (interconnected wire and wireless comm.), which is integrating in both technical and social sense. Intermediate operational independence in response to unforeseen and uncontrolled events. For instance, the Control Centre automatically suggests re-routing for a set of cars in an 'event' of two-car collision, but requires final consent of Airport administration to perform this operation.
Use of Design Principles	
Stable Intermediate forms	Optimum robustness: a variety of stable forms both in time and space are explicit in the design. Intermediate systems are capable of operating and fulfilling useful purpose of transferring passengers before full deployment of the SoS. The ticketing system and CyberCar control center can manage SSR passenger requests without any additional input from airport administration making the intermediate forms self sustaining.
Policy Triage	The oversight bodies of Airport administration and policy makers exercise very limited control and carefully restrict their control to the networks.
Leveraging at the Interface	Multiservice systems (i.e., interactive kiosks at the parking lots, parking ticket system, regular internet ticket booking system concentrate on information transfer.
Ensuring Collaboration	Mostly achieved through socio-technical methods of command and control.
Classification	
Directed with a Purpose	The system is developed and operated to a common purpose: providing personalized customer experience, easier mobility to large number of passengers with SSR requests in a short period.

ABBREVIATIONS

A	Airlines
AA	Airport Administration
ABM	Agent-based model
AODB	Airport Operational Database
CC	CyberCar
COD	Criticality of Dependency
CS	Charging station
D	Department of Transportation
DB	Database
DBMS	Database Management System
DOT	Department of Transportation
FAA	Federal Aviation Administration
ITS	Intelligent Transportation System
MCC	Monitoring & Control Center
P	Passengers
PAX	Passengers
PRT	Personal rapid transport
ROPE	Resources, Operation, Policy, and Economics
SE	Self-effectiveness
SOD	Strength of Dependency
SODA	Systems operational dependency analysis
SoS	System of Systems
SSR	Special services request
SSRP	Special services request passenger
USDOT	U.S. Department of Transportation
WVU	West Virginia University