

# Critical Infrastructures: The Nervous System of every Welfare State



**G. Stergiopoulos, D. Gritzalis**

# Αλληλεξαρτήσεις Κρίσιμων Υποδομών: Το Νευρικό Σύστημα κάθε Τεχνολογικά Προηγμένης Χώρας



Αθήνα, Φεβρουάριος 2017



**ΟΠΑ**  
**ΑΥΕΒ**

**Δρ. Γιώργος Στεργιόπουλος**  
**Καθηγητής Δημήτρης Γκριτζαλης**

Εργαστήριο Ασφάλειας Πληροφοριών & Προστασίας Υποδομών  
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

# Εισαγωγή

## Κρίσιμες Υποδομές

- **Κρίσιμη Υποδομή:** “Το σύνολο των αγαθών, συστημάτων και δικτύων, είτε φυσικών είτε εικονικών, τα οποία είναι απαραίτητα για μια χώρα».
- Ραχοκοκαλιά της **οικονομίας**, της **ασφάλειας** και του **βιοτικού επιπέδου** ενός έθνους παρέχοντας νερό και ρεύμα στα σπίτια και υποστηρίζοντας τα συστήματα μεταφοράς και επικοινωνίας όπου στηρίζεται η Κοινωνία<sup>1</sup>.
- **Μη-διαθεσιμότητα ή καταστροφή** έχει πολλαπλές **επιπτώσεις** στην εθνική ασφάλεια, οικονομία, δημόσια υγεία ή σε συνδυασμό τους<sup>1</sup>.



<sup>1</sup> Department of Homeland Security (DHS), What Is Critical Infrastructure?. Retrieved January 15, 2017 from: <http://www.dhs.gov/what-critical-infrastructure>.

# Εισαγωγή - Κρίσιμες Υποδομές



Synopsis of NISAC Modeling Capabilities (<http://www.sandia.gov/nisac/capabilities/>)



# Αντιμετώπιση Απειλών Κρίσιμων Υποδομών

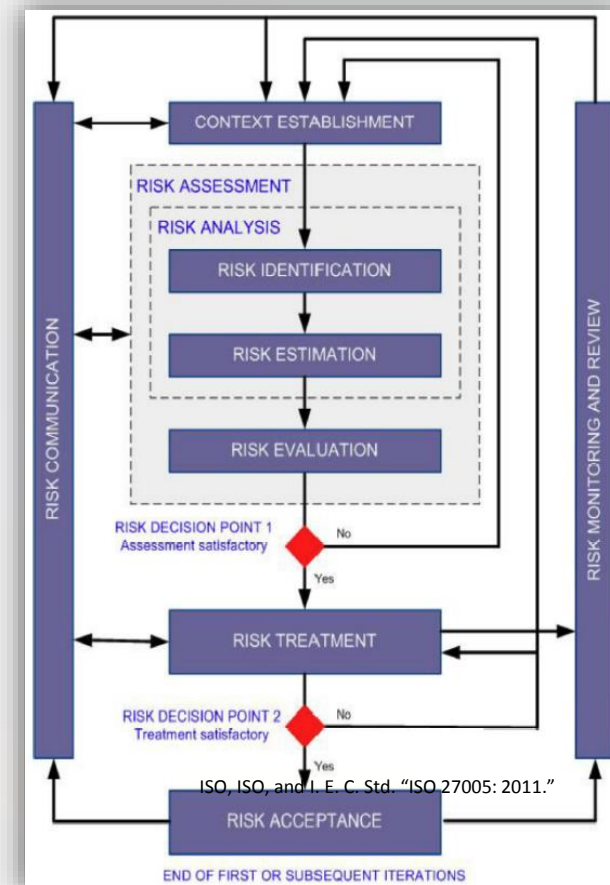
- Πολυπλοκότητα και ποικιλομορφία κινδύνων και απειλών που αντιμετωπίζουν οι Κρίσιμες Υποδομές (ΚΥ)
  - Απαιτείται συστηματική και ολοκληρωμένη προσέγγιση στους στόχους ασφάλειας.
- Μέχρι στιγμής, η έρευνα έχει επικεντρωθεί στην διασφάλιση των Κρίσιμων Υποδομών και των επιχειρήσεων μέσω διαδικασιών αξιολόγησης της επικινδυνότητας και των απειλών βασισμένες σε:
  - Διεθνή πρότυπα ISO (π.χ. ISO 27001)
  - Ελέγχους ασφάλειας
  - Δοκιμές διείσδυσης στα πληροφοριακά συστήματα Κρίσιμων Υποδομών



# Μεθοδολογίες Διαχείρισης Επικινδυνότητας

✓ Μεθοδολογίες διαχείρισης της επικινδυνότητας: Αναγνώριση, ανάλυση, αποτίμηση και διαχείριση του επιπέδου επικινδυνότητας πληροφοριακών συστημάτων

- Context Establishment: **Αναγνώριση** και ορισμός των **κριτηρίων** για την διαχείριση της επικινδυνότητας, ορισμός του **σκοπού** και των **ορίων** της μελέτης, κ.λπ.
- Risk Identification: Προσδιορισμός του **τι θα μπορούσε να προκαλέσει μια πιθανή απώλεια**, και να αποκτηθεί μια εικόνα για το πώς, πού και γιατί η απώλεια μπορεί να συμβεί.
- Risk Estimation: Υπολογισμός της **πιθανότητας εμφάνισης μιας απειλής**, της **επίπτωσης** και άλλων παραμέτρων που σχετίζονται με τους προσδιορισμένους κινδύνους.
- Risk Evaluation: **Κίνδυνοι κατατάσσονται κατά προτεραιότητα**, παρέχοντας βάση για επιλογή κατάλληλων **αντιμέτρων**.



# Μεθοδολογίες Αποτίμησης Επικινδυνότητας (1/2)

- Έχουν αναπτυχθεί πολλές μεθοδολογίες αποτίμησης επικινδυνότητας, με διαφορετική προσέγγιση, δίνοντας έμφαση σε:
  - Αγαθά, πχ. MAGERIT, OCTAVE, CRAMM
  - Επιχειρησιακές διαδικασίες, πχ. COBIT 5
  - Επικινδυνότητα που προέρχεται από αλληλο-εξαρτήσεις μεταξύ ΚΥ και τις πιθανές επιπτώσεις τους<sup>2</sup>
- Είναι προσανατολισμένες στην παροχή μελετών αξιολόγησης και περιγραφής αντιμέτρων σε συγκεκριμένα μέρη ενός πληροφοριακού συστήματος (πχ. αγαθών, επιχειρησιακών διαδικασιών).

<sup>2</sup> P. Kotzanikolaou, M. Theoharidou and D. Gritzalis, Interdependencies between critical infrastructures: Analyzing the risk of cascading effects, in Critical Information Infrastructure Security, S. Bologna, B. Hammerli, D. Gritzalis and S. Wolthusen (Eds.), Springer-Verlag, Berlin, Heidelberg, Germany, pp. 104–115, 2013.ermany, pp. 171–182, 2013.

## Μεθοδολογίες Αποτίμησης Επικινδυνότητας (2/2)

- Χρήσιμες για στοχευμένες αναλύσεις σεναρίων.
- Ωστόσο, υπολείπονται όταν απαιτούνται υψηλού επιπέδου αναλύσεις προκειμένου να:
  - αναλυθούν **σενάρια εξαρτήσεων** μεταξύ **αγαθών** ή και **ολόκληρων υποδομών** από τις επιχειρησιακές διαδικασίες στις οποίες εμπλέκονται.
  - παρασχεθεί μια πιο **ολοκληρωμένη** και **λεπτομερής** εκτίμηση της επικινδυνότητας απειλών και περιστατικών ασφάλειας στην μοντελοποίηση επιχειρησιακών διαδικασιών.



# Μεθοδολογία ανάλυσης πολλαπλών αλληλεξαρτήσεων

**Αλληλεξάρτηση υποδομής:** “Μονόδρομη εξάρτηση ενός περιουσιακού στοιχείου, συστήματος, δικτύου ή συλλογή αυτών - εντός ενός ή πολλαπλών τομέων – από την είσοδο δεδομένων, πληροφοριών, υπηρεσιών και γενικά την αλληλεπίδραση ή άλλη απαίτηση από υπηρεσίες άλλης υποδομής ή στοιχείου αυτής, προκειμένου να λειτουργήσει σωστά”

**Μοντελοποίηση** σαν γράφοι:

- Κόμβοι απεικονίζουν υποδομές ή συστατικά αυτών
- Ακμές απεικονίζουν εξαρτήσεις των υποδομών

**Εκτιμήσεις** ποσοτικοποιούν τις Επιπτώσεις και την Πιθανότητα εμφάνισης αστοχιών

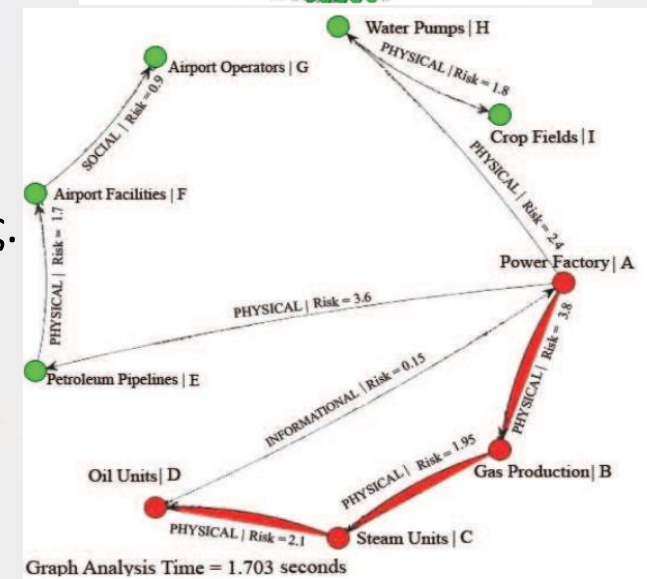
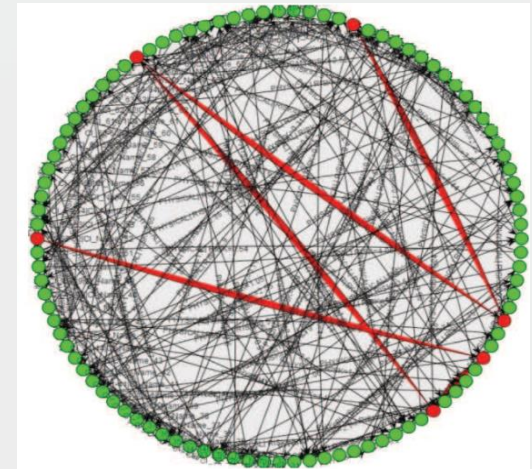
- Μετρικές Επιπτώσεων και Πιθανοτήτων εμφάνισης Απειλών περιγράφουν τις ακμές που συνδέουν Κρίσιμες Υποδομές



# Μεθοδολογία ανάλυσης πολλαπλών αλληλεξαρτήσεων

## Ανάπτυξη εργαλείων υπολογισμού Επικινδυνότητας Αλληλεξαρτήσεων (CIDA & SMEDA)

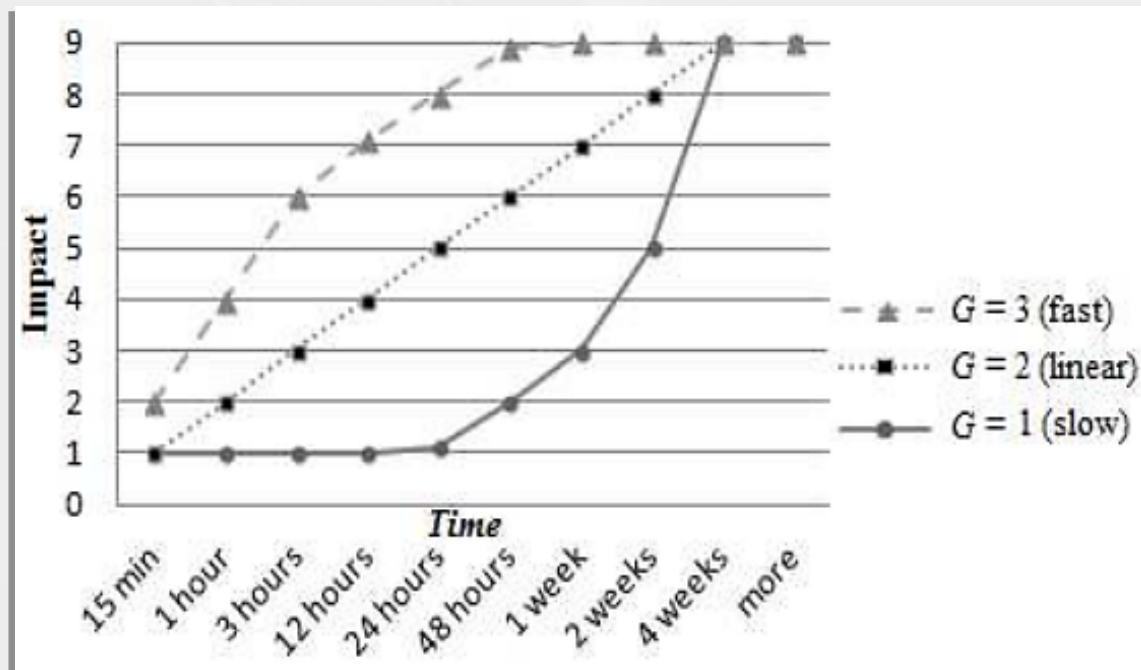
- Neo4J technology
- Java
- Δέχεται ως είσοδο αποτελέσματα Ανάλυσης Επικινδυνότητας
- Υποστηρίζει 17 τομείς Κρίσιμων Υποδομών μεταξύ των οποίων και την Ενέργεια, Μεταφορές και Τηλεπικοινωνίες.
- Υπολογίζει την Επικινδυνότητα μονοπατιών από αλληλεξαρτώμενες ΚΥ ή/και τομείς αυτών.



# Ενεργή έρευνα: Χρονική ανάλυση της Επικινδυνότητας αλληλεξαρτήσεων μεταξύ υποδομών και τομέων

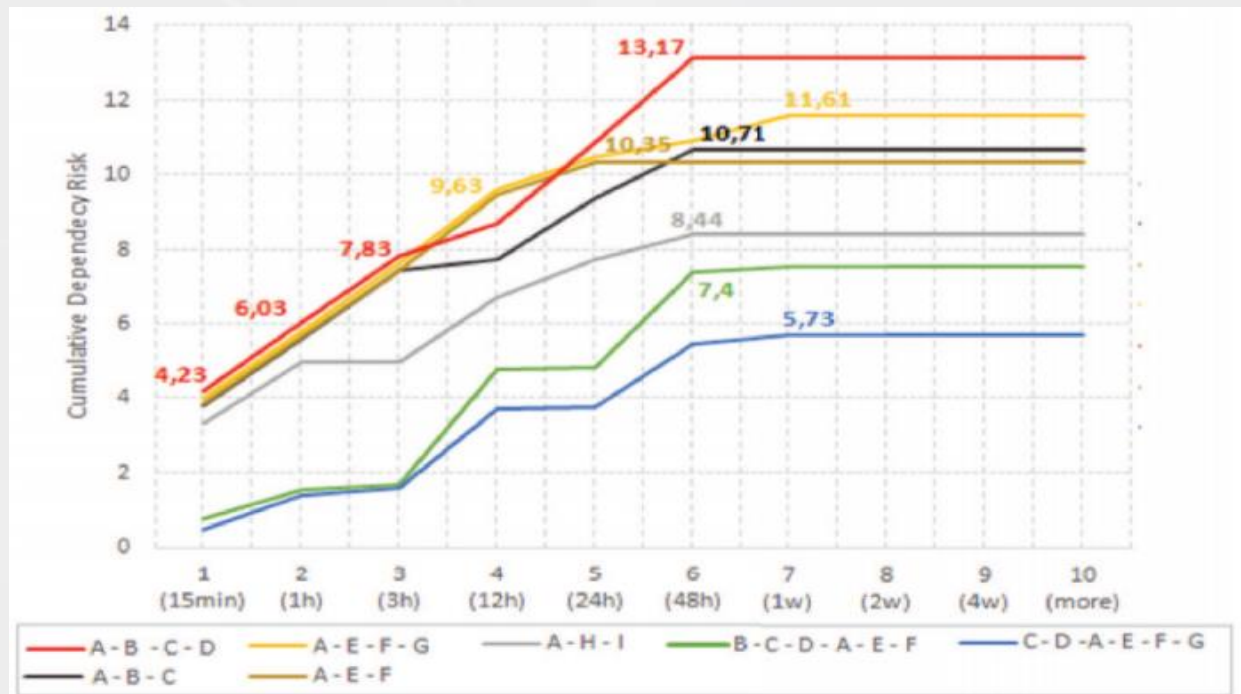
- Δίνει εκτίμηση της **εξέλιξης των επιπτώσεων** από τις αποτυχίες
  - Επιπτώσεις χειρότερου σεναρίου και ρυθμό ανάπτυξης αυτών από την αξιολόγηση των κινδύνων

**Υποστηρίζει αργή, γραμμική ή ταχεία εξέλιξη των επιπτώσεων μετά την υλοποίηση μιας απειλής**



# Ενεργή έρευνα: Χρονική ανάλυση της Επικινδυνότητας αλληλεξαρτήσεων μεταξύ υποδομών και τομέων

- **Ανιχνεύει** επικίνδυνα μονοπάτια αλληλεξαρτήσεων για κάθε χρονική στιγμή:
- Βοηθά ελέγχους ασφαλείας - Πού να επικεντρωθεί κάθε ενέργεια:
  - Πχ. 48 ώρες μετά την αρχική αστοχία πρέπει να προσπαθήσουμε να επαναφέρουμε τα components στις Κρίσιμες Υποδομές A-B-Γ
  - Πχ. 12 ώρες μετά την αρχική αστοχία πρέπει να προσπαθήσουμε τα components Κρίσιμες Υποδομές A-E-P-G



# Ενεργή έρευνα: Θεωρία γράφων για ανάλυση αλληλεξαρτήσεων μεταξύ υποδομών και τομέων

Χρήση **Θεωρίας γράφων** για εντοπισμό και περιγραφή των κρίσιμων κόμβων.

- Εντοπίζει συσχετίσεις μεταξύ μετρικών με υψηλές τιμές και αντίστοιχων κόμβων

**Διεξήγαμε tests** σε 32,950 μοντέλα για εντοπισμό κατάλληλων μετρικών γράφων:

- 700 γράφοι με 774,015,270 μονοπάτια αλληλεξαρτήσεων

INFORMATION GAIN	Inbound Test	Outbound Test
Betweenness	0.259	0.277
Eccentricity	0.238	0.285
Closeness	<b>0.387</b>	<b>0.345</b>
Eigenvector	0.151	0.260
Intersection of all Centralities	0.176	0.248
Inbound degree (sinkholes)	-	<b>0.302</b>
Outbound degree	<b>0.281</b>	-

Table 1: Weka's output ranking using the Information Gain algorithm

GAIN RATIO	Inbound Test	Outbound Test
Betweenness	0.08	0.101
Eccentricity	0.08	0.101
Closeness	<b>0.14</b>	<b>0.120</b>
Eigenvector	0.06	0.09
Intersection of all Centralities	<b>0.458</b>	<b>0.550</b>
Inbound degree (sinkholes)	-	0.103
Outbound degree	0.101	-

Table 2: Weka's output ranking using the Gain Ratio algorithm



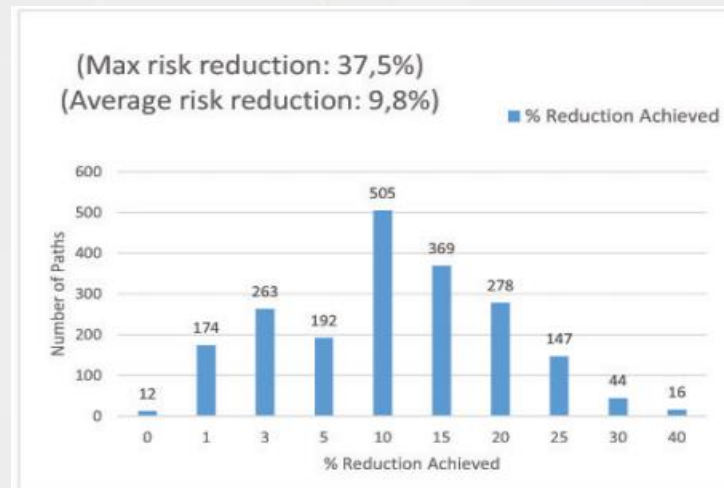
# Ενεργή έρευνα: Θεωρία γράφων για ανάλυση αλληλεξαρτήσεων μεταξύ υποδομών και τομέων

**Προτεινόμενος αλγόριθμος** ως μια στρατηγική περιορισμού του κινδύνου που επιλέγει τους πιο επικίνδυνους κόμβους (ΚΥ) για την άμβλυνση του κινδύνου

- **Αξιολογήθηκε σε** σε 2000 ειδικά μοντέλα/πειράματα

<i>Risk Metrics</i>	<i>Strategies</i>	Information Gain	Top Initiators	Top Sinkholes
Most critical path		43.7% (max)	38.4% (max)	34.5% (max)
		12.1% (avg)	11.8% (avg)	10.3% (avg)
Top 20 critical paths		37.5% (max)	28.7% (max)	29.8% (max)
		9.8% (avg)	10.0% (avg)	7.3% (avg)
Entire graph		12.2% (max)	10.1% (max)	10.8% (max)
		7.5% (avg)	5.3% (avg)	6.7% (avg)

Table 3: Comparison of results from all mitigation strategies





# Επόμενα βήματα

- Τα εθνικά δίκτυα υποδομών μπορούν να μελετηθούν με εργαλεία όπως το CIDA και το SMEDA και τους μηχανισμούς περιορισμού της Επικινδυνότητας που παρουσιάστηκαν.
- Αναγκαία η συνεισφορά από Αναλυτές Ασφάλειας Πληροφοριακών Συστημάτων για την αξιολόγηση των κινδύνων.
  - Οι μεθοδολογίες που παρουσιάστηκαν θα μπορούσαν να διευκολύνουν την περαιτέρω ανάλυση των κρίσιμων εξαρτήσεων των εθνικών υποδομών και όχι μόνο.
- Ευκαιρίες για πρακτική ανάλυση αποτελεσμάτων και ευρημάτων (**το Internet of Things (IoT) είναι εδώ...**)
- Οι κυβερνήσεις θα μπορούσαν να επωφεληθούν από τη μαζική, αυτοματοποιημένη ανάλυση εξάρτησης που προσφέρεται από τα εργαλεία για πρόβλεψη εθνικής εμβέλειας καταστροφών.



# Τι είναι αυτό το ...«Πράγμα»;

## Information Technology

- PCs
- Servers
- Virtualization
- Routers
- Switches

## Personal Technology

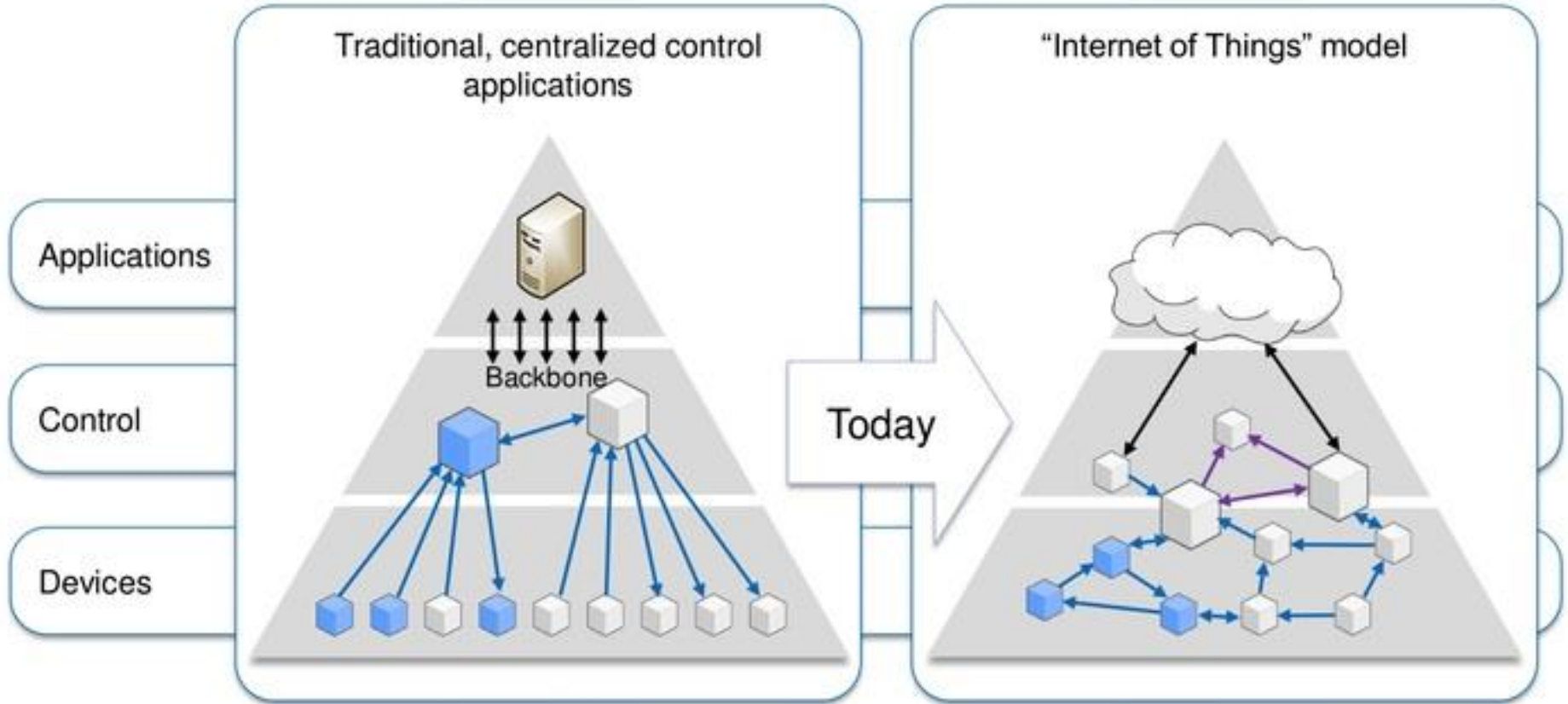
- Tablets
- Smart phones
- Smart watches
- Home energy
- Home entertainment
- Home control
- Medical implants
- Medical wearables

## Operational Technology

- Industrial Control Systems(ICS)
- Supervisory control and data acquisition
- Medical machines
- Kiosks
- Manufacturing
- Cloud service infrastructure
- Environmental Monitoring



# Internet of Things (IoT)



# Συμπεράσματα

- ✓ Σημαντικές ερευνητικές ευκαιρίες έρευνας υπάρχουν στον τομέα των κρίσιμων υποδομών και στις αλληλεξαρτήσεις αυτών, τόσο για την εκτίμηση του κινδύνου όσο και της ανίχνευσης βλάβης.
- ✓ Οι πρωτοβουλίες του Εργαστηρίου INFOSEC του ΟΠΑ αλληλοσυμπληρώνονται.
- ✓ Κάθε ερευνητικό project στοχεύει στην επίλυση διαφορετικών (αλλά συμπληρωματικών) προβλημάτων:
  - ✓ Ανάγκη για **χρονική ανάλυση** των επιπτώσεων κάθε αστοχίας
  - ✓ Ανάγκη για εντοπισμό των επικίνδυνων ΚΥ **που επηρεάζουν έντονα** άλλες ΚΥ ή συνδυασμό αυτών.
- ✓ Η κατάσταση περιπλέκεται όσο αναπτύσσονται οι τεχνολογίες των ΚΥ παρά βελτιώνεται (αλληλεξαρτήσεις, SCADA+IP, IoT κλπ.)



## References

1. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the risk of cascading effects", in *Proc. of the 6<sup>th</sup> International Workshop on Critical Infrastructure Security*, pp. 107-118, Springer (LNCS 6983), Switzerland, 2011.
2. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk assessment of multi-order interdependencies between critical information and communication infrastructures", *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 151-170, IGI Global, 2013.
3. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Accessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7<sup>th</sup> IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, March 2013.
5. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., *CIDA: Critical Infrastructure Dependency Analysis Tool*, <https://github.com/geostergiop/CIDA>, September 2014.
6. Stergiopoulos G., Theoharidou M., Kotzanikolaou P., Gritzalis D., "Using centrality measures in dependency risk graphs for efficient risk mitigation", in *Critical Infrastructure Protection IX*, pp. 25-40, Springer, 2015.
7. Stergiopoulos G., Kotzanikolaou P., Theoharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", *International Journal of Critical Infrastructure Protection*, September 2015.
8. Stergiopoulos G., Theoharidou M., Gritzalis D., "Using logical error detection in remote-terminal units to predict initiating events of Critical Infrastructures failures", in *Proc. of the 3<sup>rd</sup> International Conference on Human Aspects of Information Security, Privacy and Trust*, Springer (LNCS 9190), USA, August 2015.
9. Theoharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7<sup>th</sup> IEEE International Conference in Global Security, Safety and Sustainability*, pp. 171-178, Springer (LNICST 99), Greece, 2012.
10. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3<sup>rd</sup> IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.
11. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.