A. Appendix

In this appendix we present on section A.1 complementary tables mentioned throughout this work. On section A.2 we give a content summary of each article reviewed in this survey with a description of its classification within the taxonomy. Finally on section A.3 we present a thorough summary of the contents of this survey using tables. On section A.3 we have summarized the article references contained within each aspect, the *Studies performed* classifications that were not mentioned on section 3, and summary tables that succinctly show the classifications to which each article belongs to.

A.1 *Complementary tables*

Table A.1. Queries performed on each library. Updated: October 15th 2019

Library	Query
APS	(percolation ”multilayer networks” AND percolation ”interdependent networks” AND percolation ”multi-layer networks” AND percolation ”multilayer network” AND percolation ”interdependent network” AND percolation ”multi-layer network” AND percolation ”network of networks” AND percolation ”cascading failure” AND percolation ”cascading failures” AND robustness ”multilayer networks” AND robustness ”interdependent networks” AND robustness ”multi-layer networks” AND robustness ”multilayer network” AND robustness ”interdependent network” AND robustness ”multi-layer network” AND robustness ”network of networks” AND robustness ”cascading failure” AND robustness ”cascading failures” AND resilience ”multilayer networks” AND resilience ”interdependent networks” AND resilience ”multi-layer networks” AND resilience ”multilayer network” AND resilience ”interdependent network” AND resilience ”multi-layer network” AND resilience ”network of networks” AND resilience ”cascading failure” AND resilience ”cascading failures”)
Elsevier	(”network of networks” OR ”cascading failure” OR ”interdependent network” OR ”multilayer network” OR ”multi-layer network”) AND (percolation OR robustness OR resilience) AND NOT (neural)
PLOS ONE	(percolation OR robustness OR resilience) AND (”multilayer networks” OR ”interdependent networks” OR ”multi-layer networks” OR ”multilayer network” OR ”interdependent network” OR ”multi-layer network” OR ”network of networks” OR ”cascading failure” OR ”cascading failures”) NOT neural
Nature	(percolation OR robustness OR resilience) AND (”multilayer networks” OR ”interdependent networks” OR ”multi-layer networks” OR ”multilayer network” OR ”interdependent network” OR ”multi-layer network” OR ”network of networks” OR ”cascading failure” OR ”cascading failures”)
ACM	(percolation OR robustness OR resilience) AND (”multilayer networks” OR ”interdependent networks” OR ”multi-layer networks” OR ”multilayer network” OR ”interdependent network” OR ”multi-layer network” OR ”network of networks” OR ”cascading failure” OR ”cascading failures”)
IEEE	((”Abstract”:”interdependent network” OR ”Abstract”:”interdependent networks” OR ”Abstract”:”multilayer network” OR ”Abstract”:”multilayer networks” OR ”Abstract”:”multi-layer network” OR ”Abstract”:”multi-layer networks” OR ”Abstract”:”network of networks” OR ”Abstract”:”cascading failure”) AND (”Abstract”:percolation OR ”Abstract”:resilience OR ”Abstract”:robustness) AND NOT ”Abstract”:neural) OR ((”Document Title”:”interdependent network” OR ”Document Title”:”interdependent networks” OR ”Document Title”:”multilayer network” OR ”Document Title”:”multilayer networks” OR ”Document Title”:”multi-layer network” OR ”Document Title”:”multi-layer networks” OR ”Document Title”:”network of networks” OR ”Abstract”:”cascading failure”) AND (”Document Title”:percolation OR ”Document Title”:resilience OR ”Document Title”:robustness) AND NOT ”Document Title”:neural)

A.2 *Articles summary*

In this section we present a summary of each paper reviewed in this survey. The articles are presented in chronological order by year of publication. The summaries show the main aspects of each paper using the taxonomy presented on this survey, as well as the main results and objectives. The number assigned in this section is later used to represent citations in a more compact way.

1. **Catastrophic cascade of failures in interdependent networks** - 2010 - Sergey V. Buldyrev, Roni Parshani, Gerald Paul, H. Eugene Stanley, Shlomo Havlin [5]

   This article's objective is to develop a framework for understanding the robustness of interacting networks against cascading failures. The framework developed in this article presents the classic one to one model ("one to one like"), with two networks fully interconnected through bidirectional dependencies. It uses a "breaking-point" metric (percolation threshold), and a probability metric (probability that a giant mutually connected component exists) to measure robustness. Here, "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that one to one interdependent networks are more vulnerable to node failures than single networks.

2. **Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition** - 2010 - Roni Parshani, Sergey V. Buldyrev, Shlomo Havlin [61]

   This article studies an interdependent system composed of two networks. It uses a "directed support-dependency" model where a fraction of the nodes of each network depends on nodes in the other network. The article measures the robustness using "percolation" and "counting elements" metrics (percolation threshold, and size of the largest connected component respectively). Here, "coupling", "size of the giant connected component", and "percoltion" studies were performed. As for the framework testing, the article uses "simulated" networks only. This work shows that the model studied has a critical amount of node removals, after which the system abruptly collapses, as it goes through a first order percolation phase transition, and that reducing the coupling between networks leads to a change from a first order percolation phase transition to a second order percolation phase transition.

3. **How to glue a robust smart-grid?: a finite-network theory for interdependent network robustness** - 2011 - Gyan Ranjan, Zhi-Li Zhang [67]

   In this article, Ranjan et al. present a theoretical framework to model and study the structural properties of smart-grids as interdependent networks. In this work, they conclude that for high coupling rates the most robust network is obtained by coupling the least central nodes, while for low coupling rates the most robust network is obtained by coupling the most central nodes. They use a compressed version of the one to one model ("one to one like"), where coupled nodes are represented as single nodes in the compressed structure. The robustness is measured using the Kirchoff index, a "breaking point" metric that relates the amount of edges that must be removed to break the system in 2 sub-systems. Here, "coupling" and "Laplacian" studies are performed. As for the framework testing "real and simulated" networks were used. This work shows that coupling networks in a way that nodes are geographically dispersed produce a more robust interdependent system.

4. **Robustness of interdependent networks under targeted attack** - 2011 - Xuqing Huang, Jianxi Gao, Sergey V. Buldyrev, Shlomo Havlin, H. Eugene Stanley [32]

   This article presents a general technique to study the effect of degree based targeted attacks over the systems robustness. The framework used in this article uses the classic one to one model ("one to one like"). As metrics it uses a "breaking-point" metric (percolation threshold) and a "counting elements" metric (relative size of the largest connected component). Here, "percolation" and "targeted attacks" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that coupled Scale-Free networks are much more vulnerable to attacks than single Scale-Free networks. The results also suggest that protection strategies used in single networks may not be useful on coupled networks.

5. **An Overlay Mapping Model for Achieving Enhanced QoS and Resilience Performance** - 2011 - Xian Zhang, Chris Phillips, Xiuzhong Chen [94]

   This article focuses on the issue of mapping an application request upon a substrate network in such a way that this mapping improves quality of service (QoS) and resilience. The framework presented uses a "mapping" model where dependencies are related to the mapping process of an application request over a substrate network. Here, "cost", "time", and "counting elements" metrics are used. These metrics measure the cost of improving resilience, the average delay of the mapped request, and the percentage of links that have a backup path respectively. Here, "cost", "delay", and "optimization" studies are performed. As for the framework testing, the article uses "simulated" networks only. In order to improve QoS and resilience an Integer Linear Program (ILP) is formulated. They find that the ILP model significantly improves QoS performance, compared to heuristics, and also improves the resilience of the system.

6. **Assortativity decreases the robustness of interdependent networks** - 2012 - Di Zhou, H. Eugene Stanley, Gregorio D'Agostino, A. Scala [102]

   In this article Zhou et al. study the effects of topology on failure propagation for a one to one model ("one to one like"). To do this, they used a "counting elements" metric that measures the average size of the largest connected component, a "breaking point" metric (percolation threshold), and a "time" metric that measures the number of iterations that a cascading failure takes until it stops. Here, "assortativity", "size of the giant connected component", "cascading time", and "percolation" studies were performed. As for the framework testing, the article uses "simulated" networks only. As a result the authors find that the robustness of the system decreases with a higher assortativity.

7. **Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes** - 2012 - Jianxi Gao, Sergey V. Buldyrev, Shlomo Havlin, H. Eugene Stanley [23]

   This article presents a general framework to study the dynamics of the cascading failure process at each step caused by an initial failure in a Network of Networks system (NON). To do this, a "one to one like" model consisting of N-networks coupled instead of the usual two, is used. To assess the robustness the framework uses two "counting elements" metrics: the relative size of the largest connected component and the fractional size of the giant component of one network after t cascading failures, and a "breaking point" metric (percolation threshold). Here, "cascading time", "percolation", and "size of the giant connected component" studies are performed. In this work only "simulated" networks are used to test the framework. This article finds that for

systems whose layers are Random Regular networks, the robustness is higher than the robustness of Erdös-Rényi networks.

8. **Cascading failures in interdependent lattice networks: The critical role of the length of dependency links** - 2012 - Wei Li, Amir Bashan, Sergey V. Buldyrev, H. Eugene Stanley, Shlomo Havlin; [44]

   This article studies the cascading failures in a "geometric or spatially embedded" model. This model is comprised of two square lattice networks coupled, *A* and *B*. Each lattice is placed on the same Cartesian plane, where each node in network *A* depends on a node in network *B* randomly chosen within a certain distance *r* from the corresponding node in network *A* and vice versa. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "length", and "percolation" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results found in this work suggest that interdependent systems embedded in a Euclidean space become most vulnerable when the distance between interdependent nodes is in an intermedeiate range.

9. **Reliability Analysis of Interdependent Networks Using Percolation Theory** - 2013 - Qiong Zhang, Daqing Li, Rui Kang, Enrico Zio, Peng Zhang [92]

   In this article the reliability properties and lifetime of interdependent networks whose components have a lifetime, are studied. For this, a "one to one like" model where each component has a lifetime is used. To assess the robustness the framework uses a "breaking point" metric that measures how close the system is to a collapsed state. Here, "lifetime", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. This article finds that the lifetime of interconnected networks is significantly shorter than the lifetime of single networks under the same conditions.

10. **Percolation of interdependent networks with intersimilarity** - 2013 - Yanqing Hu, Dong Zhou, Rui Zhang, Zhangang Han, C. Rozenblat, Shlomo Havlin [31]

    This article maps the cascading process with inter-similarity to a percolation of interdependent networks. To do this, the authors used a "one to one like" model (one to one). In order to measure the robustness this article used a "counting elements" metric (size of the largest connected component), a "breaking point" metric (percolation threshold), and a "time" metric that measures the number of iterations that a cascading failure takes until it stops. Here, "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The authors find that when the two participating networks are not identical, the percolation phase transition is always first order.

11. **Robustness of Interdependent Networks: The case of communication networks and the power grid** - 2013 - Marzieh Parandehgheibi, Eytan Modiano [60]

    In this work, Parandehgheibi et al. study the robustness of interdependent networks, in which the state of one network depends on the state of the other network and vice versa. This article specifically focuses on the interdependency between the power grid and communication networks, and the minimum number of node failures needed to cause total blackout. They find that depending on the nature of the inter-dependencies the solution to the minimum number of node failures needed to cause total blackout may or not be NP-hard. The framework presented uses two "coupled

power grid" models: one with bidirectional dependencies, and one with unidirectional dependencies. To measure the robustness, the framework uses a "breaking point" metric that measures the minimum amount of nodes that must be removed to cause total failure (Minimum Total Failure Removals, MTFR). Here, "optimization" studies are performed. Finally, the authors used "real and simulated" networks to test the framework.

12. **Percolation of a general network of networks** - 2013 - Jianxi Gao, Sergey V. Buldyrev, H. Eugene Stanley, Xiaoming Xu, Shlomo Havlin [24]

    In this article an analytical framework is developed and used to analyze percolation properties of a network composed of interdependent networks. The framework uses a "directed support-dependency" model where the model may have n-layers, and only a fraction of the nodes of each layer bidirectionally depends on a node of some other layer. To measure the robustness of the system the article uses two "counting elements" metrics: one that measures the size of the giant connected component, and other that measures the fractional size of the giant component of one network after t cascading failures, and two "breaking point" metrics: the percolation threshold and coupling point where a single node failure can induce the total collapse of a network. Here, "coupling", and "percolation" studies are performed. For the framework testing only "simulated" networks were used. As a result the authors find that the percolation threshold and the giant component depend solely on the average degree of the ER network and the degree of the RR network, but not on the number of networks.

13. **Robustness of network of networks under targeted attack** - 2013 - Gaogao Dong, Jianxi Gao, Ruijin Du, Lixin Tian, H. Eugene Stanley, Shlomo Havlin [18]

    This article introduces a targeted attack probability function that depends on the node degree, and studies the robustness of two networks of networks configurations: partially interdependent star-like configuration, and fully interdependent tree-like configuration. To do this it uses a "one to one like" model consisting of n partially coupled layers. To measure the robustness, the framework uses two "counting elements" metrics: one that measures the fractional size of the giant component of one network after t cascading failures, and other that measures the fractional size of one of the layers at a stable point after a cascading failure. In addition to those metrics, a "time" metric (number of iterations that a cascading failure takes until it stops), and a "breaking point" metric (percolation threshold) are used. Here,"layer configuration", "cascading time", "coupling","targeted attack", and "percolation" studies are performed. As for the framework testing, the article uses "simulated" networks only. Among the results shown, they find that for tree-like configurations the higher the degree, the higher the probability of failure, and that there is a minimum average degree, below it the system will collapse even if just a single node fails.

14. **The effect of clustering-based and degree-based weighting on robustness in symmetrically coupled heterogeneous interdependent networks** - 2013 - Yuzhuo Qiu [62]

    This article studies the robustness of symmetrically coupled interdependent networks against load failures given a load redistribution based on weighted betweenness centrality. This article compared three weighting schemes: random, clustering-based, and degree-based. To do this, it uses a "multiple dependencies" model with loads or weights within networks. To measure the robustness, the framework uses a "cost" metric that measures the relative cost of improving the network's ability to resist a cascading failure. Here, "optimization", "load and capacity", and "cost" studies were performed. As for the framework testing, the article uses "simulated" networks

only. The results show that non-random weighting schemes are more robust against cascading failure, and that for most weighting parameters the degree-based scheme is more robust than the clustering-based scheme.

15. **Optimal weighting scheme and the role of coupling strength against load failures in degree-based weighted interdependent networks** - 2013 - Yuzhuo Qiu [63]

    This article studies the optimal weighting scheme, and the role of coupling strength and configuration against load failures on interdependent networks. To do this, a "multiple dependencies" model with loads or weights within networks is used. To assess the robustness the framework uses a "cost" metric that measures the relative cost of improving the network's ability to resist a cascading failures. Here, "coupling", "optimization", "load and capacity", and "cost" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that there exists an optimal weighting parameter for the case of one-node removal.

16. **Percolation of partially interdependent scale-free networks** - 2013 - Di Zhou, Jianxi Gao, H. Eugene Stanley, Shlomo Havlin [101]

    In this work, Zhou et al. study the percolation behaviour of two interdependent Scale-Free networks under random failures. To do this a "one to one like" model where each node can be bidirectionally connected to at most one other node is used. To measure the robustness, the framework uses a "counting elements" metric that measures the relative size of the giant connected component in one of the participating networks, a "breaking point" metric that measures the percolation threshold, and a "time" metric that measures number of iterations that a cascading failure takes until it stops. Here, "coupling", "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The authors find that as the coupling strength decreases there are two critical coupling strengths which separate three different behaviours: abrupt collapse, abrupt decrease of the size of the giant connected component, and continuous decrease of the size of the giant connected component.

17. **The extreme vulnerability of interdependent spatially embedded networks** - 2013 - Amir Bashan, Yehiel Berezin, Sergey V. Buldyrev, Shlomo Havlin [3]

    This article studies the stability of spatially embedded networks modeled as lattice networks. To do this a "geometric or spatially embedded" model is used. This model consists of spatially embedded networks where two nodes can be connected through interdependent links if the distance between them meets the requirements. To assess the robustness the framework uses a "counting elements" metric (size of the giant connected component), and a "time" metric (number of iterations that a cascading failure takes until it stops). Here, "coupling", "percolation", "cascading time", and "size of the giant connected component" studies are performed. The framework uses "real and simulated" networks for testing. As results, the authors find that in lattice systems there is no critical dependency, and any small fraction of interdependent nodes leads to abrupt collapse.

18. **Abrupt transition in the structural formation of interconnected networks** - 2013 - Filippo Radicchi, Alex Arenas [65]

    This article addresses the effect of increasing the interconnection between networks over the robustness. To do this a "one to one like" model similar to the original one to one model but with added weights is used. The robustness is measured using two "breaking point" metrics: one

that measures specific values related to the Laplacian matrix and one that measures the algebraic connectivity of the system. Here, studies about the "Laplacian" are performed. As for the framework testing, the article uses "simulated" networks only. As result Radicchi et al. find that as the interconnection increases the system undergoes a sharp transition. In particular they find that depending on the importance of the inter and intra-layer connection two regimes may appear: one where various layers are structurally decoupled, and another where the whole system behaves as a single network.

19. **Interdependent Spatially Embedded Networks: Dynamics at Percolation Threshold** - 2013 - Michael M. Danziger, Amir Bashan, Yehiel Berezin, Shlomo Havlin [14]

    In this article Danziger et al. study the relation between the degree of dependence on interconnected networks and the maximum length of the interdependent links that cause the system to have a second order percolation transition. To do this a "geometric or spatially embedded" model is used. This model consists of spatially embedded networks, where two nodes can be connected through interdependent links if the distance between them meets the requirements. To assess the robustness the framework uses a "breaking point" metric (percolation threshold), and a "time" metric (number of iterations that a cascading failure takes until it stops). Here, "coupling", "length", "percolation", and "cascading time" studies are performed. As for the framework testing, the article uses "simulated" networks only. The authors found that depending on the coupling level, different transition behaviours can be observed.

20. **Detecting Critical Nodes in Interdependent Power Networks for Vulnerability Assessment** - 2013 - Dung T. Nguyen, Yilin Shen, My T. Thai [55]

    This article studies the Interdependent Power Network Disruptor (IPND) optimization problem to identify critical nodes in an interdependent power network. To do this, the authors use a "multiple dependencies" model where in order for a node to remain functional it must be connected to the largest connected component, and at least one of their neighbours in the other networks must remain functional. To assess the robustness the framework uses a "counting elements" metric (size of the giant connected component). Here, "targeted attacks", "optimization", and "size of the giant connected component" studies are performed. The framework uses "real and simulated" networks for testing. The study finds that the IPND problem is NP-hard and can be approximated within the factor of $2-\varepsilon$.

21. **Towards designing robust coupled networks** - 2013 - Christian M. Schneider, Nuri Yazdani, Nuno A. M. Araujo, Shlomo Havlin, Hans J. Herrmann [74]

    In this article Schneider et al. propose a systematic strategy to select the minimum amount of nodes that must become autonomous to guarantee a smooth robustness transition. To do this the original one to one model ("one to one like") is used. To measure the robustness this article used a "counting elements" metric that measures the area below the curve formed by the plot of the amount of functional nodes, versus the amount of nodes removed. Here, "coupling", "percolation", and "size of the giant connected component" studies are performed. The framework uses "real and simulated" networks for testing. Among the results the authors found that the strategy proposed requires five times less autonomous nodes than the random selection approach.

22. **Diversity of multilayer networks and its impact on collaborating epidemics** - 2014 - Yong Min, Jiaren Hu, Weihong Wang, Ying Ge, Jie Chang, Xiaogang Jin [54]

This article develops a top-bottom framework that uses two different distributions to model collaborating epidemics on multilayer networks. To do this a "contagion or influence" model with Susceptible-Exposed-Infected-Recovered (SEIR) states and multiplex behaviour is used. To assess the robustness the framework uses a "probability" metric. This metric measures the probability that a node survives given that it is in an environment that allows viral spreading. Here, "evenness", "difference index", and "transmissibility" studies are performed. As for the framework testing, the article uses "simulated" networks only. This article finds that a network with moderate *difference*, high *evenness*, and slightly uneven coupling can effectively increase the robustness to resist a cascading failure.

23. **Robustness of a network formed of spatially embedded networks** - 2014 - Louis M. Shekhtman, Yehiel Berezin, Michael M. Danziger, Shlomo Havlin [76]

    In this article analytic and numeric results for percolation in a interdependent networks system formed by spatially embedded networks is presented. To do this a "geometric or spatially embedded" model with bidirectional dependencies among networks, and an amount n of network layers is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), two "breaking point" metrics (percolation threshold, and maximum coupling before collapse), and a "time" metric (number of iterations that a cascading failure takes until it stops). Here, "coupling", "length", "percolation", "layer configuration", and "cascading time" studies are performed. As for the framework testing, the article uses "simulated" networks only. This article finds that for tree-like layer configuration the critical coupling length significantly decreases. While on configurations with loops there is a critical coupling among networks above which the entire network collapses after a single node failure.

24. **Simultaneous first-and second-order percolation transitions in interdependent networks** - 2014 - Dong Zhou, Amir Bashan, Reuven Cohen, Yehiel Berezin, Nadav Shnerb, Shlomo Havlin [99]

    In this article Zhou et al. study the cascading behaviours of interdependent networks. To do this the original one to one model ("one to one like") is used. The robustness is measured using two "counting elements" metrics, one that measures the relative size of the largest connected component in one of the networks of the system, and other that measures the amount of lost nodes in one of the networks on each step of the failure. Also a "time" metric (number of iterations that a cascading failure takes until it stops), and a "rate" metric (branching factor) are used. Here, "percolation", "cascading time", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The authors find that simultaneously with the first order percolation transition, a spontaneous second order percolation occurs during the cascading process.

25. **Cascading failures in networks with proximate dependent nodes** - 2014 - Yosef Kornbluth, Steven Lowinger, Gabriel A. Cwilich, Sergey V. Buldyrev [41]

    This article studies the mutual percolation of a system composed of two interdependent random regular networks. To do this the framework uses a "geometric or spatially embedded" model where nodes in different networks can be bidirectionally interdependent if when a node is mapped onto other network then the original position and the mapped position are at less than a fixed amount of hops of distance. To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation

threshold) are used. Here, "length", "percolation", and "efficient paths" studies. As for the framework testing, the article uses "simulated" networks only. The results show a non-trivial relation between the nature of the transition through which the networks disintegrate and the parameters of the system.

26. **Enhancing resilience of interdependent networks by healing** - 2014 - Marcell Stippinger, János Kertész [78]

    This article studies a dynamic extension of the one to one interdependent network model. This extension introduces the probability of *healing* non-functioning nodes. The framework uses a "one to one like" model similar to the original one to one with the difference that here there is a probability that a pair of nodes is recovered or *healed*. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that there is a critical healing point, below this point catastrophic cascades form and the average degree of surviving nodes decreases monotonically.

27. **The effect of interdependence on the percolation of interdependent networks** - 2014 - J. Jiang, W. Li, X. Cai [36]

    This article proposes two stochastic models that generate systems composed of two interdependent Scale-Free (SF) networks or Erdös-Rényi (ER) networks. The authors used a "multiple dependencies" model where in order for a node to remain functional it must be connected to the largest connected component, and at least one of their neighbours in the other networks must remain functional. To measure the robustness the authors use a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that SF networks go through a second-order percolation phase transition and the increased dependence strength decreases the robustness of the system, whereas, interdependent ER networks show the opposite results.

28. **Cavity-based robustness analysis of interdependent networks: Influences of intranetwork and internetwork degree-degree correlations** - 2014 - [89]

    In this article Watanabe et al. develop a methodology for analyzing the percolation of interdependent networks based on the cavity method of statistical mechanics. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "targeted attacks", "node degree correlation", "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results obtained indicate that the robustness of the interdependent networks nontrivially depends on both the intra-network and inter-network degree for random failures and targeted attacks.

29. **Robustness of a partially interdependent network formed of clustered networks** - 2014 - Shuai Shao, Xuqing Huang, H. Eugene Stanley, Shlomo Havlin [75]

This article extends the study of clustering to interdependent networks with clustering within the network components. To do this two "one to one like" models were used, one where each node can be bidirectionally connected to at most one other node, and one consisting of n partially coupled layers. To assess the robustness the framework uses two "counting elements" metrics: the relative size of the giant connected component in one of the participating networks, and the fractional size of the giant component of one network after t cascading failures. The "breaking point" metric *percolation threshold* was also used. Here, "coupling", "clustering coefficient", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. Among the results it is found that as the clustering coefficient increases the system becomes less robust.

30. **Robustness of interdependent networks with different link patterns against cascading failures** - 2014 - Jianwei Wang, Chen Jiang, Jianfei Qian [83]

    This article studies the effect of different types of coupling over the robustness of a fully interdependent system with loads. To do this a "one to one like" network where a modification of the original one to one model with added loads within the networks is used. To measure the robustness, the framework uses two "counting elements" metrics: the average amount of lost nodes after a cascading failure (average avalanche), and the increased amount of lost or failed nodes relative to the same initial failure on a single network. Here, "coupling", "single network contrast", and "avalanche" studies were performed. The framework uses "real and simulated" networks for testing. The results show that coupling patterns and system parameters can dramatically improve the robustness of the system against cascading failures.

31. **Study of the Use of a Genetic Algorithm to Improve Networked System-of-Systems Resilience** - 2014 - Charles O. Adler, Cihan H. Dagli [1]

    This article studies the overall level of failure and the rate of failure progression of and interdependent networks system, and uses a genetic algorithm to demonstrate an integrated failure modeling based optimization method to select systems with improved robustness. To do this a "geometric or spatially embedded" model consisting of spatially embedded networks where two nodes can be connected through interdependent links if the distance between them meets the requirements is used. To measure the robustness, the framework uses a "counting elements" metric that measures the amount of nodes inactive after the cascading process, and a "rate" metric that measures how abrupt the cascading process. Here, "localized attacks", and "geometric algorithm" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show fast convergence to steady states and values for the methods tested.

32. **Design of Robust Dependent Networks against Flow-based Cascading Failures** - 2014 - T.M. Ouboter, D.T.H. Worm, Robert E. Kooij, Huijuan Wang [56]

    In this article strategies to increase the robustness of a communication network which depends on the proper function of an electricity network are proposed. The strategies involve selecting nodes of the communication network and decoupling them. To do this a "coupled power grid" model representing the Power Grid (PG) coupled with the Supervisory Control And Data Acquisition (SCADA), considering loads on the PG network, is used. To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component). Here, "coupling", and "size of the largest connected component" studies were performed. The framework uses "real and simulated" networks for testing. The results show that a hybrid strategy, based on the degree

of the communication nodes and the failure probabilities of the electricity nodes, give a significant improvement over a random selection strategy, and other strategies tested.

33. **Analysis of percolation behaviors of clustered networks with partial support–dependence relations** - 2014 - Gaogao Dong, Lixin Tian, Ruijin Du, Min Fu, H. Eugene Stanley [19]

    This article studies the percolation behaviour of clustered networks with partial support-dependence relations using different attack strategies. To do this a "multiple dependencies" model is used. This model considers directed dependencies where in order for a node to remain functional at least one of its supporting nodes in other networks must be functional. To measure the robustness, the framework uses two "breaking point" metrics (percolation threshold, critical coupling), and a "time" metric (number of iterations that a cascading failure takes until it stops). Here, "coupling", "cascading time", and "percolation" studies were performed. As for the framework testing, the article uses "simulated" networks only. The article's findings suggest that a more robust network can be obtained by reducing the clustering coefficient and increasing the average degree for strong coupling strength.

34. **Avoiding catastrophic failure in correlated networks of networks** - 2014 - S. D. S. Reis, Yanqing Hu, Andrés Babino, J. S. Andrade Jr., Santiago Canals, Mariano Sigman, Hernán A. Makse [68]

    In this article Reis et al. study the stability of interdependent networks. To do this the article uses a "multiple dependencies" model, where in order for a node to remain functional it must have at least one out-going link to other network and be connected to the giant component on its local network. To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "percolation", and "size of the giant connected component" studies were performed. The framework uses "real and simulated" networks for testing. As result, they find that the stability of an interdependent networks system relies on the relation between the internal structure and the coupling patterns. In particular, they show that if interconnections are provided by network hubs, and the connections between networks are moderately convergent, the system of networks is stable and robust against failure.

35. **Modeling the Interaction of Power Line and SCADA Networks** - 2014 - Yuki Matsui, Hideharu Kojima, Tatsuhiro Tsuchiya [53]

    This article discusses the robustness of a Power Grid (PG) coupled to a Supervisory Control And Data Acquisition network (SCADA) against failures. To do this a "coupled power grid" model representing the PG coupled with the SCADA considering loads on the PG network is used. To measure the robustness, the framework uses a "counting elements" metric that measures the ratio of power grid nodes that can still be observed and controlled after failure. Here, only "coupling" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results suggest that the robustness increases as the inter-similarity between the two networks increases.

36. **How breadth of degree distribution influences network robustness: Comparing localized and random attacks** - 2015 - Xin Yuan, Shuai Shao, H. Eugene Stanley, Shlomo Havlin [91]

    This article studies the effect of the breadth of the degree distribution over the robustness of interdependent networks against localized attacks (LA) and random attacks (RA). To do this the

original one to one model ("one to one like") is used. To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric. Here, "localized attacks", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that in most cases the interdependent systems are more vulnerable to LA than to RA.

37. **Cascading failure propagation in interconnected networks with tunable load redistribution strategy** - 2015 - Sheng Hong, Baoqing Wang, lianghui Wang [30]

    This article proposes a tunable load distribution model for interdependent networks, where redistribution range and homogeneity are adjustable. To do this a "load transfer among networks" model is used. In this model after a node failure, the load of a node is immediately transferred to its neighbours within and among networks. To measure the robustness, the framework uses a "counting elements" metric, and a "breaking point" metric. The first corresponds to the size of the largest connected component, and the latter measures the critical value of the tolerance parameter in the capacity formula, where the largest connected component is half of the original system size after failure. Here, "coupling", "targeted attacks", "load and capacity", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that robustness of interconnected networks depend on the coupling pattern and load redistribution strategy.

38. **Towards Optimal Link Patterns for Robustness of Interdependent Networks against Cascading Failures** - 2015 - Srinjoy Chattopadhyay, Huaiyu Dai [8]

    In this article an optimal interdependent network design is developed using information of intralayer node degrees to design more robust interdependent structures against random attacks. To do this three models were used: two "one to one like" models, and one "multiple dependencies" model. The "one to one like" models used were: the original one to one model, and a model where each node can be bidirectionally connected to at most one other node. While the "multiple dependencies" model used had directed dependencies where in order for a node to remain functional at least one of its supporting nodes in other networks must be functional. To measure the robustness, the framework uses a "counting elements" metric that measures the relative size of the largest connected component of a single network of the system. Here, "targeted attacks", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that interconnections patterns where the connections are ordered by degree, and nodes with highest degree become autonomous, improve the robustness of the system.

39. **Cascading failure of interdependent networks with different coupling preference under targeted attack** - 2015 - Zhen Chen, Wen-Bo Du, Xian-Bin Cao, Xing-Lian Zhou [11]

    This article studies the effect of coupling patterns over the robustness of interdependent network systems. To do this, the article uses a modification of the original one to one model with added loads within the networks ("one to one like"). To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component). Here, "avalanche", "coupling", "targeted attacks", "load and capacity", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only.

The results show that dissasortative coupling is more robust for sparse coupling, while assortative coupling performs better for dense coupling.

40. **Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis** - 2015 - Min Ouyang, Zhenghua Wang [57]

    This article presents an adaptation for interdependent networks of an existing resilience assessment framework for single networks. To do this a "coupled power grid" model consisting of the gas network coupled with the power grid network, including intra-networks loads, is used. To measure the robustness, the framework uses a "performance" metric that measures the performance of the system relative to the expected performance. Here, "recovery", and "genetic algorithm" studies were performed. The framework uses "real and simulated" networks for testing. The results show that *independent* recovery strategies, and *power grid first* recovery strategies perform better for power grid restoration than other strategies tested. While the *power and gas compromised* recovery strategy produces the largest total resilience.

41. **Cascading Failures in Smart Grid: Joint Effect of Load Propagation and Interdependence** - 2015 - Zhen Huang, Cheng Wang, Tieying Zhu, Amiya Nayak [34]

    This article studies the system's robustness considering cascading failures due to interdependencies among networks, and load propagation failures. To do this a "coupled power grid" model was used. This model considers the power grid with loads and capacities, and the communication network coupled. The communication network has two types of nodes: control nodes and information relays. Here each control node takes care of n information relays, and each information relay is watched by k control nodes. To measure the robustness, the framework uses a "counting elements" metric that measures the fraction of operating giant components in the steady state, and a "breaking point" metric that measures the critical tolerance parameters before collapse. Here, "percolation", "size of the giant connected component", and "load and capacity" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results analysis shows that the fraction of survivals in the power grid is always greater than that in communication network.

42. **Cascading failures in interconnected networks with dynamical redistribution of loads** - 2015 - Zhuang Zhao, Peng Zhang, Hujiang Yang [98]

    In this article flow dynamics on interdependent networks are studied. To do this a "load transfer among networks" model is used. In this model, after a failure the loads are redistributed within the network and excess network load is then transferred to other networks. To assess the robustness the framework uses the global efficiency metric ("path length"). Here, "targeted attacks", "efficient paths", and "load and capacity" studies were performed. The framework uses "real and simulated" networks for testing. The results show that enhancing the heterogeneity between nodes make networks more susceptible, and coupling preference make almost no difference on the robustness of the system.

43. **Cascade of failures in interdependent networks coupled by different type networks** - 2015 - Zunshui Cheng, Jinde Cao [12]

    This article studies the robustness of interdependent networks under targeted and random attacks. To do this the original one to one model ("one to one like") is used. To measure the robustness, the

framework uses a “counting elements” metric (size of the largest connected component), a “breaking point” metric (percolation threshold), and a “time metric” (number of iterations that a cascading failure takes until it stops). Here, “targeted attacks”, “percolation”, “cascading time”, and “size of the largest connected component” studies were performed. As for the framework testing, the article uses “simulated” networks only. Some results presented are: for random attacks, the existence of a giant connected component after an attack will vary depending if the networks used to create the system are different or not. For targeted attacks, if the highly connected nodes are protected, the system leads to a first order percolation phase transition for different type coupled-networks, and a second transition for same type coupled-networks.

44. **Percolation transitions in the survival of interdependent agents on multiplex networks, catastrophic cascades, and solid-on-solid surface growth** - 2015 - Peter Grassberger [28]

    In this article interdependent networks represented as duplex (2-layer multiplex) systems are studied using algorithms based on a solid-on-solid type growth model. To do this a “one to one like” model that represents a multiplex network is used. To assess the robustness the framework uses a “counting elements” metric (size of the largest connected component), and a “probability” metric that measures the probability that a giant connected component exists after failure. Here, “coupling”, “percolation”, “small cluster”, and “size of the giant connected component” studies are performed. As for the framework testing, the article uses “simulated” networks only. The results found that for duplex Erdös-Rényi networks the cluster statistics are exactly described by mean field theory, but that the cascade process is not. In the case of lattices it is found, among other results, that a dimension $d = 4$ is the upper critical dimension for abrupt cascading failures.

45. **Percolation on networks with antagonistic and dependent interactions** - 2015 - Bhushan Kotnis, Joy Kuri [42]

    In this article Kotnis et al. study an interdependent system consisting of two networks that exhibit antagonistic and dependent interactions. To do this a “mixed interactions” model with antagonistic or dependent interactions between node pairs is used. To measure the robustness, the framework uses two “counting elements” metrics. The first measures the size of the largest connected component, and the second measures the relative size of the giant connected component in one of the participating networks. Here, “coupling”, “percolation”, “antagonistic nodes”, “cascading time”, and “size of the giant connected component” studies are performed. As for the framework testing, the article uses “simulated” networks only. The results show that, compared to isolated networks, the system is more robust against random attacks.

46. **Small Cluster in Cyber Physical Systems: Network Topology, Interdependence and Cascading Failures** - 2015 - Zhen Huang, Cheng Wang, Amiya Nayak, Ivan Stojmenovic [33]

    In this article a mathematical method based on percolation theory is proposed. This method includes small clusters instead of only focusing on the largest connected component of an interdependent system. To do this a “coupled power grid” model was used. This model considers the power grid and the communication network coupled. The communication network has two types of nodes: control nodes and information relays. Here each control node takes care of n information relays, and each information relay is watched by k control nodes. To assess the robustness the framework uses a “counting elements” metric that measures the amount of small functional clusters. Here, “targeted attacks”, “percolation”, “small cluster”, and “size of the giant connected

components" studies are performed. The framework uses "real and simulated" networks for testing. Among the results it is found that a considerable proportion of small clusters, distinct from the largest connected component, exist after failure.

47. **Localized attacks on spatially embedded networks with dependencies** - 2015 - Yehiel Berezin, Amir Bashan, Michael M. Danziger, Daqing Li, Shlomo Havlin [4]

    In this article, Berezin et al. study a general model of interdependent spatially embedded networks under localized attack. To do this a "geometric or spatially embedded" model is used. This model consists of spatially embedded networks where two nodes can be connected through interdependent links if the distance between them meets the requirements. To measure the robustness, the framework uses a "breaking point" metric that measures the attack radius that leads the system to collapse. Here, "length", "percolation", "localized attack stability", and "localized attacks" studies were performed. As for the framework testing, the article uses "simulated" networks only. Among the results, the authors find that localized attacks cause more damage than an equivalent random attack, and that many configurations that appear stable are in fact meta-stable. Here, a meta-stable system is one that is stable for any localized attack whose radius is below a threshold, but collapses if the radius is above that threshold.

48. **Percolation in real interdependent networks** - 2015 - Filippo Radicchi [64]

    In this article a set of heuristic equations that take the adjacency matrices of the interdependent system's layers are introduced. With this, the entire phase diagram for the interconnected network is drawn. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "breaking point" metric (percolation threshold), and a "probability" metric that measures the average probability of a node of being connected to the largest connected cluster. Here, only "percolation" studies are performed. The framework uses "real and simulated" networks for testing. The results show that percolation transitions in interdependent networks can be understood by decomposing the system into uncoupled graphs: the intersection among layers, and the remainders. When the intersection dominates the remainders, the percolation transition is smooth. Conversely, if the intersection is dominated by the contribution of the remainders, the transition becomes abrupt even in small networks.

49. **Enhancing robustness of coupled networks under targeted recoveries** - 2015 - Maoguo Gong, Lijia Ma, Qing Cai, Licheng Jiao [26]

    This article analyzes the cascading failures of coupled networks during recovery, presents a metric to measure robustness during recovery, and proposes a technique to protect influential nodes and enhance robustness during recovery. To do this a "one to one like" model is used. In this model each node can be bidirectionally connected to at most one other node. To assess the robustness the framework uses a "counting elements". This metric observes the total amount of functional nodes for different amounts of recovered nodes. Here, "coupling", "percolation", and "recovery"studies are performed. The framework uses "real and simulated" networks for testing. This work shows that with the right protection strategy, only a small number nodes needs to be protected to greatly enhance the robustness of the system.

50. **Robust allocation of weighted dependency links in cyber–physical networks** - 2015 - Xin Li, Haotian Wu, Caterina Scoglio, Don Gruenbacher [45]

In this article a more realistic approach to modelling interdependent networks is taken by using a one-to-many model with weighted dependency links between the two networks. This work also formulates an optimization problem to allocate dependency links using the least resources, and proposes an algorithm to solve this problem. To do this, the authors use a weighted "multiple dependencies" model where in order for a node to remain functional it must be connected to the largest connected component, and at least one of their neighbours in the other networks must remain functional. To measure the robustness they use a "counting elements" metric that measures the average size of the largest connected component. Here, "cost", "coupling", "optimization", and "size of the giant connected component" studies are performed. The framework uses "real and simulated" networks for testing. The deployment method proposed in this article is shown to produce topologies that are more robust than the ones obtained using other techniques. It is also shown that the algorithm proposed is efficient and cost-effective in designing robust interdependent networks.

51. **Robust-yet-fragile nature of interdependent networks** - 2015 - Fei Tan, Yongxiang Xia, Zhi Wei[80]

    This article studies the effect of coupling patterns over cascading failures, considering loads, in interdependent networks. To do this a modification of the original one to one model with added loads within the networks is used ("one to one like"). To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "targeted attacks", "load and capacity", "coupling", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that interdependent Erdös-Rényi networks are robust-yet-fragile under both random failures and intentional attack, while interdependent Barabási-Albert networks are only robust-yet-fragile under random failure, but fragile under intentional attack.

52. **Effect of network size on robustness of interconnected networks under targeted attack** - 2015 - Wenping Zhang, Yongxiang Xia, Bo Ouyang, Lurong Jiang [93]

    This article studies the effect that different network sizes have over the cascading failures on interdependent networks with loads. To do this a "load transfer among networks" model is used. In this model there are loads within networks, and if a node fails, the overload is redistributed through inner-links and inter-links. To assess the robustness the framework uses two "counting elements" metrics: one that measures the relative size of the giant connected component in one of the participating networks, and other that measures the size of the largest connected component. This framework also uses a "breaking point" metric that measures the critical load tolerance parameter (involved in the node capacity formula) at which the largest connected component is cut by half after a cascading failure. Here, "coupling", "targeted attacks", "load and capacity", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that when two networks with similar sizes are coupled, sparse coupling results in a fragile system, while dense coupling results in a robust system. For the case of two networks with different sizes, the larger one is more robust for sparse coupling, while it is more fragile for dense coupling.

53. **Robustness of network of networks with interdependent and interconnected links** - 2015 - Gaogao Dong, Ruijin Du, Lixin Tian, Runran Liu [17]

In this article Dong et al. develop a framework to analytically and numerically study the robustness of interdependent systems considering no-feedback and feedback conditions. The no-feedback implies bidirectional dependency between nodes. To do this a "mixed interactions" model is used. This model has N networks coupled through dependency and connectivity links, here, a node is functional if it is connected to some giant connected component. To measure the robustness, the framework uses a "counting elements" metric (average size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results suggest that, for no-feedback and feedback conditions, increasing density of connectivity links (intra-connectivity links or inter-connectivity links) can increase the robustness of the system, while the inter-links decrease its robustness.

54. **Cascading load model in interdependent networks with coupled strength** - 2015 - Jianwei Wang, Yun Li, Qiaofang Zheng [84]

    This article studies the robustness of the interdependent networks against cascading failures using load related metrics. To do this a modification of the original one to one model with added loads within the networks is used ("one to one like"). To measure the robustness, the framework uses two "breaking point" metrics, and one "counting elements metric". The two "breaking point" metrics measure the critical β within the capacity formula at which a phase transition occurs (β_c), and the smallest capacity threshold $\beta_{c,s}$ where if β is below this threshold any removal can can lead to the cascading propagation in the whole interdependent system. While the "counting element" metric measures the average amount of nodes lost after a cascading failure (avalanche). Here, "targeted attakcs", "coupling", "avalanche", and "load and capacity" studies were performed. As for the framework testing, the article uses "simulated" networks only. Among the results shown in the article it is found that for disassortative coupling and random coupling the values of β_c increase monotonically with the coupled strength, while the values of $\beta_{c,s}$ almost monotonically decreases with the coupled strength for all the coupling patterns tested.

55. **Complex interdependent supply chain networks: Cascading failure and robustness** - 2016 - Liang Tang, Ke Jing, H. Eugene Stanley [81]

    In this article cascading failure processes considering loads are used to study the robustness of an interdependent supply-chain network. To do this a "supply-chain" model is used. This model considers a cyber-layer and a physical-layer, each with loads and load constraints. In the physical-layer edges are directed as nodes represent suppliers, manufacturers, distributors and costumers, while in the cyber-layer link are non-directed since they represent information pathways. The interactions between both networks are bidirectional and each node can be interconnected to one node in the other network. To assess the robustness the framework uses robustness a "counting elements" metric. This metric measures the area below the curve formed by the plot of the amount of functional nodes versus the amount of nodes removed. Here, "size of the giant connected component", and "load and capacity" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that when the number of removed nodes increases the interdependent supply chain network undergoes a first-order discontinuous phase transition, and that even removing a small number of nodes will cause the system to collapse.

56. **Improving interdependent networks robustness by adding connectivity links** - 2016 - Xingpei Ji, Bo Wang, Dichen Liu, Guo Chen, Fei Tang, Daqian Wei, Lian Tu [35]

This articles aims to improve the robustness of interdependent networks by adding connectivity links. This article tests existing link addition strategies as well as new strategies. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "coupling", "fraction of added intralinks", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that, given the number of added links, link allocation strategies have great effects on the robustness of interdependent networks. In particular it is shown that the double-network link allocation strategy is superior to single-network link allocation strategy, and that the link addition strategies proposed excel the existing strategies tested.

57. **Resilience of interdependent communication and power distribution networks against cascading failures** - 2016 - Wei Koong Chai, Konstantinos V. Katsaros, George Pavlou [7]

    This article empirically studies the robustness of interdependent systems formed by the coupling of power grids and communication networks by putting real power grids to the test. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "path length metric" (how fast information spreads in a network). Here, "targeted attacks", "amount of components", and "size of the giant connected component" studies were performed. The framework uses "real and simulated" networks for testing. Among the results it is shown that current medium voltage grids are highly vulnerable to cascading failures, and that the formation of hub hierarchies, which is known to enhance independent network robustness, has detrimental effects on interdependent network robustness

58. **Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks** - 2016 - Shiwen Sun, Yafang Wu, Yilin Ma, Li Wang, Zhongke Gao, Chengyi Xia [79]

    This article studies the effect of degree heterogeneity on interdependent networks' robustness under targeted attacks. To do this a "one to one like" model is used. In this model each node can be bidirectionally connected to at most one other node. To assess the robustness the framework uses a "path length" metric that measures the lost efficiency of the system. Here, "targeted attacks", "coupling", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that degree heterogeneity can significantly decrease interdependent network robustness, that interdependent links between two networks make the entire system much more fragile to attacks, and that enhancing coupling strength between networks can greatly increase the fragility of both networks against targeted attacks.

59. **Hybrid phase transition into an absorbing state: Percolation and avalanches** - 2016 - Deokjae Lee, S. Choi, Marcell Stippinger, János Kértesz, B. Kahng [43]

    This article studies the hybrid phase transition phenomena of interdependent network. To do this the original one to one model ("one to one like"), and a "geometric or spatially embedded" model consisting of spatially embedded networks where two nodes can be connected through interdependent links if the distance between them meets the requirements are used. To measure the robustness, the framework uses a "counting elements" metric that measures the average amount of nodes lost after a cascading failure (avalanche), a "time" metric (number of iterations that a cascading failure takes until it stops), and a "probability" metric that measures the probability that a

giant connected component exists after failure. Here, "percolation", and "avalanche" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show divergence of the fluctuations of the order parameter and Power-Law size distribution of finite avalanches at a transition point. Also, at the transition point global or "infinite" avalanches occur, and the finite ones have a Power-Law size distribution.

60. **Modeling region-based interconnection for interdependent networks** - 2016 - Xiangrong Wang, Robert E. Kooij, Piet Van Mieghem [88]

    This article proposes and evaluates the robustness of two models that take into consideration the geographic position of nodes. To do this two "geometric or spatially embedded" models are used. In the first one a node might depend on zero or one or more than one node, and two nodes get connected if the Euclidean distance between them is smaller than a given threshold. The second one is similar to the first one, but here two nodes get connected if there is no third node in the intersection region of two circles with centers at each node with radius equal to their Euclidean distance. To assess the robustness the framework uses a "counting elements" metric (size of the largest connected component), and a "rate" metric (size of the largest connected component derivative respect to the amount of nodes lost). Here, "length", and "size of the giant connected component" studies are performed. The framework uses "real and simulated" networks for testing. The results show that the metric proposed allows to quantify robustness even for a small amount of nodes lost.

61. **Interdependent lattice networks in high dimensions** - 2016 - Steven Lowinger, Gabriel A. Cwilich, Sergey V. Buldyrev [52]

    This article studies the percolation of two interdependent lattice networks with dimensions ranging from two to seven. To do this a "geometric or spatially embedded" model is used. This model considers two coupled lattices, each with dimension D. In this model each node is connected to its $2D$ nearest-neighbor nodes, and inter-connections are bidirectional and can be established between nodes whose distance is no larger than r. To measure the robustness, the framework uses a "breaking point" metric (percolation threshold), and a "probability" metric (cumulative distribution of the mutual giant component). Here, "length", "size of the second largest component", "percolation", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. Among the results the authors find that for each dimension studied there is a radius r of minimum robustness, for radius below or below it the robustness increases.

62. **The effect of capacity redundancy disparity on the robustness of interconnected networks** - 2016 - Yongxiang Xia, Wenping Zhang, Xuejun Zhang [90]

    This article analyzes the effect of capacity redundancy disparity on the robustness of interconnected networks. To do this a "load transfer among networks" model is used. In this model there are loads within networks, and if a node fails, the overload is redistributed through inner-links and inter-links. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "coupling", "targeted attacks", and "load and capacity" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that when the capacity redundancy is fixed, the robustness of the system may not correlate to it as expected.

63. **Targeted attack on networks coupled by connectivity and dependency links** - 2016 - Ruijin Du, Gaogao Dong, Lixin Tian, Runran Liu [20]

    This article analytically and numerically analyzed the robustness of coupled networks under three types of targeted attack strategies. To do this a "mixed interactions" model is used. This model has N networks coupled through dependency and connectivity links, and a node is functional if it is connected to some giant connected component. To assess the robustness the framework uses a "breaking point" metric (percolation threshold), and a "counting elements" metric (size of the giant connected component). Here, "coupling", "targeted attacks", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results imply that the degree distribution and coupling strength can be adjusted to modify the systems robustness. The results also imply that one should not only protect nodes with high degree of intra-links or inter-links, but also defend nodes where the sum of both quantities is big.

64. **Reducing the impact of targeted attacks in interdependent telecommunication networks** - 2016 - Diego F. Rueda, Eusebi Calle, F. A. Maldonado-Lopez, Y. Donoso [70]

    In this article Rueda et al. study the changes in robustness when interdependent networks with similar topological properties interact. They focus on interdependent telecommunication networks modeled as two Erdös-Rényi (ER) random graphs, and propose three link patterns to couple them. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "probability" metric. This metric is the Average Two-Terminal Reliability (ATTR) and it measures the probability of the connectivity between a randomly chosen node pair in a single network. Here, "coupling", and "targeted attacks" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results indicate that different coupling patterns allow them to identify new critical parts of the network and improve robustness level under targeted attacks.

65. **Shell attack on interdependent networks** - 2016 - Gaogao Dong, Ruijin Du, Hao Huifang, Lixin Tian [25]

    This article studies the effect of localized attacks over the robustness of interdependent networks, where nodes can be protected or unprotected. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (average size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "localized attacks", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results suggest that the robustness of the systems relies not only on the coupling strength, but also on the average degree.

66. **Improved percolation theory incorporating power flow analysis to model cascading failures in Cyber-Physical Power System** - 2016 - Yuqi Han, Zhi Li, Yuezhong Tang [29]

    This article presents an improved percolation theory to analyze power grids which incorporates the AC power flow analysis to model cascading failure process. To do this a "coupled power grid" model is used. This model considers the power grid and its control network. The power grid considers loads and capacities, and a node can fail due to overload, to not being connected to the largest connected component, or because it lost all of its counterparts. To assess the robustness the framework a "counting elements" metric that measures the ratio of lost nodes after the cascading

process. Here, “targeted attacks”, “coupling”, and “avalanche” studies are performed. As for the framework testing, the article uses “simulated” networks only. Among the results it is shown that topological centrality based node attack can cause heavier damage, and that compared with the conventional percolation theory, the proposed percolation theory model provides a better way to understand the robustness of power grid systems.

67. **Study of Robustness in Functionally Identical Coupled Networks against Cascading Failures** - 2016 - Xingyuan Wang, Jianye Cao, Xiaomeng Qin [87]

    In this article an interdependent system of functionally identical coupled networks that consider node load and capacities is proposed. To do this a “load transfer among networks” model where after a node failure the load of a node is immediately transferred to its neighbours within and among networks is used. To measure the robustness, the framework uses a “counting elements” metric that measures the normalized amount of functional nodes after failures. Here, only “load and capacity” studies are performed. The framework uses “real and simulated” networks for testing. Among the results, it is found that functionally identical coupled networks are more robust than single networks under random attack, and that a broader degree distribution and a higher average degree increase the robustness of functionally identical coupled networks under random failure.

68. **Redundant Design in Interdependent Networks** - 2016 - Lijun Liu, Yongfeng Yin, Zenghu Zhang, Yashwant K. Malaiya [48]

    This article proposes two redundant design methods to enhance the robustness of interdependent systems that consider node loads and capacities: node back-up, and dependency redundancy. To do this a modification of the original one to one model with added loads within the networks is used (“one to one like”). To assess the robustness the framework uses a “counting elements” metric (average size of the largest connected component). Here, “avalanche”, “cost”, “failure distribution”, and “load and capacity” studies are performed. As for the framework testing, the article uses “simulated” networks only. The results show that selecting nodes back-ups using a historical failure distribution criteria combined with dependency redundancy is an effective way to implement redundant design on interdependent networks.

69. **Operational resilience: concepts, design and analysis** - 2016 - Alexander A. Ganin, Emanuele Massaro, Alexander Gutfraind, Nicolas Steen, Jeffrey M. Keisler, Alexander Kott, Rami Mangoubi, Igor Linkov [22]

    This article proposes quantitative measures that capture and implement the definition of engineering resilience adviced by the National Academy of Sciences. To do this a “one to one like” model is used. In this model each node can be bidirectionally connected to at most one other node. To measure the robustness, the framework uses two “counting elements” metrics: the amount of functional nodes on a certain time t, and the integral of the first metric over time. Here, “recovery”, and “size of the giant connected component” studies were performed. The framework uses “real and simulated” networks for testing. The results indicate that desired resilience and robustness levels are achievable by trading off different design parameters, such as redundancy, node recovery time, and backup supply available.

70. **Recovery of Interdependent Networks** - 2016 - M. A. Di Muro, C. E. La Rocca, H. Eugene Stanley, Shlomo Havlin, Lidia A. Braunstein [15]

This article proposes a recovery strategy for failed nodes on an interdependent networks system, and develops an analytic and numerical framework for studying the concurrent failure and recovery of the system. To do this the original one to one model ("one to one like") is used. To assess the robustness the article uses a "counting elements" metric (relative size of the largest connected component in one of the networks of the system), and a "time" (number of iterations that a cascading failure takes until it stops). Here, "percolation", "recovery", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that for a given initial fraction of failed nodes there is a critical probability of recovery. Above this critical probability the cascade is halted and the system fully restores to its initial state, and below it the system abruptly collapses.

71. **The robustness of multiplex networks under layer node-based attack** - 2016 - Da-wei Zhao, Lian-hai Wang, Yong-feng Zhi, Jun Zhang, Zhen Wang [96]

    This article studies the robustness of multiplex networks under layer node-based attacks, random or targeted. Under layer node-based attacks, nodes just suffer attacks in a given layer, yet there is no additional influence to their connections beyond this layer. To do this a "mixed interactions" model representing a multiplex network is used. In his model a pair of multiplex nodes are regarded to have connection if there exists at least one type of link between them, and thus, attacking nodes on some layer may not destroy their connection with other nodes. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "targeted attacks", "probability of failure", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that layer node-based attacks makes multiplex networks more vulnerable compared to node-based attacks, regardless of the underlying topology.

72. **Cascading failures in coupled networks with both inner-dependency and inter-dependency links** - 2016 - Runran Liu, Ming Li, Chun-Xiao Jia, Bing-Hong Wang [50]

    This article studies the percolation of coupled networks with inner-dependency and inter-dependency links. To do this a "mixed interactions" model is used, where nodes can connect to nodes in any network through dependency links or to nodes of the same network through non-directed links. In this model, dependency links are bidirectional. To measure the robustness, the framework uses a "counting elements" metric (relative size of the largest connected component in one of the networks of the system). Here, "coupling", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that when there is a great majority of inner-links or inter-links, the system goes through a discontinuous percolation transition, and when there is a balance between both types of dependency links, the system becomes more robust as it undergoes a continuous percolation transition.

73. **Supporting differentiated resilience classes in multilayer networks** - 2016 - Abdulaziz Alashaikh, David Tipper, Teresa Gomes [2]

    This articles proposes an approach to simplify the design of robust services over communications networks using a multi-layered approach. To do this a "mapping" model considering loads is used. This model represents an application request to a substrate network, and considers a physical network, and a logical topology on top of which an overlay network is mapped. To assess the robustness a "time" metric that measures how long a user can access to the services provided by

the network is used. Here, “cost”, “optimization”, and “load and capacity” studies are performed. The framework uses “real and simulated” networks for testing. The results show that, compared to existing techniques, the model proposed in this article can create a wider range of availability levels.

74. **Cascading failures in coupled networks: The critical role of node-coupling strength across networks** - 2016 - Runran Liu, Ming Li, Chun-Xiao Jia [49]

    This article studies the robustness of interdependent networks where the node-coupling strength is controlled by a specific parameter α. To do this a “one to one like” model is used. This model has one to one interactions, but here, if a node fails then its counterpart will lose each connectivity link with a certain probability $(1-\alpha)$. The probability of losing connectivity links can be set so all the connectivity links are lost, and thus, the resulting model is equal to the original one to one. To measure the robustness, the framework uses a “counting elements” metric (relative size of the largest connected component in one of the networks of the system), and a “breaking point” metric (percolation threshold). Here, “coupling”, “percolation”, and “size of the giant connected component” studies were performed. As for the framework testing, the article uses “simulated” networks only. The authors find that there is a rich phase diagram for the studied scenarios, with a crossover point at which a first-order percolation transition changes to a second-order percolation transition.

75. **Cascade-robustness optimization of coupling preference in interconnected networks** - 2016 - Xue-Jun Zhang, Guo-Qiang Xu, Yan-Bo Zhu, Yongxiang Xia [95]

    This articles uses the memetic algorithm (MA) to optimize the coupling of interdependent networks. To do this a “one to one like” model is used. In this model each node can be bidirectionally connected to at most one other node. To measure the robustness, the framework uses a “counting elements” metric (size of the largest connected component). Here, “targeted attacks”, “coupling”, “load and capacity”, an “size of the giant connected component” studies were performed. The framework uses “real and simulated” networks for testing. The results show that the MA optimized coupling strategy with a moderate assortative value greatly improves the robustness of the system.

76. **Fuzzy-information-based robustness of interconnected networks against attacks and failures** - 2016 - Qian Zhu, Zhiliang Zhu, Yifan Wang, Hai Yu [103]

    This article studies cascading failures on interdependent networks using fuzzy information to resist failures and attacks. To do this a “load transfer among networks” model is used. In this model after a node failure the load of that node is immediately transferred to its neighbours within the network and among interacting networks. To measure the robustness, the framework uses a “counting elements” metric (size of the largest connected component). Here, “percolation”, “coupling”, “information to attack”, and “size of the giant connected component” studies were performed. The framework uses “real and simulated” networks for testing. The results show that, given the coupling probability, the robustness of the assortative coupling, and random coupling of the network model increases with the coupling probability.

77. **Reliability analysis of interdependent lattices** - 2016 - Zhang Limiao, Daqing Li, Qin Pengju, Fu Bowen, Jiang Yinan, Enrico Zio, Rui Kang [46]

In this article the reliability properties of interdependent lattices with different ranges of spatial constraints are studied. To do this a "geometric or spatially embedded" model is used. This model considers that each element has a lifetime after which it fails, that dependencies between nodes of different networks are bidirectional, that there are distances between nodes, and that a node must be connected to the largest connected component in order to remain functional. Two nodes can be inter-connected if the distance between them is less than r. To measure the robustness, a "breaking point" metric that measures how close the system is to a collapsed state is used. Here, "length", "lifetime", and "size of the giant connected component" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that interdependent lattices with strong spatial constraints are more resilient than interdependent Erdös-Rényi networks, and that there is an intermediate range of spatial constraints where coupled lattices have minimal resilience.

78. **Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach** - 2016 - Mahshid Rahnamay-Naeini, Majeed M. Hayat [66]

    In this article an interdependent Markov-chain based framework to capture and analyze the the robustness of an interdependent network system is proposed. To do this a "defined by probabilities" model is used. This model provides a probabilistic framework to capture the effects of interdependencies among physical networks on the stochastic dynamics of cascading failures in an abstract setting. To assess the robustness a "probability" metric that measures whether the system is reliable or unreliable given the probability distribution of the cascading size. Here, "failure size PMF", "probability of stabiization", and "Markov-chains" studies were performed. As for the framework testing, the article uses "simulated" networks only. Using the proposed framework it is shown that interdependencies among reliable systems can make individually reliable systems behave unreliably as a whole.

79. **Robustness of single and interdependent scale-free interaction networks with various parameters** - 2016 - Shuai Wang, Jing Liu [85]

    This article studies the change of robustness along with different parameters, including scaling exponent and assortativity of interdependent networks. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "coupling", "targeted attacks", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that a balanced degree distribution, and higher propensity of similar-degree connectivity contribute to the robustness of interdependent networks against node attacks.

80. **Percolation-cascading in multilayer heterogeneous network with different coupling preference** - 2017 - Wang Xiao Juan, Guo Shi Ze, Jin Lei, Wang Zhen [37]

    This article focuses on the study of percolation-cascading process in multilayer heterogeneous networks, and design a stochastic structural algorithm to generate dependency edges between the system's layers. To do this the original one to one model ("one to one like") is used. To assess the robustness a "probability" metric that measures the probability that a randomly chosen node belongs to the resulting mutual largest component after a cascading failure occurred is used. Here, "coupling", and "size of the giant connected component" studies are performed. As for the

framework testing, the article uses “simulated” networks only. Among the results it is shown that assortative networks perform better against cascading failures.

81. **Cascading failures in interdependent networks due to insufficient received support capability** - 2017 - Pengshuai Cui, Peidong Zhu, Chengcheng Shao, Peng Xun [13]

    In this article Cui et al. propose a capability based dependency model of interdependent networks that takes support capability and required capability into account. To do this a “multiple dependencies” model where support-dependency links allow nodes to give and receive resources or capability from other nodes is used. In this model a node remains functional if it belongs to the giant component, and if it receives at least the required amount of capability needed. To measure the robustness, the framework uses a “counting elements” metric (relative size of the largest connected component in one of the networks of the system), and a “breaking point” metric (percolation threshold). As for the framework testing, the article uses “simulated” networks only. Among the results it is found that interdependent networks without redundant support-dependence links are very vulnerable, that increasing support-dependency links and redistributing the nodes' dependency properties can enhance the robustness, and that improving the redundancy degree could enhance network robustness without adding support-dependence links.

82. **A preferential attachment strategy for connectivity link addition strategy in improving the robustness of interdependent network** - 2017 - Xingyuan Wang, Jianye Cao, Rui Li, Tianfang Zhao [86]

    In this article a link addition strategy for interdependent networks is proposed and compared with existing strategies. To do this the original one to one model (“one to one like”) is used. To measure the robustness, the framework uses a “counting elements” metric (size of the largest connected component). Here, “fraction of added intra-links”, “coupling”, and “size of the giant connected component” studies were performed. As for the framework testing, the article uses “simulated” networks only. It is found that improved link addition strategies increase the robustness of the system.

83. **A stochastic model for cascading failures in smart grid under cyber attack** - 2017 - Dong Liu, Xi Zhang, Chi K. Tse [47]

    This article presents a stochastic model for describing cascading failure in a cyber-coupled smart grid, and develops an algorithm to simulate the dynamic profile of the cascading failures, with consideration of the effect of power overloading, malware contagion and interdependency between the power grid and cyber network. To do this a “defined by probabilities” model is used. This model describes a power-grid coupled with its control network where the behaviour of each node within each network is defined through probabilities. To assess the robustness a “counting element” metric measures the average amount of nodes lost after a cascading failure (avalanche) is used. Here, “single network contrast”, “cascading time”, and “avalanche” studies are performed. As for the framework testing, the article uses “simulated” networks only. Among the results it is shown that compared with the isolated power system, the extent and rapidity of power blackouts are intensified by the coupling with the control network.

84. **Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures** - 2017 - Srinjoy Chattopadhyay, Huaiyu Dai, Do Young Eun, Seyyedali Hosseinalipour [10]

This article studies the optimal design of interlinks to maximize the robustness interdependent networks systems, using intra-layer node degrees information. To do this two "one to one like" models, and two "multiple dependencies" models are used. The first "one to one like" model is the original one to one model, and the second is the relaxed version of the original model where each node can be bidirectionally connected to at most one other node. For both "multiple dependencies" models in order for a node to remain functional it must be connected to the largest connected component. For the first model a node must also have at least one of their neighbours functional in one of the other networks, while for the second model a node must have all of their neighbours in the other networks functional. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "targeted attacks", "coupling", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. This work derives optimal interdependence structures, which are verified using network simulations.

85. **Designing optimal interlink structures for interdependent networks under budget constraints** [9]

    This article addresses the problem of obtaining optimal interlink structures that maximize the robustness of interdependent systems against random failure, while in a cost constrained setting. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "cost", "coupling", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that the designed algorithms have close to optimal performance while being much cheaper than other network designs.

86. **Robustness of multiple interdependent networks under shell attack** - 2017 - Wang Fan, Gaogao Dong, Ruijin Du, Lixin Tian [21]

    This article studies the robustness of interdependent networks under shell attacks. To do this, the authors use a weighted "multiple dependencies" model where in order for a node to remain functional it must be connected to the largest connected component, and at least one of their neighbours in the other networks must remain functional. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "localized attacks", "coupling", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results suggest that the robustness of the networks with multiple support-dependence links under shell attack depends on both connectivity links and support links.

87. **Balancing interdependent networks: Theory and algorithm** - 2017 - Zheng Liu, Qing Li, Dan Wang, Mingwei Xu [51]

    In this article Liu et al. study interdependent networks robustness through the balance coefficient defined in this work. To do this a "multiple dependencies" model with directed dependencies where in order for a node to remain functional at least one of its supporting nodes in other networks must be functional was used. To measure the robustness, the framework uses a "counting element" (balance coefficient). The balance coefficient measures the difference between the *lethality* of two networks to the system, and the lethal set is the set of nodes in either network

whose initial removals will cause system collapse. Here, “balance coefficient”, and “avalanche studies” are performed. As for the framework testing, the article uses “simulated” networks only. It is concluded that the balance coefficient is an appropriate metric to measure robustness of inter-dependent networks.

88. **Improving the robustness to targeted attacks in software defined networks (SDN)** - 2017 - Diego F. Rueda, Eusebi Calle, Jose L. Marzo [72]

    In this article a robust design of SDN control plane is presented. To do this a “one to one like” model representing a switch-switch network coupled with a control-switch network is used. In this model interdependencies are the same as in the original one to one model (fully connected, one to one, bidirectional dependencies), but here nodes in the control-switch network must be within a certain distance range of the controller, and a node must be connected to the controller to remain functional. To measure the robustness, the framework uses a “probability” metric. This metric is the Average Two-Terminal Reliability (ATTR) and it measures the probability of the connectivity between a randomly chosen node pair in a single network. Here, “intra-network topology”, and “targeted attack” studies are performed. The framework uses “real and simulated” networks for testing. Among the results it is shown that the network designed using the proposed algorithms is more robust than the study cases.

89. **Contact Adaption during Epidemics: A Multilayer Network Formulation Approach** - 2017 - Faryad Darabi Sahneh, Aram Vajdi, Joshua Melander, Caterina Scoglio [73]

    This article studies the preventive change in contacts that people show in response to infection diseases. To do this a “contagion or influence” model with Susceptible-Alert-Infected-Susceptible states where nodes can change their neighbourhoods when they become alert is used. To measure the robustness, the framework uses a “breaking point” metric. This metric measures the epidemic threshold at which the infection of the system persist for a extended period of time. Here, “fraction of infected nodes”, “contagion”, and “contagion or alerting rates” studies were performed. As for the framework testing, the article uses “simulated” networks only. The results show that the network adaptation model predicts that changing contacts may adversely lead to lower network robustness against epidemic spreading if the contact adaptation is not fast enough

90. **On the effectiveness of link addition for improving robustness of multiplex networks against layer node-based attack** - 2017 - Yui Kazawa, Sho Tsugawa [38]

    This article studies a methodology for effectively improving the robustness of multiplex networks against attacks is proposed. In particular, the effectiveness of existing link addition strategies for improving robustness. To do this a “one to one like” model consisting of a multiplex network is used. To measure the robustness, the framework uses a “counting elements” metric (size of the largest connected component). Here, “targeted attacks”, “fraction of added intra-links”, “link addition strategy”, and “size of the giant connected component” studies were performed. As for the framework testing, the article uses “simulated” networks only. The results show that strategic link addition can effectively improve the robustness of multiplex networks, and it is even more effective when a large number of nodes are attacked.

91. **Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids** - 2017 - Ye Cai, Yong Li, Yijia Cao, Wenguo Li, Xiangjun Zeng [6]

This article analyzes the impact of interdependencies and structure characteristics of communication networks on cascading failures in power grids. To do this a "coupled power grid" model where the power grid has loads and capacities and the inter-dependencies are probabilistic is used. In this model overloads happen over time, and thus, can be repaired. If a node is removed then its counterpart will get removed depending on the inter-link value. To assess the robustness a "probability" metric that measures the cummulative probability of the load shedding is used. Here, "coupling", and "load and capacity" studies were performed. The framework uses "real and simulated" networks for testing. Among the results it is shown that greater interdependency leads to a lower probability of a large blackout.

92. **Core Percolation in Coupled Networks** - 2017 - Jiayu Pan, Yuhang Yao, Luoyi Fu, Xinbing Wang [58]

    This article studies core percolation in coupled networks and proposes an algorithm to tackle the problem. In *core percolation* instead of randomly removing a fraction of the nodes, the leaves of the networks are removed until the core becomes stable. To do the study, the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "mean degree", "core percolation", and "percolation" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that the presence of a core leads to a first order transition in coupled networks.

93. **Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks** - 2017 - Diego F. Rueda, Eusebi Calle [71]

    This article studies the effect of targeted attack over the telecommunications network coupled with power grid using interdependency matrices. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses a "probability" metric. This metric is the Average Two-Terminal Reliability (ATTR) and it measures the probability of the connectivity between a randomly chosen node pair in a single network. Here, "targeted attacks", and "coupling" studies are performed. As for the framework testing, the article uses "simulated" networks only. The results show that the interdependency matrix used to couple the networks can determine the robustness of the system.

94. **Social contagions on interdependent lattice networks** - 2017 - Panpan Shu, Lei Gao;Pengcheng Zhao, Wei Wang, H. Eugene Stanley [77]

    In this article a non-Markovian contagion model on interdependent spatial networks composed of two identical two-dimensional lattices is presented. To do this a "geometric or spatially embedded" model is used. This model consists of spatially embedded networks (lattices) where nodes can become *adopted* (from adopting a social behaviour), and these adopted state can be propagated to their interdependent counterparts. To measure the robustness the article uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "cascading time", "percolation", "contagion", "initially infected nodes", and "size of second largest component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that as the fraction of dependency links is increased, the phase transition switches from second-order to first-order. It is also found that in strongly inter-connected interdependent spatial networks increasing

the fraction of initial adopted nodes can induce the switch from a first-order to second-order phase transition, associated with social contagion dynamics, and both the second-order and first-order phase transition points can be decreased by increasing the fraction of dependency links or the number of initially-adopted nodes.

95. **Enhancing robustness of interdependent network under recovery based on a two-layer-protection strategy** - 2017 - Maoguo Gong, Yixing Wang, Shanfeng Wang, Wenfeng Liu [27]

    This article proposes a two-layer-protection strategy to enhance the robustness of coupled networks under their reconstruction. To do this the original one to one model ("one to one like") is used. To assess the robustness a "counting elements", and a "path length" metric are used. The first metric observes the total amount of functional nodes for different amounts of recovered nodes. While the latter measures the average inverse geodesic length of each network given an amount p of recovered nodes. Here, "node protection strategy", "coupling", "length", and "recovery" studies were performed. The framework uses "real and simulated" networks for testing. The results show that the two-layer-protection strategy increases the robustness of coupled networks more efficiently than methods which only protect nodes in one layer.

96. **Cascading Failures in Interdependent Networks with Multiple Supply-Demand Links and Functionality Thresholds** - 2017 - M. A. Di Muro, L. D. Valdez, H. H. Aragao Rego, Sergey V. Buldyrev, H. Eugene Stanley, Lidia A. Braunstein [16]

    In this article an interdependent networks model for two networks where each node has its own supply threshold is developed. To do this a "multiple dependencies" model where each node is bidirectionally connected to 0 or more nodes in the other network. In this model each node has its own supply requirements that must be fulfilled for it to remain functional. To measure the robustness, the framework uses a "counting elements metric" (normalized amount of active nodes within network one of the networks after a cascading failure), and a "breaking point" metric (percolation threshold). Here, "components size", "percolation", and "k-core rule" studies are performed. As for the framework testing, the article uses "simulated" networks only. Among the results it is shown that the system is more robust when the supply threshold is lower.

97. **Reducing cascading failure risk by increasing infrastructure network interdependence** - 2017 - Mert Korkali, Jason G. Veneman;Brian F. Tivnan, James P. Bagrow, Paul D. H. Hines [40]

    This article compares the robustness of interdependent networks with simple topological network models to more realistic models. To do this a "coupled power grid" model consisting of the power grid coupled with its communication network is used. In this model loads and capacities are considered, and communication network nodes can have 3 modes: vulnerable (no backup), ideal (fully functional backup), and intermediate. Thus, the cascading process will depend on the modes of the communication network nodes. To assess the robustness a "probability" metric that measures the probability that more than half of the original N nodes remain within the giant component after a cascading failure. Here, "coupling", and "size of second largest component" studies were performed. The framework uses "real and simulated" networks for testing. The results show that robustness can be enhanced by interconnecting networks with complementary capabilities if modes of inter-network failure propagation are constrained.

98. **The interdependent network of gene regulation and metabolism is robust where it needs to be** - 2017 - David F. Klosik, Anne Grimbs, Stefan Bornholdt, Marc-Thorsten Huutt [39]

This article studies the interdependent network of gene regulation and metabolism for the model organism Escherichia coli in terms of a biologically motivated percolation model. To do this a "mixed interactions" model with three layers is used. This model defines three types of links (conjuct, disjunct, and regulation) that determine the interactions between nodes. To measure the robustness, the framework uses a "counting elements" metric that measure the susceptibility using the size of the largest cluster, and a "breaking point" metric that measures the percolation threshold of the system. Here, "localized attacks", and "percolation" studies were performed. The framework uses "real and simulated" networks for testing. The results show that the interdependent system is sensitive to gene regulatory and protein-level perturbations, yet robust against metabolic changes.

99. **Overload-based cascades on multiplex networks and effects of inter-similarity** - 2017 - Dong Zhou, Ahmed Elmokashfi [100]

    In this article a model for load-based cascading failures in multiplex networks is proposed. To do this a "one to one like" model consisting of a multiplex network with loads is used. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "system intersimilarity", "coupling", "load and capacity", and "size of the giant connected component" studies were performed. The framework uses "real and simulated" networks for testing. The results suggest that inter-similarity can have a negative impact on the robustness against overload cascades.

100. **Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks** - 2017 - Adam Tyra, Jingtao Li, Yilun Shang, Shuo Jiang, Yanjun Zhao, Shouhuai Xu [82]

    This article characterizes the robustness of complex networks, including interdependent networks, against dependent and adaptive attacks. To do this the original one to one model ("one to one like") is used. To measure the robustness, the framework uses two "counting elements" metrics (size of the largest connected component, mean size of small components). Here, "targeted attacks", "localized attacks", "coupling", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. Among the results it is shown that powerful attack strategies (e.g., targeted attacks and dependent attacks, dependent attacks and adaptive attacks) are not compatible and do not cause more damage when used collectively.

101. **Emergence of robustness in networks of networks** - 2017 - Kevin Roth, Flaviano Morone, Byungjoon Min, Hernán A. Makse [69]

    In this article an approach to model the brain as interdependent networks is presented. To do this a "multiple dependencies" model is used. In this model in order for a node to remain functional it must have at least one functional support node, and have an *active* status. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component), and a "breaking point" metric (percolation threshold). Here, "coupling", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that the in model proposed the dependencies do not lead to cascading failures as this model does not require nodes to be connected to the largest connected component to remain functional.

102. **Generalized model for k-core percolation and interdependent networks** - 2017 - Nagendra K. Panduranga, Jianxi Gao, Xin Yuan, H. Eugene Stanley, Shlomo Havlin [59]

    In this article interdependent networks are studied using a k-core percolation. To do this a "one to one like" model is used. In this model each node can be bidirectionally connected to at most one other node. To measure the robustness, the framework uses a "counting elements" metric (size of the largest connected component). Here, "interdependent k-core percolation", "average local threshold", "coupling", "percolation", and "size of the giant connected component" studies were performed. As for the framework testing, the article uses "simulated" networks only. The results show that the phase diagram for interdependent networks studied using k-core percolation is very rich, having regions of second and first order phase transitions.

103. **Enhancing the robustness of interdependent cyber-physical systems by designing the interdependency relationship** - 2017 - Yangming Zhao, Chunming Qiao [97]

    This article studies how to optimize the interdependencies among the components in interdependent Cyber-Physical Systems, in order to enhance the system robustness. To do this a "multiple dependencies" model where support-dependence links allow nodes to give and receive resources or capability from other nodes is used. Here, there are different types of resources and each node needs and give a certain amount of each type of resource. In this model a node remains functional if it belongs to the giant component and if it receives the required amount of capability from the resource types needed. To measure the robustness, the framework uses a "counting elements" metric that measures the group of components that may fail due to the cascading failure incurred by the same component (Shared Failure Group). In this work, "system size", "redundant ratio", and "resources provided per node" studies were performed. The framework uses "real and simulated" networks for testing. The results show that if 1.3 times of the resources required by all the components are provided, the cascading failure incurred by a single component failure can be eliminated.

A.3 *Summary tables*

In this section we present summary tables of the contents presented in this survey. These tables outline the taxonomy presented and the papers surveyed. On table A.2 we present a summary of each aspect identified during the survey, showing the classifications of each aspect, and the papers that belong to each classification. On table A.3 we present all the studies that were not discussed on section 3.3 along with the papers that belong to each study classification. Finally on tables A.4, A.5, A.6, A.7, A.8, A.9, and A.10 we show a summary of each paper and the classifications it belongs to.

Table A.2. Main aspects of frameworks studied

Aspect	Summary
Interdependent network models	Eleven classifications: "One to one like" [5, 7, 8, 11, 12, 15, 18, 22, 23, 25, 26, 28, 31, 32, 35, 43, 48, 49, 64, 65, 67, 70, 74, 75, 78–80, 83–85, 89, 91, 92, 95, 99, 101, 102], "Geometric or spatially embedded" [1, 3, 4, 14, 41, 43, 44, 46, 52, 76, 88] "multiple dependencies" [8, 19, 36, 45, 55, 62, 63, 68], "coupled power grid" [29, 33, 34, 53, 56, 57, 60], "load transfer among networks" [30, 87, 90, 93, 98, 103], "mixed interactions" [17, 20, 42, 50, 96], "mapping" [2, 94],"directed support-dependencies" [24, 61], "supply chain"[81], "contagion" [54], and "defined by probabilities"[66].
Robustness measure	Eight classifications: "counting elements" [1, 3, 7, 8, 11, 12, 15, 17, 18, 20, 22–26, 28–36, 41–45, 48–50, 53, 55, 56, 61, 68, 74–76, 78, 80, 81, 83–85, 87–91, 93–96, 99, 101–103], "breaking point" [4, 5, 12, 14, 17–20, 23–25, 30–32, 34, 36, 41, 44, 46, 49, 52, 60, 61, 64, 65, 67, 68, 75, 76, 78, 84, 89, 91–93, 101, 102], "time" [2, 3, 12, 14, 15, 18, 19, 31, 43, 76, 94, 99, 101, 102], "probability" [5, 28, 43, 52, 54, 64, 66, 70], "ratio" [1, 88, 99], "cost" [62, 63, 94], "path length" [7, 79, 98], and "Performance"[57].
Studies performed	Eight main categories: "size of the giant connected component" [3, 5, 7, 8, 11, 12, 15, 17, 20, 22, 23, 25, 28, 30, 31, 33–36, 42, 45, 46, 49, 50, 52, 55, 56, 61, 68, 74, 75, 78–81, 85, 88, 89, 91–93, 95, 96, 99, 101–103], "coupling" [3, 11, 14, 17–20, 24–26, 28–30, 35, 36, 42, 44, 45, 49, 50, 53, 56, 61, 63, 67, 68, 70, 74–76, 79, 80, 83–85, 90, 93, 95, 101, 103], "percolation" [3–5, 12, 14, 15, 17–20, 23, 24, 26, 28, 31–34, 36, 41–44, 49, 50, 52, 61, 64, 68, 74–76, 78, 89, 91, 99, 101–103], "targeted attacks" [7, 8, 11, 12, 18, 20, 29, 30, 32, 33, 55, 70, 79, 80, 84, 85, 89, 90, 93, 95, 96, 98], "Load and capacity" [2, 11, 30, 34, 48, 62, 63, 80, 81, 84, 87, 90, 93, 95, 98], "cascading time" [3, 12, 14, 18, 19, 23, 42, 76, 99, 102], "length" [7, 41, 44, 52, 76, 79, 88, 98], and "avalanche" [11, 29, 43, 47, 48, 51, 83, 84].
Networks used to test the framework	Two classifications: "simulated" [1, 4, 5, 8, 11, 12, 14, 15, 17–20, 23–25, 28–32, 34–36, 41–44, 46, 48–50, 52–54, 61–63, 65, 66, 70, 75, 76, 78–81, 84, 85, 89–94, 96, 99, 101, 102], and "real and simulated" [2, 3, 7, 22, 26, 33, 45, 55–57, 60, 64, 67, 68, 74, 83, 87, 88, 95, 98, 103].

Table A.3: Other studies performed

Classification	Description	Papers
"Localized attacks"	Studies the effect over the system's robustness of an attack that affects an area typically centered on a node.	[1, 4, 21, 25, 39, 82, 91]
"Optimization"	Studies ways to optimize the system's robustness.	[2, 45, 55, 60, 62, 63, 94]
"Cost"	Studies the costs of improving the networks robustness.	[2, 9, 45, 48, 62, 63, 94]
"Recovery"	Studies the robustness of a recovery process on the interdependent networks system.	[15, 22, 26, 27, 57]
"Size of second largest component"	Studies the size of the second largest connected component.	[40, 52, 77]
"Fraction of added intra-links"	Studies the effect of adding new links within a network, over the system's robustness	[35, 38, 86]
"Laplacian"	Studies of the system's robustness based on the Laplacian matrix of the neworks.	[65, 67]
"Small cluster"	Studies the size or amount of operating clusters of interdependent networks. A small operating cluster is a subgraph that has everything to be functional (for example the necessary interlinks) but is not connected to the largest connected component in its original network.	[28, 33]
"Single network contrast"	Studies the differences between the interdependent network system and a single network version of it.	[47, 83]
"Contagion"	Studies the effect over the robustness of the interdependent system of different contagion behaviours.	[73, 77]
"Efficient paths"	Studies the length variations of shortest paths in a network under different conditions.	[41, 98]
"Core percolation"	Studies the percolation of the system when leaves are removed (instead of removing random nodes) in the participant networks, removing dependent nodes when necessary, until it stabilizes.	[58, 59]
"Genetic algorithm"	Studies the result of creating interdependent networks using genetic algorithms.	[1, 57]

"Lifetime"	Studies the lifetime of an interdependent network system under different conditions.	[46, 92]
"Layer configuration"	Studies about the effect over the system robustness of different layer configurations.	[18, 76]
"Interdependent k-core percolation"	Studies the k-core percolation process. Here, the process is initiated by removing a fraction (1 - p_0) of randomly chosen nodes from both networks. In k-core percolation, nodes in each network with fewer than k neighbors are pruned (the local threshold of each node may differ), along with all the nodes in the second network that are dependent on them. This cascade process is continued in both networks until a steady state is reached.	[59]
"Clustering coefficient"	Studies the changes of the clustering coefficient under different scenarios.	[75]
"Balance coefficient"	Studies the effects different balance coefficients over the system's robustness.	[51]
"Delay"	Studies the delay of services offered by the interdependent network system.	[94]
"Information to attack"	Studies the effect over the system's robustness of different parameters related to amount of information that an attacker can have to attack a system.	[103]
"Evenness"	Studies the effect of the evenness on the robustness of the system. The evenness describes the connectivity among network layers.	[54]
"Antagonistic nodes"	Studies the effect of the amount of antagonistic nodes in the robustness of the system. Antagonistic nodes are nodes with a negative effect on their interdependent nodes.	[42]
"Intra-network topology"	Studies the effect over the system's robustness of changing the topology of the interconnected networks.	[72]
"Link addition strategy"	Studies the effect on the robustness of the system of adding links given a specific link addition strategy within a network.	[38]

"Contagion or alerting rates"	Studies the effect of changing the alerting or contagion rates over the robustness of the system.	[73]
"Redundancy degree"	Studies the effect of changing the redundancy degree over the robustness of the system. The redundancy degree represents the ratio of the total support capability of all nodes to the total required capability of all nodes.	[13]
"Node degree correlation"	Studies the effect the degree correlation over the robustness of the system.	[89]
"Localized attack stability"	Studies the stability of a system under localized attacks. Spatially embedded networks can be stable if they tolerate a radius targeted attack of any radius, meta stable if they are stable under attack of at most a r_c critical radius (a bigger radius makes the system collapse), and unstable if any attack radius destroys the network.	[4]
"Lattice dimension"	Studies the effect of lattice dimensions on the robustness of the system. Here, one or more networks of the interdependent system are lattices.	[52]
"System size"	Studies the effect of the size of the system over the robustness.	[97]
"Resources provided per node"	Given that each node provide resources that can be used by other nodes, studies the effects of changing the amount of resources provided per node over the system robustness.	[97]
"Node protection strategy"	Studies the effect over the system robustness of using different node protection strategies against attacks or failures.	[27]
"Probability of stabilization"	Studies the probability of transiting from a state with some number of failures in a "cascading failure state" to a "stable state" with the same amount of failures.	[66]
"Markov-chains"	Studies networks whose behaviour is defined through Markov-chains.	[66]
"Probability of failure"	Studies the effect of the probability of failure of the components.	[96]

"Fraction of infected nodes"	Studies the fraction of infected nodes given the initial conditions. Here, different initial conditions are tested.	[73]
"Assortativity"	Studies if the degree distribution of a network is assortative or disassortative, and the effect of different distributions over the system's robustness.	[102]
"Average local threshold"	Studies the effect over the system's robustness of different average local thresholds. The average local threshold is the average amount of neighbours that a k-core needs to survive k-core percolation.	[59]
"Transmissibility"	Studies the effect of the transmissibility on the robustness of the system. The transmissibility is the probability of a node of being exposed by each of its infected neighbor instances in the a layer.	[54]
"Redundant ratio"	Studies the effect of the 'redundant ratio' on the robustness of the system. The redundant ratio is defined as the ratio of offered services versus needed services of a node.	[97]
"Difference index"	Studies the effect of the difference index on the robustness of the network. The difference index is defined as the normalization of the reciprocal of average number of layers involved in each overlaid edge λ, where the difference describes how network layers share the same overlaid edges, $\lambda \to 1$ indicates that few layers appear in an overlaid edge, whereas $\lambda \to 0$ indicates that many layers have the same overlaid edges.	[54]
"System intersimilarity"	Studies the effect over the robustness of link overlapping on multiplex or one-to-one networks.	[100]
"Failure distribution"	Studies the probability distribution of failures on edges and/or nodes.	[48]
"Initially infected nodes"	Studies the effect over the system robustness of different fractions of initially infected nodes.	[77]
"Amount of components"	Studies the amount or number of components under different adverse scenarios.	[7]
"Failure size PMF"	Studies the probability mass function (PMF) behaviour under different adverse conditions.	[66]

"Components size"	Studies the effect over the system's robustness of the size of the components. Here a finite component of size h survives with probability $1-q(h)$.	[16]
"Mean degree"	Studies the effect over the robustness of the mean degree average.	[58]
"K-core rule"	Studies the effect over the robustness of the amount of neighbors needed for a node i to survive. Here, a node i survives if it has at least k_i active neighbors.	[16]

Table A.4. Summary table I

Papers		[5]	[61]	[94]	[67]	[32]	[102]	[44]	[23]	[65]	[55]	[14]	[63]	[24]	[31]	[101]
Models	One to one like	✓			✓	✓	✓		✓	✓					✓	✓
	Geometric or spatially embedded							✓				✓				
	Multiple dependencies										✓		✓			
	Coupled power grid															
	Load transfer among networks															
	Mixed interactions															
	Directed support-dependency		✓											✓		
	Mapping			✓												
	Contagion or influence															
	Supply-chain															
	Defined by probabilities															
Metrics	Counting elements		✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
	Breaking point	✓	✓		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓
	Time			✓			✓					✓			✓	✓
	Probability	✓														
	Rate															
	Cost			✓									✓			
	Path length															
	Performance															
Studies	Size of the giant connected component	✓	✓				✓		✓		✓				✓	✓
	Coupling		✓		✓			✓				✓	✓	✓		✓
	Percolation	✓	✓			✓	✓	✓	✓			✓		✓	✓	✓
	Targeted attacks					✓					✓					
	Load and capacity												✓			
	Cascading time						✓		✓			✓				
	Length							✓				✓				
	Cost			✓									✓			
	Optimization			✓							✓		✓			
	Laplacian				✓					✓						
	Delay			✓												
	Assortativity						✓									
Networks	Simulated	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
	Real and simulated				✓						✓					

Table A.5. Summary table II

Papers		[60]	[18]	[62]	[3]	[74]	[19]	[68]	[56]	[53]	[75]	[1]	[36]	[83]	[78]	[41]
Models	One to one like		✓			✓					✓			✓	✓	
	Geometric or spatially embedded				✓							✓				✓
	Multiple dependencies			✓			✓	✓					✓			
	Coupled power grid	✓							✓	✓						
	Load transfer among networks															
	Mixed interactions															
	Directed support-dependency															
	Mapping															
	Contagion or influence															
	Supply-chain															
	Defined by probabilities															
Metrics	Counting elements		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
	Breaking point	✓	✓				✓	✓			✓		✓		✓	✓
	Time		✓		✓		✓									
	Probability															
	Rate											✓				
	Cost			✓												
	Path length															
	Performance															
Studies	Size of the giant connected component				✓	✓		✓	✓		✓		✓		✓	
	Coupling		✓		✓	✓	✓	✓	✓	✓	✓		✓	✓		
	Percolation		✓		✓	✓	✓	✓			✓		✓		✓	✓
	Targeted attacks		✓													
	Load and capacity			✓												
	Cascading time		✓		✓		✓									
	Length															✓
	Cost			✓												
	Avalanche													✓		
	Localized attacks											✓				
	Optimization	✓		✓												
	Single network contrast													✓		
	Efficient paths															✓
	Genetic algorithm											✓				
	Clustering coefficient										✓					
	Layer configuration		✓													
Networks	Simulated		✓	✓			✓			✓	✓	✓	✓		✓	✓
	Real and simulated	✓			✓	✓		✓	✓					✓		

Table A.6. Summary table III

Papers		[99]	[76]	[54]	[89]	[12]	[98]	[34]	[84]	[93]	[26]	[4]	[64]	[45]	[80]	[33]
Models	One to one like	✓			✓	✓			✓		✓		✓		✓	
	Geometric or spatially embedded		✓									✓				
	Multiple dependencies													✓		
	Coupled power grid							✓								✓
	Load transfer among networks						✓			✓						
	Mixed interactions															
	Directed support-dependency															
	Mapping															
	Contagion or influence			✓												
	Supply-chain															
	Defined by probabilities															
Metrics	Counting elements	✓	✓		✓	✓		✓	✓	✓	✓			✓	✓	✓
	Breaking point		✓		✓	✓		✓	✓	✓		✓	✓			
	Time	✓	✓			✓										
	Probability			✓									✓			
	Rate	✓														
	Cost															
	Path length						✓									
	Performance															
Studies	Size of the giant connected component	✓			✓	✓		✓		✓				✓	✓	✓
	Coupling		✓						✓	✓	✓			✓	✓	
	Percolation	✓	✓		✓	✓		✓			✓	✓	✓			✓
	Targeted attacks				✓	✓	✓		✓	✓					✓	✓
	Load and capacity						✓	✓	✓	✓					✓	
	Cascading time	✓	✓			✓										
	Length		✓									✓				
	Cost													✓		
	Avalanche								✓							
	Localized attacks											✓				
	Optimization													✓		
	Recovery										✓					
	Small cluster															✓
	Efficient paths						✓									
	Evenness			✓												
	Node degree correlation				✓											
	Localized attack stability											✓				
	Layer configuration		✓													
	Transmissibility			✓												
	Difference index			✓												
Networks	Simulated	✓	✓	✓	✓	✓		✓	✓	✓		✓			✓	
	Real and simulated						✓				✓		✓	✓		✓

Table A.7. Summary table IV

Papers		[17]	[30]	[8]	[11]	[57]	[42]	[28]	[91]	[35]	[81]	[66]	[2]	[7]	[70]	[25]
Models	One to one like			✓	✓			✓	✓	✓				✓	✓	✓
	Geometric or spatially embedded															
	Multiple dependencies			✓												
	Coupled power grid					✓										
	Load transfer among networks		✓													
	Mixed interactions	✓					✓									
	Directed support-dependency															
	Mapping												✓			
	Contagion or influence															
	Supply-chain										✓					
	Defined by probabilities											✓				
Metrics	Counting elements	✓	✓	✓	✓		✓	✓	✓	✓	✓			✓		✓
	Breaking point	✓	✓						✓							✓
	Time												✓			
	Probability							✓				✓			✓	
	Rate															
	Cost															
	Path length													✓		
	Performance					✓										
Studies	Size of the giant connected component	✓	✓	✓	✓		✓	✓	✓	✓	✓			✓		✓
	Coupling	✓	✓		✓		✓	✓		✓					✓	✓
	Percolation	✓					✓	✓	✓							
	Targeted attacks		✓	✓	✓									✓	✓	
	Load and capacity		✓		✓						✓		✓			
	Cascading time						✓									
	Cost												✓			
	Avalanche				✓											
	Localized attacks								✓							✓
	Optimization												✓			
	Recovery					✓										
	Fraction of added intra-links									✓						
	Small cluster							✓								
	Markov-chains											✓				
	Genetic algorithm					✓										
	Antagonistic nodes						✓									
	Probability of stabilization											✓				
	Amount of components													✓		
	Failure size PMF											✓				
Networks	Simulated	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓			✓	✓
	Real and simulated					✓							✓	✓		

Table A.8. Summary table V

Papers		[29]	[87]	[48]	[22]	[15]	[96]	[50]	[79]	[49]	[95]	[103]	[46]	[85]	[20]	[90]
Models	One to one like			✓	✓	✓			✓	✓	✓			✓		
	Geometric or spatially embedded												✓			
	Multiple dependencies															
	Coupled power grid	✓														
	Load transfer among networks		✓									✓				✓
	Mixed interactions						✓	✓							✓	
	Directed support-dependency															
	Mapping															
	Contagion or influence															
	Supply-chain															
	Defined by probabilities															
Metrics	Counting elements	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓
	Breaking point									✓			✓		✓	
	Time					✓										
	Probability															
	Rate															
	Cost															
	Path length								✓							
	Performance															
Studies	Size of the giant connected component				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Coupling	✓						✓	✓	✓	✓	✓		✓	✓	✓
	Percolation					✓		✓		✓		✓			✓	
	Targeted attacks	✓					✓		✓		✓			✓	✓	✓
	Load and capacity		✓	✓							✓					✓
	Length												✓			
	Cost			✓												
	Avalanche	✓		✓												
	Recovery				✓	✓										
	Lifetime												✓			
	Information to attack											✓				
	Probability of failure						✓									
	Failure distribution			✓												
Networks	Simulated	✓		✓		✓	✓	✓	✓	✓			✓	✓	✓	✓
	Real and simulated		✓		✓						✓	✓				

Table A.9. Summary table VI

Papers		[43]	[88]	[52]	[37]	[71]	[77]	[27]	[16]	[40]	[39]	[100]	[82]	[69]	[59]	[58]
Models	One to one like	✓			✓	✓		✓				✓	✓		✓	✓
	Geometric or spatially embedded	✓	✓	✓			✓									
	Multiple dependencies								✓					✓		
	Coupled power grid									✓						
	Load transfer among networks															
	Mixed interactions										✓					
	Directed support-dependency															
	Mapping															
	Contagion or influence															
	Supply-chain															
	Defined by probabilities															
Metrics	Counting elements	✓	✓				✓	✓	✓		✓	✓	✓	✓	✓	✓
	Breaking point			✓			✓		✓		✓			✓		
	Time	✓														
	Probability	✓		✓	✓	✓				✓						
	Rate		✓													
	Cost															
	Path length							✓								
	Performance															
Studies	Size of the giant connected component		✓	✓	✓							✓	✓	✓	✓	
	Coupling				✓	✓	✓	✓		✓		✓	✓	✓	✓	
	Percolation	✓		✓			✓		✓		✓			✓	✓	✓
	Targeted attacks					✓							✓			
	Load and capacity											✓				
	Cascading time						✓									
	Length		✓	✓				✓								
	Avalanche	✓														
	Localized attacks										✓		✓			
	Recovery							✓								
	Contagion						✓									
	Size of second largest component			✓			✓			✓						
	Core percolation															✓
	Interdependent k-core percolation														✓	
	Lattice dimension			✓												
	Node protection strategy							✓								
	Average local threshold														✓	
	System intersimilarity											✓				
	Initially infected nodes						✓									
	Components size								✓							
	Mean degree															✓
	K-core rule								✓							
Networks	Simulated	✓		✓	✓	✓	✓		✓				✓	✓	✓	✓
	Real and simulated		✓					✓		✓	✓	✓				

Table A.10. Summary table VII

Papers		[6]	[13]	[86]	[47]	[10]	[9]	[21]	[51]	[72]	[73]	[38]	[97]
Models	One to one like			✓		✓	✓			✓		✓	
	Geometric or spatially embedded												
	Multiple dependencies		✓			✓		✓	✓				✓
	Coupled power grid	✓											
	Load transfer among networks												
	Mixed interactions												
	Directed support-dependency												
	Mapping												
	Contagion or influence										✓		
	Supply-chain												
	Defined by probabilities				✓								
Metrics	Counting elements		✓	✓	✓	✓	✓	✓	✓			✓	✓
	Breaking point		✓					✓			✓		
	Time												
	Probability	✓								✓			
	Rate												
	Cost												
	Path length												
	Performance												
Studies	Size of the giant connected component		✓	✓		✓	✓	✓				✓	
	Coupling	✓	✓	✓		✓	✓	✓					
	Percolation		✓					✓					
	Targeted attacks					✓				✓		✓	
	Load and capacity	✓											
	Cascading time				✓								
	Cost						✓						
	Avalanche				✓				✓				
	Localized attacks							✓					
	Contagion										✓		
	Fraction of added intra-links			✓								✓	
	Single network contrast				✓								
	Balance coefficient								✓				
	Intra-network topology									✓			
	Link addition strategy											✓	
	Contagion or alerting rates										✓		
	Redundancy degree		✓										
	System size												✓
	Resources provided per node												✓
	Fraction of infected nodes										✓		
	Redundant ratio												✓
Networks	Simulated		✓	✓	✓	✓	✓	✓	✓		✓	✓	
	Real and simulated	✓								✓			✓

References

[1] ADLER, C. O. & DAGLI, C. H. (2014) Study of the Use of a Genetic Algorithm to Improve Networked System-of-Systems Resilience. *Procedia Computer Science*, **36**, 49–56.

[2] ALASHAIKH, A., TIPPER, D. & GOMES, T. (2016) Supporting differentiated resilience classes in multilayer networks. in *2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 31–38. IEEE.

[3] BASHAN, A., BEREZIN, Y., BULDYREV, S. V. & HAVLIN, S. (2013) The extreme vulnerability of interdependent spatially embedded networks. *Nature Physics*, **9**(10), 667–672.

[4] BEREZIN, Y., BASHAN, A., DANZIGER, M. M., LI, D. & HAVLIN, S. (2015) Localized attacks on spatially embedded networks with dependencies. *Scientific reports*, **5**.

[5] BULDYREV, S. V., PARSHANI, R., PAUL, G., STANLEY, H. E. & HAVLIN, S. (2010) Catastrophic cascade of failures in interdependent networks. *Nature*, **464**(7291), 1025–1028.

[6] CAI, Y., LI, Y., CAO, Y., LI, W. & ZENG, X. (2017) Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids. *International Journal of Electrical Power & Energy Systems*, **89**, 106–114.

[7] CHAI, W. K., KYRITSIS, V., KATSAROS, K. & PAVLOU, G. (2016) Resilience of interdependent communication and power distribution networks against cascading failures. *15th IFIP Networking, Vienna, Austria*.

[8] CHATTOPADHYAY, S. & DAI, H. (2015) Towards Optimal Link Patterns for Robustness of Interdependent Networks against Cascading Failures. in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6. IEEE.

[9] ——— (2017) Designing optimal interlink structures for interdependent networks under budget constraints. *Technical Report, Dept. of ECE, NCSU*.

[10] CHATTOPADHYAY, S., DAI, H., HOSSEINALIPOUR, S. ET AL. (2017) Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures. *IEEE Transactions on Communications*, **65**(9), 3847–3862.

[11] CHEN, Z., DU, W.-B., CAO, X.-B. & ZHOU, X.-L. (2015) Cascading failure of interdependent networks with different coupling preference under targeted attack. *Chaos, Solitons & Fractals*, **80**, 7–12.

[12] CHENG, Z. & CAO, J. (2015) Cascade of failures in interdependent networks coupled by different type networks. *Physica A: Statistical Mechanics and its Applications*, **430**, 193–200.

[13] CUI, P., ZHU, P., SHAO, C. & XUN, P. (2017) Cascading failures in interdependent networks due to insufficient received support capability. *Physica A: Statistical Mechanics and its Applications*, **469**, 777–788.

[14] DANZIGER, M. M., BASHAN, A., BEREZIN, Y. & HAVLIN, S. (2013) Interdependent spatially embedded networks: dynamics at percolation threshold. in *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on*, pp. 619–625. IEEE.

[15] DI MURO, M., LA ROCCA, C., STANLEY, H., HAVLIN, S. & BRAUNSTEIN, L. (2016) Recovery of Interdependent Networks. *Scientific reports*, **6**.

[16] DI MURO, M., VALDEZ, L., RÊGO, H. A., BULDYREV, S., STANLEY, H. & BRAUNSTEIN, L. (2017) Cascading Failures in Interdependent Networks with Multiple Supply-Demand Links and Functionality Thresholds. *Scientific reports*, **7**(1), 15059.

[17] DONG, G., DU, R., TIAN, L. & LIU, R. (2015) Robustness of network of networks with interdependent and interconnected links. *Physica A: Statistical Mechanics and its Applications*, **424**, 11–18.

[18] DONG, G., GAO, J., DU, R., TIAN, L., STANLEY, H. E. & HAVLIN, S. (2013) Robustness of network of networks under targeted attack. *Physical Review E*, **87**(5), 052804.

[19] DONG, G., TIAN, L., DU, R., FU, M. & STANLEY, H. E. (2014) Analysis of percolation behaviors of clustered networks with partial support–dependence relations. *Physica A: Statistical Mechanics and its Applications*, **394**, 370–378.

[20] DU, R., DONG, G., TIAN, L. & LIU, R. (2016) Targeted attack on networks coupled by connectivity and dependency links. *Physica A: Statistical Mechanics and its Applications*, **450**, 687–699.

[21] FAN, W., GAOGAO, D., RUIJIN, D. & LIXIN, T. (2017) Robustness of multiple interdependent networks under shell attack. in *Control Conference (CCC), 2017 36th Chinese*, pp. 1447–1450. IEEE.

[22] GANIN, A. A., MASSARO, E., GUTFRAIND, A., STEEN, N., KEISLER, J. M., KOTT, A., MANGOUBI, R. & LINKOV, I. (2016) Operational resilience: concepts, design and analysis. *Scientific reports*, **6**.

[23] GAO, J., BULDYREV, S. V., HAVLIN, S. & STANLEY, H. E. (2012) Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes. *Physical Review E*, **85**(6), 066134.

[24] GAO, J., BULDYREV, S. V., STANLEY, H. E., XU, X. & HAVLIN, S. (2013) Percolation of a general network of networks. *Physical Review E*, **88**(6), 062816.

[25] GAOGAO, D., RUIJIN, D., HUIFANG, H. & LIXIN, T. (2016) Shell attack on interdependent networks. in *Control Conference (CCC), 2016 35th Chinese*, pp. 1198–1201. TCCT.

[26] GONG, M., MA, L., CAI, Q. & JIAO, L. (2015) Enhancing robustness of coupled networks under targeted recoveries. *Scientific reports*, **5**.

[27] GONG, M., WANG, Y., WANG, S. & LIU, W. (2017) Enhancing robustness of interdependent network under recovery based on a two-layer-protection strategy. *Scientific reports*, **7**(1), 12753.

[28] GRASSBERGER, P. (2015) Percolation transitions in the survival of interdependent agents on multiplex networks, catastrophic cascades, and solid-on-solid surface growth. *Physical Review E*, **91**(6), 062806.

[29] HAN, Y., LI, Z., GUO, C. & TANG, Y. (2016) Improved percolation theory incorporating power flow analysis to model cascading failures in Cyber-Physical Power System. in *Power and Energy Society General Meeting (PESGM), 2016*, pp. 1–5. IEEE.

[30] HONG, S., WANG, B. & WANG, J. (2015) Cascading failure propagation in interconnected networks with tunable load redistribution strategy. in *Prognostics and System Health Management Conference (PHM), 2015*, pp. 1–7. IEEE.

[31] HU, Y., ZHOU, D., ZHANG, R., HAN, Z., ROZENBLAT, C. & HAVLIN, S. (2013) Percolation of interdependent networks with intersimilarity. *Physical Review E*, **88**(5), 052805.

[32] HUANG, X., GAO, J., BULDYREV, S. V., HAVLIN, S. & STANLEY, H. E. (2011) Robustness of interdependent networks under targeted attack. *Physical Review E*, **83**(6), 065101.

[33] HUANG, Z., WANG, C., NAYAK, A. & STOJMENOVIC, I. (2015) Small cluster in cyber physical systems: Network topology, interdependence and cascading failures. *Parallel and Distributed Systems, IEEE Transactions on*, **26**(8), 2340–2351.

[34] HUANG, Z., WANG, C., ZHU, T. & NAYAK, A. (2015) Cascading Failures in Smart Grid: Joint Effect of Load Propagation and Interdependence. *Access, IEEE*, **3**, 2520–2530.

[35] JI, X., WANG, B., LIU, D., CHEN, G., TANG, F., WEI, D. & TU, L. (2016) Improving interdependent networks robustness by adding connectivity links. *Physica A: Statistical Mechanics and its Applications*, **444**, 9–19.

[36] JIANG, J., LI, W. & CAI, X. (2014) The effect of interdependence on the percolation of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, **410**, 573–581.

[37] JUAN, W. X., ZE, G. S., LEI, J. & ZHEN, W. (2017) Percolation-cascading in multilayer heterogeneous network with different coupling preference. *Physica A: Statistical Mechanics and its Applications*, **471**, 233–243.

[38] KAZAWA, Y. & TSUGAWA, S. (2017) On the effectiveness of link addition for improving robustness of multiplex networks against layer node-based attack. in *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*, vol. 1, pp. 697–700. IEEE.

[39] KLOSIK, D. F., GRIMBS, A., BORNHOLDT, S. & HÜTT, M.-T. (2017) The interdependent network of gene regulation and metabolism is robust where it needs to be. *Nature communications*, **8**(1), 534.

[40] KORKALI, M., VENEMAN, J. G., TIVNAN, B. F., BAGROW, J. P. & HINES, P. D. (2017) Reducing cascading failure risk by increasing infrastructure network interdependence. *Scientific reports*, **7**, 44499.

[41] KORNBLUTH, Y., LOWINGER, S., CWILICH, G. & BULDYREV, S. V. (2014) Cascading failures in networks with proximate dependent nodes. *Physical Review E*, **89**(3), 032808.

[42] KOTNIS, B. & KURI, J. (2015) Percolation on networks with antagonistic and dependent interactions. *Physical Review E*, **91**(3), 032805.

[43] LEE, D., CHOI, S., STIPPINGER, M., KERTÉSZ, J. & KAHNG, B. (2016) Hybrid phase transition into an absorbing state: Percolation and avalanches. *Physical Review E*, **93**(4), 042109.

[44] LI, W., BASHAN, A., BULDYREV, S. V., STANLEY, H. E. & HAVLIN, S. (2012) Cascading failures in interdependent lattice networks: The critical role of the length of dependency links. *Physical review letters*, **108**(22), 228702.

[45] LI, X., WU, H., SCOGLIO, C. & GRUENBACHER, D. (2015) Robust allocation of weighted dependency links in cyber–physical networks. *Physica A: Statistical Mechanics and its Applications*, **433**, 316–327.

[46] LIMIAO, Z., DAQING, L., PENGJU, Q., BOWEN, F., YINAN, J., ZIO, E. & RUI, K. (2016) Reliability analysis of interdependent lattices. *Physica A: Statistical Mechanics and its Applications*, **452**, 120–125.

[47] LIU, D., ZHANG, X. & CHI, K. T. (2017) A stochastic model for cascading failures in smart grid under cyber attack. in *Future Energy Electronics Conference and ECCE Asia (IFEEC 2017-ECCE Asia), 2017 IEEE 3rd International*, pp. 783–788. IEEE.

[48] LIU, L., YIN, Y., ZHANG, Z. & MALAIYA, Y. K. (2016) Redundant Design in Interdependent Networks. *PloS one*, **11**(10), e0164777.

[49] LIU, R.-R., LI, M. & JIA, C.-X. (2016) Cascading failures in coupled networks: The critical role of node-coupling strength across networks. *Scientific Reports*, **6**.

[50] LIU, R.-R., LI, M., JIA, C.-X. & WANG, B.-H. (2016) Cascading failures in coupled networks with both inner-dependency and inter-dependency links. *Scientific reports*, **6**.

[51] LIU, Z., LI, Q., WANG, D. & XU, M. (2017) Balancing interdependent networks: Theory and algorithm. in *Performance Computing and Communications Conference (IPCCC), 2017 IEEE 36th International*, pp. 1–2. IEEE.

[52] LOWINGER, S., CWILICH, G. A. & BULDYREV, S. V. (2016) Interdependent lattice networks in high dimensions. *Physical Review E*, **94**(5), 052306.

[53] MATSUI, Y., KOJIMA, H. & TSUCHIYA, T. (2014) Modeling the Interaction of Power Line and SCADA Networks. in *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*, pp. 261–262. IEEE.

[54] MIN, Y., HU, J., WANG, W., GE, Y., CHANG, J. & JIN, X. (2014) Diversity of multilayer networks and its impact on collaborating epidemics. *Physical Review E*, **90**(6), 062803.

[55] NGUYEN, D. T., SHEN, Y. & THAI, M. T. (2013) Detecting critical nodes in interdependent power networks for vulnerability assessment. *Smart Grid, IEEE Transactions on*, **4**(1), 151–159.

[56] OUBOTER, T., WORM, D., KOOIJ, R. & WANG, H. (2014) Design of robust dependent networks against flow-based cascading failures. in *Reliable Networks Design and Modeling (RNDM), 2014 6th International Workshop on*, pp. 54–60. IEEE.

[57] OUYANG, M. & WANG, Z. (2015) Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety*, **141**, 74–82.

[58] PAN, J., YAO, Y., FU, L. & WANG, X. (2017) Core Percolation in Coupled Networks. in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, p. 28. ACM.

[59] PANDURANGA, N. K., GAO, J., YUAN, X., STANLEY, H. E. & HAVLIN, S. (2017) Generalized model for k-core percolation and interdependent networks. *Physical Review E*, **96**(3), 032317.

[60] PARANDEHGHEIBI, M. & MODIANO, E. (2013) Robustness of interdependent networks: The case of communication networks and the power grid. in *Global Communications Conference (GLOBECOM), 2013 IEEE*, pp. 2164–2169. IEEE.

[61] PARSHANI, R., BULDYREV, S. V. & HAVLIN, S. (2010) Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Physical review letters*, **105**(4), 048701.

[62] QIU, Y. (2013a) The Effect of Clustering-Based and Degree-Based Weighting on Robustness in Symmetrically Coupled Heterogeneous Interdependent Networks. in *2013 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 3984–3988. IEEE.

[63] ——— (2013b) Optimal weighting scheme and the role of coupling strength against load failures in degree-based weighted interdependent networks. *Physica A: Statistical Mechanics and its Applications*, **392**(8), 1920–1924.

[64] RADICCHI, F. (2015) Percolation in real interdependent networks. *Nature Physics*, **11**(7), 597–602.

[65] RADICCHI, F. & ARENAS, A. (2013) Abrupt transition in the structural formation of interconnected networks. *Nature Physics*, **9**(11), 717–720.

[66] RAHNAMAY-NAEINI, M. & HAYAT, M. M. (2016) Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach. *IEEE Transactions on Smart Grid*, **7**(4), 1997–2006.

[67] RANJAN, G. & ZHANG, Z.-L. (2011) How to glue a robust smart-grid?: a finite-network theory for interdependent network robustness. in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, p. 22. ACM.

[68] REIS, S. D., HU, Y., BABINO, A., ANDRADE JR, J. S., CANALS, S., SIGMAN, M. & MAKSE, H. A. (2014) Avoiding catastrophic failure in correlated networks of networks. *Nature Physics*, **10**(10), 762–767.

[69] ROTH, K., MORONE, F., MIN, B. & MAKSE, H. A. (2017) Emergence of robustness in networks of networks. *Physical Review E*, **95**(6), 062308.

[70] RUEDA, D., CALLE, E., MALDONADO-LOPEZ, F. & DONOSO, Y. (2016) Reducing the impact of targeted attacks in interdependent telecommunication networks. in *Telecommunications (ICT), 2016 23rd International Conference on*, pp. 1–5. IEEE.

[71] RUEDA, D. F. & CALLE, E. (2017) Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks. *International Journal of Critical Infrastructure Protection*, **16**, 3–12.

[72] RUEDA, D. F., CALLE, E. & MARZO, J. L. (2017) Improving the robustness to targeted attacks in software defined networks (SDN). in *DRCN 2017-Design of Reliable Communication Networks; 13th International Conference; Proceedings of*, pp. 1–8. VDE.

[73] SAHNEH, F. D., MELANDER, J., SCOGLIO, C. ET AL. (2017) Contact Adaption during Epidemics: A Multilayer Network Formulation Approach. *IEEE Transactions on Network Science and Engineering*.

[74] SCHNEIDER, C. M., YAZDANI, N., ARAÚJO, N. A., HAVLIN, S. & HERRMANN, H. J. (2013) Towards designing robust coupled networks. *Scientific reports*, **3**.

[75] SHAO, S., HUANG, X., STANLEY, H. E. & HAVLIN, S. (2014) Robustness of a partially interdependent network formed of clustered networks. *Physical Review E*, **89**(3), 032812.

[76] SHEKHTMAN, L. M., BEREZIN, Y., DANZIGER, M. M. & HAVLIN, S. (2014) Robustness of a network formed of spatially embedded networks. *Physical Review E*, **90**(1), 012809.

[77] SHU, P., GAO, L., ZHAO, P., WANG, W. & STANLEY, H. E. (2017) Social contagions on interdependent lattice networks. *Scientific reports*, **7**, 44669.

[78] STIPPINGER, M. & KERTÉSZ, J. (2014) Enhancing resilience of interdependent networks by healing. *Physica A: Statistical Mechanics and its Applications*, **416**, 481–487.

[79] SUN, S., WU, Y., MA, Y., WANG, L., GAO, Z. & XIA, C. (2016) Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks. *Scientific Reports*, **6**.

[80] TAN, F., XIA, Y. & WEI, Z. (2015) Robust-yet-fragile nature of interdependent networks. *Physical Review E*, **91**(5), 052809.

[81] TANG, L., JING, K., HE, J. & STANLEY, H. E. (2016) Complex interdependent supply chain networks: Cascading failure and robustness. *Physica A: Statistical Mechanics and its Applications*, **443**, 58–69.

[82] TYRA, A., LI, J., SHANG, Y., JIANG, S., ZHAO, Y. & XU, S. (2017) Robustness of non-interdependent and interdependent networks against dependent and adaptive attacks. *Physica A: Statistical Mechanics and its Applications*, **482**, 713–727.

[83] WANG, J., JIANG, C. & QIAN, J. (2014) Robustness of interdependent networks with different link patterns against cascading failures. *Physica A: Statistical Mechanics and its Applications*, **393**, 535–541.

[84] WANG, J., LI, Y. & ZHENG, Q. (2015) Cascading load model in interdependent networks with coupled strength. *Physica A: Statistical Mechanics and its Applications*, **430**, 242–253.

[85] WANG, S. & LIU, J. (2016) Robustness of single and interdependent scale-free interaction networks with various parameters. *Physica A: Statistical Mechanics and its Applications*, **460**, 139–151.

[86] WANG, X., CAO, J., LI, R. & ZHAO, T. (2017) A preferential attachment strategy for connectivity link addition strategy in improving the robustness of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, **483**, 412–422.

[87] WANG, X., CAO, J. & QIN, X. (2016) Study of Robustness in Functionally Identical Coupled Networks against Cascading Failures. *PloS one*, **11**(8), e0160545.

[88] WANG, X., KOOIJ, R. E. & VAN MIEGHEM, P. (2016) Modeling region-based interconnection for interdependent networks. *Physical Review E*, **94**(4), 042315.

[89] WATANABE, S. & KABASHIMA, Y. (2014) Cavity-based robustness analysis of interdependent networks: Influences of intranetwork and internetwork degree-degree correlations. *Physical Review E*, **89**(1), 012808.

[90] XIA, Y., ZHANG, W. & ZHANG, X. (2016) The effect of capacity redundancy disparity on the robustness of interconnected networks. *Physica A: Statistical Mechanics and its Applications*, **447**, 561–568.

[91] YUAN, X., SHAO, S., STANLEY, H. E. & HAVLIN, S. (2015) How breadth of degree distribution influences network robustness: Comparing localized and random attacks. *Physical Review E*, **92**(3), 032122.

[92] ZHANG, Q., LI, D., KANG, R., ZIO, E. & ZHANG, P. (2013) Reliability Analysis of Interdependent Networks Using Percolation Theory. in *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on*, pp. 626–629. IEEE.

[93] ZHANG, W., XIA, Y., OUYANG, B. & JIANG, L. (2015) Effect of network size on robustness of interconnected networks under targeted attack. *Physica A: Statistical Mechanics and its Applications*, **435**, 80–88.

[94] ZHANG, X., PHILLIPS, C. & CHEN, X. (2011) An overlay mapping model for achieving enhanced QoS and resilience performance. in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, pp. 1–7. IEEE.

[95] ZHANG, X.-J., XU, G.-Q., ZHU, Y.-B. & XIA, Y.-X. (2016) Cascade-robustness optimization of coupling preference in interconnected networks. *Chaos, Solitons & Fractals*, **92**, 123–129.

[96] ZHAO, D.-W., WANG, L.-H., ZHI, Y.-F., ZHANG, J. & WANG, Z. (2016) The robustness of multiplex networks under layer node-based attack. *Scientific reports*, **6**.

[97] ZHAO, Y. & QIAO, C. (2017) Enhancing the robustness of interdependent cyber-physical systems by designing the interdependency relationship. in *Communications (ICC), 2017 IEEE International Conference on*, pp. 1–6. IEEE.

[98] ZHAO, Z., ZHANG, P. & YANG, H. (2015) Cascading failures in interconnected networks with dynamical redistribution of loads. *Physica A: Statistical Mechanics and its Applications*, **433**, 204–210.

[99] ZHOU, D., BASHAN, A., COHEN, R., BEREZIN, Y., SHNERB, N. & HAVLIN, S. (2014) Simultaneous first-and second-order percolation transitions in interdependent networks. *Physical Review E*, **90**(1), 012803.

[100] ZHOU, D. & ELMOKASHFI, A. (2017) Overload-based cascades on multiplex networks and effects of inter-similarity. *PloS one*, **12**(12), e0189624.

[101] ZHOU, D., GAO, J., STANLEY, H. E. & HAVLIN, S. (2013) Percolation of partially interdependent scale-free networks. *Physical Review E*, **87**(5), 052812.

[102] ZHOU, D., STANLEY, H. E., D'AGOSTINO, G. & SCALA, A. (2012) Assortativity decreases the robustness of interdependent networks. *Physical Review E*, **86**(6), 066103.

[103] ZHU, Q., ZHU, Z., WANG, Y. & YU, H. (2016) Fuzzy-information-based robustness of interconnected networks against attacks and failures. *Physica A: Statistical Mechanics and its Applications*, **458**, 194–203.