

<http://dx.doi.org/10.17703/JCCT.2022.8.6.531>

JCCT 2022-11-65

메가시티 국가기반체계의 핵심노드 식별 방법

How to Identify Critical Nodes of National Infrastructure Systems in Megacities

심준학*, 장찬규**, 박성준***, 김기원****, 조상근*****, 박상혁*****

Jun Hak Sim*, Jang chan Kyu**, Sung Jun Park***,
Ki Won Kim****, Sang Keun Cho*****, Sang Hyuk Park*****

요약 전 세계적으로 국가경쟁력, 효율성, 중요성 등의 이유로 메가시티가 속속 등장하고 있으며, 점차 각 국가의 중심지로 자리를 잡아가고 있다. 또한, 메가시티는 현존, 잠재적, 초국가, 비군사 등 다양한 위협에 노출될 수밖에 없다. 특히, 최근 우크라이나-러시아 전쟁에서 볼 수 있듯이 국가기반체계는 적대 및 위협세력의 주요 목표가 되고 있다. 하지만 메가시티의 막대한 규모, 다양한 위협의 양상, 한정된 자원 등을 고려할 때 모든 국가기반체계를 완벽하게 방호하는 것은 현실적으로 어렵다. 따라서 여러 국가기반체계 중 핵심노드를 식별하여 중점적으로 방호하는 접근이 필요하다. 핵심노드는 다양한 국가기반시설이 연결된 국가기반체계의 중요도가 매우 높면서도 동시에 급소에 해당한다. 이를 위해 본 연구에서는 핵심노드를 논리적·체계적으로 식별하기 위해 네트워크 이론인 노드 중심성(Centrality) 분석방법과 군사이론인 중심(Center of Gravity) 분석방법을 제시하였다.

주요어 : 메가시티, 국가기반체계, 위협, 핵심노드, 노드 중심성, 중심

Abstract Megacities are emerging all over the world and gradually becoming the center of an country. Therefore, Megacities are inevitably exposed to various threats such as existing, potential, supra-national, and non-military. In particular, as seen in the recent Ukraine-Russia war, national infrastructure systems has become a major target of enemies. However, considering the size of Megacities, various types of threats, and limited resources, it is impossible to completely protect all national infrastructure systems. Therefore, wisdom is necessary to identify and protect critical nodes. The critical node is the vital point to which the national infrastructure is connected. To this end, in this study, as a method for logically and systematically identifying critical nodes, Node centrality analysis method, which is a network theory, and the Center of Gravity analysis method, which is a military theory, were presented.

Key words : Megacity, National Infrastructure Systems, Threat, Critiacl node, Node centrality, Center of Gravity

*정회원, 육군대학 지상작전 교관 (제1저자)
**정회원, 육군대학 지상작전 교관 (참여저자)
***정회원, 육군대학 전략학 교관 (참여저자)
****정회원, 대경대학교 군사학과 교수 (참여저자)
*****정회원, 육군대학 전략학 교관 (참여저자)
*****정회원, 우석대학교 군사학과 교수 (교신저자)
접수일: 2022년 10월 31일, 수정완료일: 2022년 11월 6일
게재확정일: 2022년 11월 9일

Received: October 31, 2022 / Revised: November 6, 2022
Accepted: November 9, 2022
*****Corresponding Author: plbas@hanmail.net
Dept. of Military Science, WooSuk Univ, Korea

I. 서 론

오늘날 전 세계적으로 산업화의 고도화는 물론 도시화가 매우 빠르게 가속화되고 있다. 대부분의 선진국 또는 강대국에서는 인구 1,000만 명 이상의 인구가 거주하며, 정치·경제·사회·산업 등 국가기반시설이 집적해 있는 이른바 “메가시티”가 생성되었으며, 이는 국가 경쟁력을 좌우되는 요소로 작용하기도 한다[1]. 2016년 UN의 통계에 따르면, 이러한 메가시티는 전 세계에 47개 도시가 해당하는 것으로 확인되었다.

우리나라의 서울·경기·인천을 포함한 수도권은 이를 중심으로 활동하는 인구가 2,500만 명에 육박한다. 1,000만명을 넘어서는 등 메가시티로 분류된지 오래이다. 우리 정부에서는 2014년 10월 14일 수도권은 물론 지방에 대해서도 초광역 경제·생활권 형성을 목표로 하는 ‘초광역 협력지원전략’을 수립하였다[2]. 현재는 이미 메가시티인 수도권이 아닌 부산·울산·경남, 대구·경북, 광주·전남, 충청권 등 3개 지역에 대해 초광역권 발전 계획을 수립하여 추진 중이며, 이들 초광역권은 현재의 수도권에 버금가는 메가시티가 될 것으로 전망된다. 남한 내의 전 지역을 도시화하는 것이 아닌 특정 거점을 중심으로 수 개의 도시들을 유기적으로 연결하여 하나의 권역을 형성하고 이들 권역은 메가시티 化되어 수천 만명의 국민들이 생활가능한 인프라를 토대로 집약될 것이다.

메가시티는 많은 인구와 경제·산업·교통·문화 등의 기능이 복합되어 발생하는 시너지를 바탕으로 국가의 경쟁력을 향상시키고, 인간의 삶을 풍성하게 해준다는 이점이 있다. 반면에 다양한 기반 시설과 인구의 밀집으로 인한 취약점을 수반하기도 한다.

특히, 우리나라와 같이 적대국 및 적대세력의 군사적 긴장 상태를 유지하고 있는 상황에서 수도권 등 향후 조성된 메가시티는 북한과의 전쟁 혹은 군사도발, 테러 집단에 의한 공격 등에 매우 취약하다. 직접적인 물리적 파괴뿐만 아니라 막대한 유동인구, 밀집된 시설·기능을 대상으로한 사이버 공격 등과 같은 간접적, 비물리적인 공격이 이루어질 경우, 상상을 뛰어넘는 큰 피해를 초래할 수 있다. 적대세력도 이와 같은 메가시티의 중요성을 적대세력 인식하고 있을 것이며, 이를 전쟁수행 간 유리하게 활용하려 할 것이다. 즉, 메가시티의 취약점을 식별하고, 이에 대한 집중적인 공격과

함께 산재된 중요시설에 대한 교란작전으로 아군의 효율적 대응을 방해할 것이다.

한편, 메가시티의 물리적, 기능적 막대한 규모로 인해 이를 구성하는 모든 국가 기반시설을 완벽하게 방호하는 것은 불가능에 가깝다. 전술(前述)한 것처럼 메가시티의 거대한 규모와 다양한 위협의 양상을 고려했을 때, 한정된 국가 및 군사 자원으로 이들 모두를 방호하기에는 충분하지 않다. 이에 따라, 메가시티에 산재된 모든 국가 기반시설을 동시에 방호하는 것보다는 적이 집중적으로 공격할 대상이나 공격을 받게 되었을 때 메가시티 전체에 미치는 파급효과가 지대한 것. 즉 메가시티의 급소를 식별하여 집중적으로 방호하는 전략적, 전술적 접근이 필요하다.

본 연구에서는 이와 같은 문제의식을 바탕으로 국가 기반시설의 급소인 핵심노드를 식별하는데 다음의 두 가지 방법을 제시하였다. 네트워크 분야에서 활용하고 있는 “노드 중심성 분석방법”과 “군사 분야의 중심(CoG) 분석방법”이다.

II. 메가시티를 구성하는 국가기반체계와 국가기반시설

국가기반시설은 국가기반체계의 한 구성요소이다. 여기서 국가기반체계는 에너지, 정보·통신, 교통·수송, 금융, 산업, 보건·의료, 원자력, 건설·환경, 식·용수 등으로, 그 기능이 마비될 경우 인명·재산피해와 국가 경제에 심각한 영향을 미칠 수 있는 인적·물적체계를 의미한다[3]. 그리고 국가기반시설은 전술한 국가기반체계를 보호하기 위해 계획적으로 관리할 필요가 있다고 인정되는 시설을 의미한다[4].

이와 같은 국가기반시설은 표1과 같이 ‘국토의 계획 및 이용에 관한 법률 제2조(기반시설)’에 의거 도로, 철도, 항만, 공항, 하천시설, 댐, 저수지 등 SOC 7종과 수소, 하수도, 전기, 가스, 열공급, 통신, 송유, 공동구 등 지하시설물 8종으로 분류된다[5].

국가기반시설의 지정 기준은 ‘재난 및 안전관리 기본법’ 시행령에서 정한 바에 따른다. 이 법에 따르면 다른 국가기반체계에 미치는 연쇄효과, 중앙행정기관의 공동 대응의 필요성, 국가안전·경제·사회에 미치는 피해 규모와 범위 등을 고려하여 분야별 국가기반시설을 지정하도록 되어 있다[6]. 국가기반시설은 외부 위협 세력에

효과적으로 대응하기 위해 경찰조직이 주도하고 군(軍)이 지원하는 시스템으로 되어 있다[7]. 메가시티의 국가기반시설의 지정 소요는 4차 산업혁명 도래에 따라 메가시티의 국가기반체계가 더욱 지능화·초연결되고 융복합화됨에 따라 더욱 다변화될 것으로 전망된다.

표 1. 국토계획법에 제시된 국가기반시설 종류
 Table 1. Types of national infrastructure proposed in the National Land Planning Act

분야별	계	지정시설
에너지 (43)	전력	21 화력(13), 원자력(4), 수력(2), 전기(2)
	가스	4 생산기지(인수, 저장, 기화, 송출)(4)
	석유	18 생산시설(5), 비축시설(9), 수송시설(4)
정보통신 (19)	통신	11 통신교환국사(7), 망관리센터(3), 해저케이블육양국(1)
	전산	8 전산망(4), 정보센터(4)
교통수송 (34)	철도	1 철도(1) : 한국철도공사(전국 철도시설)
	항공	9 항공교통센터(1), 공항(8)
	화물	1 내륙컨테이너기지(1)
	도로	1 고속국도(1) : 한국도로공사
	지하철	11 지하철(11): 서울·부산·인천·광안·마산 등
금융(8)	금융	8 금융(8): 한국·한국수출입·산업은행 등
	의료 서비스	12 병원(12): 국립중앙의료원 등
보건의료 (31)	혈액	19 혈액원(16), 혈액검사센터(3)
	원자력 (36)	원자력 36 원자력발전소(4), 방사성폐기물처분시설(1)
환경(6)	매립	6 매립장(6)
식용수 (84)	댐	34 다목적댐(20), 생공용수댐(14)
	정수장	50 광역정수장(20), 지방정수장(30)
정부중요시설 (12)	정부중요시설	12 중앙행정기관(12)

III. 메가시티 국가기반체계의 핵심노드 식별 방법

현실적으로 현존, 잠재적, 초국가, 비군사 등의 다양한 위협으로부터 메가시티의 모든 국가기반시설을 온전하게 보호할 수는 없을 것이다. 메가시티 내 존재하는 국가기반시설의 수가 많고, 이를 위한 상당한 인력, 장비, 물자, 예산 등이 소요되기 때문이다. 이에 따라, 꼭 필요한 메가시티의 필수적인 기능발휘를 보장해주는 차원에서 국가기반체계의 핵심노드 위주로 보호하는 방안이 필요한 것이다.

이를 위해, 본 연구에서는 메가시티의 국가기반체계 내 존재하는 핵심노드 식별을 위한 방법으로 네트워크

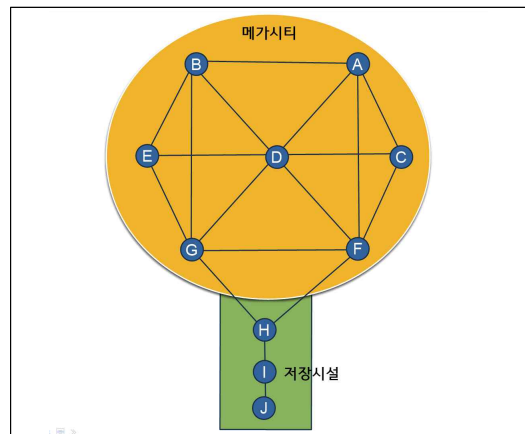
분야에서 활용하고 있는 노드 중심성 분석 방법과 군사 분야의 중심 분석 방법을 다음과 같이 제시하였다.

3.1 '노드 중심성' 분석 방법

'노드 중심성'은 드루 맥키(Drew Mackie)가 사회 네트워크에서 개인이 가지는 영향력이라는 관점에서 개발되었으며, 인적 네트워크 상에서 핵심 인물이 누구인지를 확인하는 데 주로 사용된다. '노드 중심성' 분석을 통해 한 네트워크에서 중요한 역할을 하거나 주목받는 행위자가 누구인지, 또는 각 행위자는 그 중심에 어느 정도 접근하고 있는지 알 수 있다[8].

이와 같은 개념을 적용하면 메가시티에 존재하는 국가기반체계의 핵심노드를 식별하는 것이 가능하다. 국가기반체계도 앞서 언급한 드루 맥키의 인적 네트워크 처럼 에너지, 정보·통신, 교통·수송, 금융, 산업, 보건·의료, 원자력, 건설·환경, 식·용수 등이 인적·물적 체계로 연결되어 있기 때문이다. '노드 중심성' 분석을 통해 핵심노드를 식별하는 방법은 다음과 같다.

우선, 국가기반체계 유형별 '노드 중심성'을 분석한다. '노드 중심성'은 자체 및 인접한 체계에 존재하는 노드들 간의 상호 관계성을 분석하여 규명할 수 있다. 그림1처럼 ㉠는 주위 노드와 가장 많이 연결된 노드는 '연결노드'라고 부른다. ㉡·㉢는 '연결노드'와 인접하면서 인접한 체계의 노드와 가까운 위치에 있는 노드로 '근접노드'라고 부른다. ㉣는 서로 다른 체계가 접합하는 부분에 위치한 노드로 '중계노드'라고 부른다.



출처: <https://www.williemiller.com/network-mapping.htm>

그림 1. 노드 중심성 분석 개념도

Figure 1. Conceptual diagram of centrality analysis of nodes

다음으로, 선정된 ‘연결노드’, ‘근접노드’, ‘중계노드’ 중에서 ‘핵심노드’를 선정한다. 앞에서 언급한 것처럼 ‘핵심노드’ 선정 기준 중 가장 중요한 것은 메가시티의 필수기능 발휘 가능 여부이다. 이를 쉽게 설명하기 위해 그림1을 메가시티 내외부에 형성된 송유관 네트워크라고 가정하자. 여기서 ‘C-F-G-H-B-A(6각형)’는 메가시티의 실제 면적이고, ‘①’는 메가시티 외부에 위치한 유류 저장시설이다.

우선, 연결노드(④)가 공격받게 되면 ①로부터 공급되는 유류가 메가시티 중심지역을 제외한 나머지 지역으로 공급될 수 있다. 다음으로, 근접노드(⑤)가 공격받았을 경우 유류는 ④를 경유하여 메가시티 대부분의 곳으로 공급될 수 있다. 또 다른 근접노드(⑥) 경우도 마찬가지이다. 한편, 중계노드(③)가 공격받게 되어 파괴된다면 메가시티 내부로의 유류 공급은 전면 차단된다. 따라서 유류 공급 차원에서 메가시티의 ‘핵심노드’는 중계노드인 ③가 된다. 물론, 메가시티에 유류를 공급하는 원점인 ①(저장시설)도 ‘핵심노드’이다.

이와 관련하여 2019년 9월 14일 사우디아라비아 아람코(Aramco) 석유 저장시설에 대한 드론 테러가 발생했다. 당시 예멘의 후티(Houthi) 반군은 장거리 드론과 순항미사일을 운용하여 테러를 자행한 것으로 추정되고 있다[9]. 이에 따라, 메가시티의 원활한 에너지 공급을 위해서는 핵심노드(③-①)를 방호할 수 있는 저고도 방공체계를 비롯한 해킹에 대비한 사이버 방호체계 등 다양한 대책을 강구해야 할 것이다.

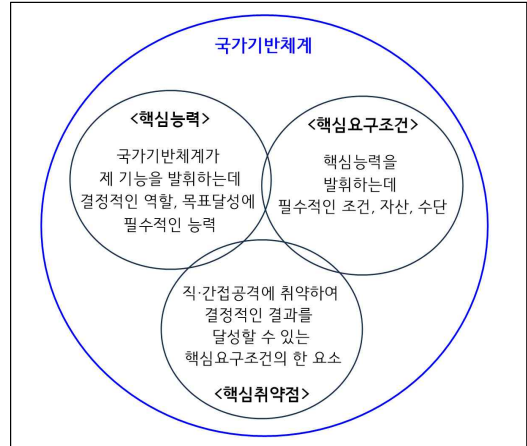


출처: <https://www.saudiembassy.net/archive/201909>

그림 2. 아람코 석유 시설을 공격한 드론들
Figure 2. Drones that attacked Oil Facilities of Aramco

3.2 ‘중심’ 분석 방법

‘중심(Center of Gravity, CoG)’은 1996년 미해병대 전쟁대학원의 스트레인지(Joe Strange) 박사가 제시하였다. 그는 중심(CoG)을 정신적·물리적 힘, 행동의 자유 또는 전투의지를 제공하는 능력이나 힘의 원천으로 정의하고, 중심(CoG) 구성하는 3요소로 핵심능력(Critical Capability, CC), 핵심요구조건(Critical Requirement, CR) 및 핵심취약점(Critical Vulnerability, CV)을 제시했다[10].



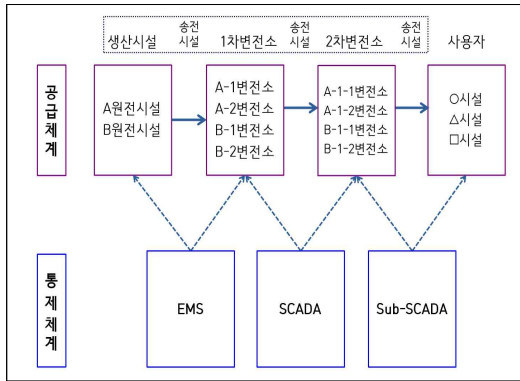
출처: Joe starange, centers of gravity & critical vulnerabilities, perspectives on warfighting number four, 2nd ed. (Quantico, VA: Marine Corps University, 1996), pp. 1-152.

그림 3. 중심 분석 방법을 적용한 국가기반체계의 핵심노드 식별 방법

Figure 3. How to identify critical nodes of the national infrastructure systems by applying the COG analysis method

여기서 핵심능력(CC)은 국가기반체계가 제 기능을 발휘하는 데 결정적인 역할을 하는 능력으로써 목표 달성에 필수적인 능력을 의미한다. 핵심요구조건(CR)은 핵심능력이 온전하게 발휘되는데 필수적인 조건, 자원, 수단 등을 의미한다. 핵심취약점(CV)은 외부로부터의 직·간접공격에 취약하여 결정적이고 중대한 결과를 조성할 수 있는 핵심요구조건 그 자체 또는 핵심요구조건의 한 요소나 핵심요구조건의 취약점을 의미한다. 핵심취약점은 국가기반체계 그 자체 또는 국가기반체계의 핵심능력과 직접적으로 관련된 약점들도 고려하여 분석한다[11]. 즉, 국가기반체계의 핵심노드는 주로 핵심취약점 중에서 식별된다[12].

이를 아래 그림4의 원전 중심의 전력 공급망을 예를 들어 설명하면 다음과 같다. 우선, 메가시티의 전력체계가 갖는 핵심능력(CC)은 ‘메가시티 전력을 공급·통제할



출처: The transactions of the Korean Institute of electrical engineers, pp. 318-319.

그림 4. 메가시티 전력체계 핵심노드 식별 개념도
 Figure 4. Conceptual diagram of Identifying Megacity Electronic System critical nodes

수 있는 능력'이다. 이 중에서 '메가시티 전력을 공급할 수 있는 능력'이 온전하게 발휘되는데 필수적인 자산인 핵심요구조건(CR)은 원전시설, 변전소, 송전시설, 통제체계 등이 있다[13]. 이중 핵심취약점(CV)은 전력계통운영시스템(Energy Management System, EMS)과 송·변전 원방감시제어시스템(Supervisory Control and Data Acquisition, SCADA)인 EMS와 SCADA가 될 수 있다. 이것들은 전력체계의 주제어실이고 외부의 직·간접 공격에 취약하기 때문이다. 즉, 메가시티에 전력을 공급하는 원전 중심의 전력 공급망의 핵심노드는 EMS와 SCADA로 선정할 수 있다[15].

이와 관련하여 2022년 3월 러시아 해커들이 미국 켄 사스 버링턴(Burlington)에 위치한 울프 크릭(Wolf Creek) 원전의 SCADA에 대한 해킹을 시도했다[14]. 전 세계 4차 산업혁명 시대로 진입함에 따라 점차 초연결될 것이다. 이로 인해, 원전 네트워크에 대한 사이버 공격은 점차 고도화될 것으로 전망된다. 따라서 메가시티에 안정적인 전력 공급을 위해서는 원전 통제체계(핵심노드)에 인공지능(AI), 블록체인, 양자암호 등 첨단과학기술이 덧입혀진 사이버 방호체계를 구축해야 할 것이다.

IV. 결론

오늘날 세계 주요 국가들은 메가시티가 갖는 중요성, 효율성, 경쟁력 등으로 인해 정책적으로 메가시티 육성을

적극 추진하고 있다. 4차 산업혁명 기술의 구현장, 융복합된 기능과 시스템의 복합체계로서 인류가 만든 가장 거대한 구조인 메가시티는 한 국가의 중심이라고 해도 과언이 아닌 막대한 가치를 내포한다. 이에 따라, 전시뿐만 아니라 유사시에도 메가시티의 필수적인 기능 발휘를 보장하기 위해서는 국가기반체계에 대한 체계적인 방호가 요구된다.

본 연구에서는 이와 같은 문제의식을 바탕으로 국가기반체계의 핵심노드 식별을 위한 논리적인 방법을 다음과 같이 제시하였다. 첫 번째는 노드 중심성 분석방법이다. 이것은 국가기반체계의 노드 중심성을 분석하여 연결노드, 근접노드, 중계노드 등을 식별하고, 이를 바탕으로 핵심노드를 선정하는 방법이다. 두 번째는 중심(CoG) 분석방법이다. 이것은 국가기반체계의 3대 핵심요소인 핵심능력, 핵심요구조건, 핵심취약점을 분석하고, 핵심취약점 중에서 핵심노드를 선정하는 방법이다.

전술(前述)한 두 가지 방법은 미래 메가시티의 국가기반체계를 방호하기 위한 하나의 안(案)에 불과하다. 앞으로 4차 산업혁명의 주요기술이 발전함에 따라 메가시티의 국가기반체계에 가해지는 위협은 고도화될 것이다. 따라서 후속 연구를 통해 다양한 핵심노드 식별 방법을 발굴하고, 이와 동시에 핵심노드를 효율적으로 방호할 수 있는 다양한 방안을 도출할 필요가 있다.

References

- [1] K. B. Kim & G. C. Kim & C. H. Jin, "Status and Prospect of Smart City in the Fourth Industrial Revolution Era", Journal of the Korea Convergence Society, 9(9), pp. 191-197, 2018.
- [2] Ministry of the Interior and Safety, "Ultra-wide Cooperation Support Strategy" 2021.
- [3] Presidential Decree No. 233, "Regulations on the operation and situation management of the Central Disaster and Safety Countermeasure Headquarters related to the protection of the national infrastructure", Chapter 1.
- [4] S. J. Dong, "National Infrastructure Vulnerability Assessment and Safety Management Technology Development", Journal of Disaster Prevention, vol. 15(4), pp. 93-97, 2018.
- [5] Act No. 17453, "National Land Planning And Utilization Act", Chapter 2.

- [6] Act No. 17698, "Framework Act On The Management Of Disasters And Safety", Chapter 4.
- [7] Presidential Decree No. 309, "National Counter-Terrorism Guidelines", Chapter 5.
- [8] <https://www.williemiller.com/network-mapping.htm> (accessed September 22, 2022)
- [9] <https://www.aljazeera.com/economy/2019/9/14/houthi-drone-attacks-on-2-saudi-aramco-oil-facilities-spark-fires>
- [10] Joe Starange, Centers of Gravity & Critical Vulnerabilities, Perspectives on Warfighting Number Four, 2nd ed. (Quantico, VA: Marine Corps University, 1996), pp. 1-152.
- [11] US Joint Chiefs of Staff, "Joint Publication 5-0 Joint Planning", 2020.
- [12] US Joint Chiefs of Staff, "Joint Publication 2-01.3 Joint Intelligence Preparation of the Operational Environment", 2014.
- [13] D. J. Kang, "Quantitative Methodology to Assess Cyber Security Risks of SCADA system in Electric Power Industry", Journal of the institute of information Security & Cryptology (JKIISC), pp.446-447, 2013.
- [14] <https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical>
- [15] R. W. Jong, "A Study on Network Architecture for KEPCO SCADA Systems", Industry Promotion Research, pp. 2-3. 2017.