### Understanding the Security of Traffic Signal Infrastructure

#### Zhenyu Ning, Fengwei Zhang, and Stephen Remias

COMPASS Lab Wayne State University



#### DIMVA, June 19, 2019

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

・ロト ・四ト ・ヨト ・ヨト

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

イロン イロン イヨン イヨン



Traffic signal systems have introduced large regional networks and operation centers to help alleviate traffic congestion.

- Traditional traffic signal systems use rotating gears and wheels to control the traffic signals.
  - Simple, but lack of flexibility.
- Modern traffic signal systems have achieved an efficient control over the vehicle traffic via numerous technologies.

イロト 不得 トイヨト イヨト 二日

#### Modern Traffic Signal System





source: https://www.orangetraffic.com/product/mtq-traffic-light-distribution-and-control-cabinet/

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

<ロト <回 > < 注 > < 注 > … 注

#### Modern Traffic Signal System





source: https://www.orangetraffic.com/product/mtq-traffic-light-distribution-and-control-cabinet/

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

æ

ヘロン 人間 とくほと 人ほとう

Introduction



# Is it secure?

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

#### Introduction



### Is the traffic signal system secure?

- Previous research mainly focus on the traffic controller and network vulnerabilities.
  - [1, 2, 3]
- However, traffic signal systems are actually comprised of many components!
  - E.g., traffic controller, fail-safe systems, surveillance cameras, et, al.

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

イロン イロン イヨン イヨン



- A modern traffic signal systems is comprised of many hardware components.
- These components are normally placed in a roadside cabinet.
- Cabinet standards are applied to the components inside the cabinet.
  - TS-2 cabinet standard and ITS cabinet standard.

イロト 不得 トイヨト イヨト 二日



The Advanced Transportation Controller (ATC) is the core part for a traffic signal control system.

- Build upon a Linux kernel with BusyBox.
- Directly controls the traffic signals with specific software.
- E.g., Intelight Model 2070 ATCs and Siemens Model 60 ATCs.

イロト 不得 トイヨト イヨト 二日



The fail-safe components are used to guarantee that the traffic signals would not turn to a dangerous state even when the ATC is malfunctional.

- ► Malfunction Management Unit (MMU) in TS-2 Standard.
- Cabinet Monitor Unit (CMU) in ITS Standard.





Understanding the Security of Traffic Signal Infrastructure, DIMVA 19



Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

æ





Understanding the Security of Traffic Signal Infrastructure, DIMVA 19



Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

æ



The conflict status is predefined by **Programming Card** in MMU and **Datakey** in CMU.

- In Programming Card, the conflict status is defined by soldered wire jumpers.
- Datakey is an EEPROM memory device.

イロト 不得 トイヨト イヨト 二日

#### MMU Programming Card





source: https://www.flickr.com/photos/robklug/5617557995/in/photostream/

< 17 ▶

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

#### CMU Datakey





source: https://manualzz.com/doc/8353064/888-1212-001-monitorkey-operation-manual

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

æ

・ロト ・回ト ・ヨト ・ヨト

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

イロン イロン イヨン イヨン

#### Security Analysis



- Methodology: Partnering with a municipality in USA.
- Analysis Environment:
  - A standard traffic signal system in our lab.
  - The traffic signal system lab in the municipality.
  - The deployed traffic signal system in the municipality.
- Devices:
  - TS-2 cabinets with Siemens Model 60 ATC and EDI MMU-16LE.
  - ITS cabinets with Intelight Model 2070 ATC and CMU-212.

イロト 不得 トイヨト イヨト 二日





## How to attack the system?

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

э

イロン 不同 とくほう イロン

#### Security Analysis



How to attack the traffic signal system?

3

ヘロト ヘヨト ヘヨト ヘヨト

#### Security Analysis



How to attack the traffic signal system?

Step 1 - Access the Traffic Signal System Step 2 - Control the Traffic Signals

Step 3 - Bypass Fail-Safe Components



Obstacles for accessing the traffic signal system physically:

- Surveillance Camera
- Cabinet Lock
- Cabinet Door Status Monitoring

3



According to the municipality officials,

- ► There are 750 vehicle intersections in the municipality.
- ▶ 275 vehicle intersections are covered by traffic cameras.
- ▶ More than 60% of the intersections are out of surveillance.

< ロ > < 同 > < 回 > < 回 > < □ > <



According to the cabinet specifications, both TS-2 and ITS cabinets shall be provided with a Corbin #2 key.

- ► However, the Corbin #2 master key is sold online.
- The sold key is marked with the ability to open most traffic signal cabinets in the United States.
- With \$5 USD, we are able to open all cabinets in the municipality lab.



In the ITS cabinets, the status of the door can be monitored by the CMU.

- ATC send query message to CMU to get the door status.
- In real-world deployment,
  - The door alarm message is saved to log file by ATC.
  - The log file is forwarded to the municipality every one-to-five minute.

イロン 不同 とくほう イロン

#### **Physical Access**



Obstacles for accessing the traffic signal system physically:

- Surveillance Camera
   60% intersections are out of surveillance
- Cabinet Lock
   \$5 USD for the master key
- Cabinet Door Status Monitoring Non-real-time alarm

イロン イロン イヨン イヨン



- Previous work [3] has shown that the wireless communication network is vulnerable.
- We find that both types of ATCs use default credentials for the SSH and Telnet.
  - The municipality were not aware of the ability to login to the ATC over SSH.
- The public IP addresses of a number of ATCs can be identified on Shodan [4] website.

イロト 不得 トイヨト イヨト 二日

#### Security Analysis



How to attack the traffic signal system?

Step 1 - Access the Traffic Signal System
Step 2 - Control the Traffic Signals
Step 3 - Bypass Fail-Safe Components

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19



With physical access,

- The signal pattern can be configured by the control buttons on the front panel.
- ► No authentication is activated in analyzed ATCs.
  - Access code can be set to control the access, but the partnering municipality didn't do so.

### Control the Traffic Signals



Normally, the traffic signals are controlled by specific software running in the Linux kernel via several serial ports. With remote access,

- Directly write commands to the serial ports.
  - Command specification is publicly available.
  - Communication is unencrypted.
  - No authentication is required.
- Manipulate the driver of the front panel.

イロン 不同 とくほう イロン

#### Security Analysis



How to attack the traffic signal system?

3

ヘロン 人間 とくほと 人ほとう



With physical access,

- For MMU, resolder the wire jumpers of the programming card.
- ► For CMU, reconfigure the parameters stored in the Datakey.
  - The configuration is unencrypted.
  - A customized Datakey access tool can be built by an Arduino Uno starter-kit.

イロン 不同 とくほう イロン



With remote only access, we are not able to bypass the fail-safe components completely.

We design a transient avoidance tactic to fight the fail-safe components.

イロト 不得 トイヨト イヨト 二日

#### Transient Avoidance Tactic





#### TRADITIONAL CONFLICT FAULT STATE INITIATION

CONFLICT FAULT STATE INITIATION AVOIDANCE BY UTILIZING TRANSIENT ATTACKS

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

э

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

<ロ> <同> <同> < 回> < 回>

#### Attacks and Mitigations





#### Test environment in the municipality lab and our lab

Image: A math a math



- Stealthy Manipulation and Control
  - Stealthy control the traffic signal to introduce congestion.
- Ransomware Deployment
  - Change login credentials and block ATC startup process.
- All-Direction Green Lights
  - Transient avoidance tactic helps to make green light flashing.
  - Increase the flicker frequency to introduce optical illusion.



The Recurrent Pulse Detection (RPD) looks for voltage leaks lasting 1ms to 200ms and triggers a conflict state if a certain criteria level is met.

- In a certain time window, the duration of green light is cumulative.
- In practice, 24ms green light on-time with 17ms off-time will bypass the RPD.

イロト 不得 トイヨト イヨト 二日

#### All-Direction Green Lights



Understanding the Security of Traffic Signal Infrastructure, DIMVA 19



- Avoid default password and master key.
- The design should put security in mind.
  - Secure communication
  - Encrypted configuration
- Open access to the related software and specification with strict verification.

イロン 不同 とくほう イロン

#### Outline



- Introduction
- Background
- Security Analysis
- Attacks and Mitigations
- Conclusion

æ

・ロト ・四ト ・ヨト ・ヨト

#### Conclusion



- We present a comprehensive vulnerability analysis of the traffic signal system and identify a number of vulnerabilities.
- Attackers can conduct a variety of attacks including all-direction green lights to the traffic system.
- More attention should be paid to the security threats in the transportation community.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

#### References I



- [1] C. Cerrudo, "Hacking US (and UK, Australia, France, etc.) traffic control systems," 2014.
- [2] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in <u>Proceedings of 25th Network and Distributed System Security</u> Symposium (NDSS'18), 2018.
- [3] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in <u>Proceedings of the 8th USENIX Workshop on Offensive Technologies</u> (WOOT'14), 2014.
- [4] Shodan, "Search engine for Internet-connected devices," https://www.shodan.io/.

イロン 不同 とくほう イロン

Thank you!



# Questions?

 $\{ zhenyu.ning \} @wayne.edu \\$ 



http://compass.cs.wayne.edu

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

# **Backup Slides**

Understanding the Security of Traffic Signal Infrastructure, DIMVA 19

3

ヘロン 人間 とくほと 人ほとう

#### Cabinet Standards



- The TS-2 Cabinet Standard was initially commissioned by National Electrical Manufacturers Association (NEMA) in 1998.
  - A replacement of NEMA TS-1 standard.
  - Using serial communication to replace hardwired I/O.
- The ITS Cabinet Standard is designed to supersede the NEMA TS-2 standard.
  - Published by American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), and NEMA.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

#### **Cabinet Standards**





3

・ロト ・回ト ・ヨト ・ヨト

#### Security Analysis



How to attack the traffic signal system?

э

・ロト ・四ト ・ヨト ・ヨト



According to the municipality officials,

- Due to the geography that must be covered, the deployed traffic network are generally linear in communication flows.
- Redundant protocols are not used due to extra cost of additional equipment.
- Troubleshooting process of the traffic system mainly focus on the down point.

< ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

#### **Diversionary Tactic**





э