Emergency Fuel Rationing system using RFID Smart Cards

Noor Ahmed Khudhur

Email: noorea04@yahoo.com

Abstract

Rationing is a commonly used solution for shortages of resources and goods that are vital for the citizens of a country. This paper identifies some common approaches and policies used in rationing as well asrisks that associated to suggesta system for rationing fuelwhichcan work efficiently. Subsequently, addressing all possible security risks and their solutions. The system should theoretically be applicable in emergency situations, requiring less than three months to implement at a low cost and minimal changes to infrastructure.

Keywords: Rationing, Smart-card, authentication, RFID, Security, Risk management.

1. Introduction

Shortages of resources often lead to significant rise in prices even up to 300%, leading governments to interfere and protect consumers by taxes, controlling prices, rationing or discounts [1].A Rationing system limits the acquisition of Commodities equally among citizens, ensuring that everyone entitled to goods can get their fair share [2]. Rationing has been historically used for food, water, energy, and other resources that are considered essential. In the past few years, petrol levels declined around the world, most countries may find themselves in need of rationing systems for fuel or risk economical breakdown [2].

1.1 Case Studies

A.   Odd-even system: This system has been commonly used in emergency situations in many countries including Iraq in recent years, however a well-documented recent and successful example was the 2012 hurricane Sandy crisis in the US, as some pipelines were damaged, 67% of gas stations were compromised in the New York-New Jersey area, then took two weeks to recover. To face this emergency, the US deployed the odd-even system [3]. A similar system had been applied in Iraq and other countries during crisis time, using car numbers as a guideline. Cars with odd numbered plates received fuel rations on odd numbered days, a car with an even numbered plate however, got fuel days of even numbers. [4]. This system is ideal for emergencies where there is little time available for employing something more substantial, yet, it lacks the ability to deal with complex special cases and prevention of black market activities.

B.   Iran Smartcard : The fuel rationing system in Iran was introduced in 2007, as a solution to the constantly rising prices of petrol, and to get the country to a more efficient fuel consumption level. This was accomplished by fixing prices all year long [5][6]. Every vehicle was issued a smartcard to distribute rations, while gas stations were equipped with card readers. The system would continue to function even if the network is down. Counterfeit cards, when discovered, are blocked within 24 hours. The Iranian rationing system did effectively reduce fuel utilization and increase the public awareness, thus it's considered as a successful model, one reason for that is the advertising and preparation done before the launch, that allowed the public to understand the system and accept it [7]. This

system offers a framework, a look at what a rationing system can accomplish and highlights the importance of advertising to avoid confusion. It is quite similar to the system this paper is aiming to develop; we are looking for a more versatile system that can be deployed within three months in case of emergency.

1.2 . Approaches and Policies

The case studies in this paper, as well as others, such as the World War II rationing of food or the 1970s petrol crisis in western countries, offer three general models for rationing:

A. **Controlled or Fixed pricing**: Governments can control the supply of goods by regulating prices. A fixed, usually low, price or range of prices is imposed on all suppliers if they want to deal with a particular commodity that is needed this way theoretically ensure equal opportunities, and is commonly used for regulating medicine and healthcare in some countries such as the UK.

B. **Time based :**In this model rations are distributed on timely bases, meaning a ration is earned daily, weekly, or monthly. One example of this is the Odd-even system mentioned previously, as rations are received every-other-day. Another example is the food rationing system employed in Iraq and Cuba, which is a monthly distribution system.

C. **Quantity based:** This model administers the quantities of a certain commodity that a person or a family is allowed, sometimes given free or at reasonable prices making it accessible to everyone. This model is used for essential resources such as food and water, it is often used in poor areas of refugee camps, it was also heavily employed during World War I & II.

These models, on their own, are often used as reaction to a crisis, such as war or natural disasters. A more efficient and regulated system could use two or all three combined to achieve better results.

1.3 Techniques for Implementation
1.3.1 Coupons

In the early twentieth century, governments relied on plain paper IDs, with signatures, serial numbers and later photographs for identifying individuals [8] thus; early rationing systems utilized paper coupons to identify a citizen's right to rations. Security measures were limited, that included serial numbers and signatures, sometimes with other visual features such as watermarks or deliberate spelling mistakes.

1.3.2 Automatic Identification

With recent technological advancement, Automatic identification or Auto-ID is starting to replace tokens and coupons used previously in rationing systems. There are different identification technologies that need to be studied before determining the most appropriate one for any given situation. Table (1) lists commonly used Auto-ID systems along with a breakdown of their advantages and disadvantages.

As we seen from Table (1), every technology has its difficulties and advantages; different methods are better suited for different applications. For example, Biometrics is often used for high security locations as a means of access control, but rarely in regular public systems where it is too expensive and time consuming. Barcodes on the other hand are widely accessible and used regularly by shop owners, but are unsuited for any sort of reliable authentication. The large scope of rationing, and the importance of making the system secure but affordable and accessible at the same time, means we are more likely to consider Smartcards or RFID, Which are highly secure, commonly used in authentication, and are not complicated or expensive. Smartcards are generally considered more secure, but RFID are convenient and faster to read which makes them more ideal for the system as they help reduce long queues.

2. The Proposed Policy

The suggested policy is based on both time and quantity rationing, employing smart RFID cards. It is designed specifically to combat black market and corruption, based on the following guidelines: Cardholders are divided into 7 categories, each user group would have a distinct Application process, fuel allotment based on their needs and numbers, as well as Different guidelines and rules. The cards would have the same design and security features, but differ in color to easily represent the different groups. The 7 categories are shown in Table 2.

Table 1,

Auto -ID	Description	Advantages	Disadvantages
Barcodes	A pattern of lines and spaces (squares and spaces in QR Barcode) interpreted by a machine to conduct information.	• Easy to print, with readers commonly available. • Inexpensive.	• Low capacity • Lack of resilience and durability. • Can be copied or modified easily.
OCR: Optical character recognition	Simple plain text that can be interpreted by text recognition software.	• The Cards require no special technology, traditional printers only. • Fast.	• Complex and unreliable software. • Expensive reading devices. • Lack of resilience and durability
Magnetic Stripes	A card that holds a magnetic tape appearing as a thick black line.	• Inexpensive.	• Can be copied or modified easily. • Unreliable, prone to failure. • Lack of resilience and durability
Smartcard	A card that stores information in a memory, it's contact based, i.e must be inserted into a reading device for authentication	• Can be designed to prevent unwanted access or alteration. • Hard to copy or forge.	• Readers are expensive and require constant maintenance. • Lack of resilience and durability
RFID: Radio Frequency ID	A card that can store information and communicate it using Radio frequency, thus no physical contact is required between card and reader.	• Highly resilient and unaffected by outside elements. • Fast	• Might cause health issues, if used in long range. • Expensive • Frequency Collision when multiple cards are used in the same range.
Biometrics	Unique and measurable human features, like voice, fingerprints, DNA, or Retina scan.	• Theoretically impossible to copy or forge. • Highly resilient and unaffected by outside elements.	• Expensive • Complicated registration process • The matching process requires huge databases and high processing power.

Commonly used Auto-IDs (compiled by researcher [9][10][11][12][13]).

*Some references use the term "smart card" for any type of card with any sort of memory, in this paper it is used to refer more specifically to cards with a memory chip, the technology often used in credit cards.

Table 2,
The seven categories suggested for rationing (The estimated number of cars is, just in example based on latest statistics about cars in Iraq [14].)

Category	Type of Users/Cars	Estimated number of cars*	Suggested fees (in dollars)			How to apply
			issue	renew	replace	
Blue	Personal cars	4.5-5.5 Million	5$	3$	10$	online
Red	Government cars	67-94 Thousand	free	free	20$	Through department
black	Transport (buses, taxis)	1-1.5 million	5$	5$	10$	Online
Gold	Company Cars, Light/Heavy goods vehicles	1 thousand	10$	8$	20$	Through company
Silver	Visitors, Foreigners	>1 thousand	10$	N/A	10$	online
purple	Multiple Cars	>1 thousand	15$	10$	25$	At office
Green	Other uses (ex. Generators)	0.5-1 million	5$	5$	10$	At office

- Each user must apply and pay a small fee for a card that is valid for 1 year, after which the card must be renewed if the program is still in effect.
- Vehicles will be registered by plate numbers, as it is the most suitable option for category selection. The green category (for fuel uses other than cars) will have to be issued on case-by-case bases.
- The amount of fuel given a user should be determined a specialists to ensure it is enough for the every users' needs.
- Ration sizes will not be fixed rather will be set as an equation combing the category and car type, thus the rationing can be adjusted or cancelled and the cards would continue to work properly, it will also make it harder to tamper with the system.
- Card readers will be employed at gas stations, then used by the station operators to read the cards and know the ration size and when a user is due one.
- All other procedures will continue as usual.
- The system should provide for all cost internally, which means the fees paid for the cards should go to staffing, purchasing of equipment and advertisement necessary for the project. Ideally, no extra government spending would be needed for the program, even if an external company is contracted.
- The time between rations is also limited, once a user receives the ration, the card is disabled until it is time for another ration, this way users can't deceive operators or conspire with them receive more rations than they are allowed.

2.1 Parts of the System

The system has three critical parts for operation:

A. Database: the system requires an accurate, up-to-date database, large enough to hold all users information.

B. Operators: gas station workers are responsible for running the distribution of rations, thus they are critical to the system.

C. Cards: as the system authentication token, the system relies on the authenticity of the cards to work properly.

3. Risks, Threats and Mitigation

- There are common risk factors and threats associated with all rationing system and online systems such as the one proposed, in this section we will look at these common risks and discuss methods of mitigation that could be implemented.

3.1 Insider Threat

Insider threat is a disruption to a processes introduced by a person, or group of people with legal access to the system, such as employees, mangers, suppliers or contractors...etc. if it is intentional, it is commonly known as corruption [15]. CPNI report [16] listed some of the motivations for insiders to break the law, financial gain was on the top of the list, followed by: ideologies, desire for appreciation, outsider loyalties and vengeance. Some insider threats though, are not intentional, as people can simply make mistakes if they lack the experience or training necessary [15].

In our proposed system, the insider threat is extremely high, because of the dependence on registration employees for correct issue of cards as well as station workers for honest distribution of fuel. Some precautions can lessen this threat or reduce its effects:

- Registration employees have to go through background checks and interviews, to ensure they have no past criminal records or questionable affiliations.
- Matching every application with the national car registration database - at the directorate of traffic department- this limits the employee's ability of issuing false cards.
- For station operators, some training and guidelines are required to reduce errors, the system interface should also simple and straightforward, clearly displaying the needed information.
- The card readers usually have the ability to compile a list of cards used, so by using this list, the amount of fuel that supposedly been dispensed for one day can be calculated then matched with the actual fuel levels, highlighting any discrepancy that needs further investigation.
- A mechanism must be implemented to allow users and operators to report any suspicious behaviour, or faults in the system they notice.

3.2 Counterfeiting

Counterfeiting is the creation of fake documents or the replication or modification of legitimate ones [17]. It is a major threat for systems that use an authentication process for identifying users. A number of anti-counterfeiting measures have developed over the years, they are however not perfect and instead of making counterfeiting impossible, these measures simply make it not worth the effort, i.e they make the cost of making a counterfeit document exceeds the cost to be gained from breaking the system. [18] For this reason, the intensity of anti-counterfeiting is proportional to the value of the system itself, so in our case, the counterfeit measures are medium levels, as the cost of creating a secure, hard to replicate card, should be in line with the cost of fuel rations themselves. The system will have a combination of security features known as Overt, Covert and Forensics. Thus, the Cards are equipped with the following features:

- Overt (easily noticeable by any user or operator): Hologram, Watermark.
- Covert (requires a device or special light to detect):, UV- fluorescent image, Microprinting.
- Forensics (used by specialists after confiscation to study the counterfeit): A magnetic Stripe, containing the user name, plate number, issue and category type, this is not used in authentication, only as a match with original chip.
- Read/write RFID cards provide authentication, read-only do not offer authentication [9].
- Derived key encryption: this method of encryption derives the decryption key from cards' serial numbers, using a unified secret algorithm [9]. If one key is compromised, it does not mean all of them are. Figure 1 shows a template for the card suggested with all the security features.
- A template for the card suggested is shown in Figure 1, highlighting the security features required. It's also important to raise awareness about fraudulent documents and how to detect them.
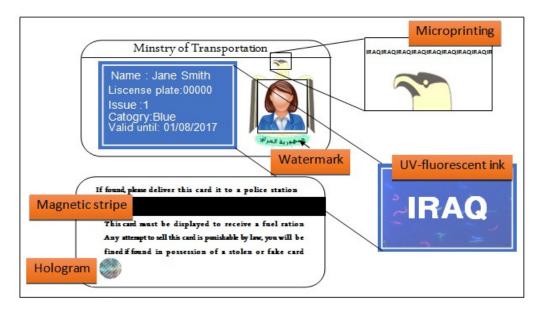

Fig. 1. A template for the card suggested.

3.3. System Failure

A system failure is the event of a system failing to function as intended under all conditions at all times [19]. Rationing systems are prone to failures due to their wide scope of application and their nature as emergency measures instead of well thought-out plans. The huge numbers and the diversity of users create all kinds of exceptions and puts pressure on the performance. Urgency cause lack of proper debugging or a trial period, as well as the possibility of going over budget or cutting corners, all these factors increase the chances of system failure [19].

Stoneburner, et.al [20] gave six possible responses for risk management: Assumption, Avoidance, planning, limitation, transference or

research. For a rationing system, complete avoidance is unattainable, so is transference, thus we must accept the possibility of system failure, instead we need a recovery plan and ways to limit the affects of one system failing on any other. The following guidelines could lessen the effects of potential system failure:

- Back up the database every day. Update it only once per day, before backup, thus if the data is damaged during update, there is always a copy.
- Card readers are ideally equipped to keep a record of all transactions. In the case of the system going offline, operators are capable of authorizing sales, this way they must visually identify the card, and while it is possible to take some small advantage of such system failure, the risks are manageable and preferable to halting all sales, it is also possible to detect any fraud once the system is back online and take action.
- Provide multiple readers per station, if one is down, operators can replace it until it is fixed.

3.4 Hacking the Registration System

In the case of a system hack, it's becomes possible to issue fake or duplicate card or change details like the category, if this was done on a small scale it could possibly go un-noticed, thus the some measures are suggested to reduce the likelihood of successfully hacking the system :

- Implement SSL, use anti-SQL injection techniques, firewalls, and input control, particularly on online application forms.
- Match entries of the application form with the national vehicle-licensing database, refuse the application if it didn't match.
- Plate numbers are unique, so a simple check can ensure they are never repeated.
- Send the card to the registered or work address; or require proof of identity before handing it out to the user, in case the form was filled by someone, claiming to be someone else.
- In the case of someone being unable to apply because of a repeated plate number, allow them to visit a registration office, once their ownership of the car is proven, the old card is disabled and a new one is issued.

3.5   Hacking the System Database

In the case of database hack, rations for any number of people could be manipulated to increase rations or reduce waiting period, the following measures are suggested to lessen the affects of a potential database hack:

- Limit the functionality of readers, allow them to read values and alert the system, this will automatically set the value of the variable 'last use' to the current date. All other values should be locked, read-only values and.
- The database is updated once per day at night to add new cards or remove reported ones, this will mean one-day waiting period before a new card is usable, and a one-day window for fraudulent cards to take rations, which is negligible. After update, the database is backed ups. So the next day, a comparison between the back up and the database before update should reveal any unauthorized changes.
- The ration size and waiting period between rations is not identified as a fixed value within database but is computed from other values, such as category and vehicle type (ex. 'bus', 'coach' or 'car').This way, a simple number change is not possible instead the only way to change a ration size or waiting period is changing the algorithm that calculate it, which can be easily monitored and noticed.

3.6 Problems   with   the   Transmission: Listening,   Interference   and   Health Concerns

The RFID technology is contactless, meaning a card not inserted in the reader device but is transmitting information wirelessly through air, this introduces a set of problems, such as outsiders listening in on the transmission, compromising privacy of the users, also when multiple card are used near each other the signals may interfere confusing the reader device and disrupting the process. One more concern that rose up in recent years is the effect of transmission on safety, and if constant exposure to the signal can cause health issue, the issues listed above are illustrated in Figure 2.
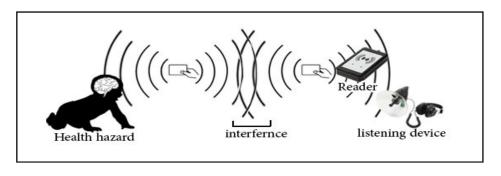
Fig. 2. Risks caused by RFID wireless transmission.

One way to limit all the previous concerns is using Passive Ultra high frequency transmission, making the range the transmission shorter (around 1 meter) complicating listening and reducing interference greatly, the use of passive transmission as well as the lower range will reduce all health and safety concerns.

Other ways to protect privacy is using encryption between the reader and the card (derived key encryption), as well as between the reader and the central system and Limiting the Information stored on the card not to include personal data.

3.7. Tampering with Readers

All readers should be located inside secure buildings when not in use, along with regular inspection for the devices, operators would be held responsible in the event of failing to report any stolen or damaged devices.

3.8 Lost or Stolen Cards

Cards are the method of authentication, it is important that if they are stolen or lost, that we have good measures for replacing them without creating redundancy, on the other hand, if someone suspect that their card has been duplicated there should be a way to resolve the situation. The following measures are suggested

- A reporting system is necessary to report any missing cards, or if a person is being rejected by the system and suspects his card has been compromised somehow.
- Cards are disabled after use, until the waiting period between rations has passed; a missing card reported early could only be used few times, limiting the damage.
- When a card is reported missing, it must be disabled before a new one is issued, and extra fees are charged for re-issue this discourages

people from making false claims or being careless.

3.9. Selling Cards or Unneeded Shares

There is always a risk of people selling their cards or any rations they do not need, the mitigation process is policy based, not technological, and it varies between personal cars and company, or government cars.

A. Private use (Blue, black, purple, green):
- Offering a discount for next year rations for a percentage of fuel saved, for example, if a user is assigned 52 rations per year, yet received 46 or less, that's 10% saving, making them eligible for a discount . This will discourage selling rations as well as encourage reasonable fuel consumption.
- Any person discovered to have sold or bought a card, will be liable to a fine. It is easy to discover sold cards since they contain a picture and plate numbers.

B. Government and company cars (Red, Gold, Black):
- The old card must be submitted for renewal, failing to present it makes the owner liable to a fine. A heavier punishment must be set for cardholders caught selling a card.

4. Implementation
4.1 Database

The system database should be simple and straight forward, most items in the database would be read only, and inserted directly from the vehicle registration database rather than manually, while the values of the time stamp and permission set to be automatically calculated by the system.

Table 3 shows the fields of the proposed database and their data types.

Note that the ration size is not fixed, rather it is calculated by an algorithm that uses both the category vehicle type to calculate, the same is true for the duration, this is meant to give the system some flexibility so the rations can be adjusted depending on supply and demand, it is also a security measure because if the system was hacked and a single number is changed it may not be noticeable, but a change in the algorithm would be discovered immediately.

Table 3,
The system database.

Field	Type
Serial number	PK
Name	Read Only
Category	Read Only
Plate number	Read Only
Vehicle type	Read Only
Time stamp of last use	Automatic
Time for next allowed use	Automatic
Permission(Boolean)	Automatic

4.2. Equipment

Every gas station is provided with a number of short-range RFID readers, compatible with the cards. A good practice is to have the supplier company do the installation or supervise it. All readers must:
- Have derived key decryption, for contact with the card.
- Use encryption for contact with the central system.

- Be equipped with clear display screens that show all the required information to dispense fuel.
- Have a memory space large enough to record transactions up to a month
- Can send daily records to the central system, to be compared with the fuel dispensed from station.

To have all These requirements, the readers might have to be developed specifically, however, it's a common practice for developer companies to offer customizable RFID readers, and while the extra features will have added cost, but it's necessary for risk management.

4.3 Delivery plan

As an emergency system, it is designed to have minimum changes in infrastructure and must not disrupt regular procedures during implementation; it does however require preparation that includes hiring registration workers, building the system, and purchase of devices as well as any possible contracts if the implementation was to be fully or partially outsourced. There should also be an adjustment and training period, where cards are distributed to users but no ration is applicable yet. This will be very useful in finding bugs or required adjustment to the program, before it goes into full operation. Another suggestion is to have a promotional campaign throughout the project to get the public informed. Figure 3 shows the suggested 3 months plan for the implementation of the system.
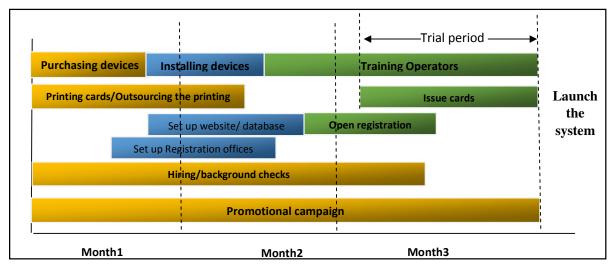

Fig. 3. Delivery plan.

5. Conclusion

This paper suggested a system for fuel rationing that could be applied within three months ideally. The paper suggest the use of RFID cards for authentication, and a 7 category allotment system to account for the needs of the public, the system proposed accounts for the risks associated with such a system and their mitigation. However, it is sufficient for emergency and temporary use only. A more durable system would require case studies, interviews or surveys among affected parties as well detailed cost analysis.

6. References

[1] R. H. Bezdek and W. B. Taylor, "Allocating petroleum products during oil supply disruptions.," Science, vol. 212, no. 4501, pp. 1357–63, Jun. 1981.

[2] D. Fleming and S. Chamberlin, "TEQs (Tradable Energy Quotas):A Policy Framework for Peak Oil and Climate Change," 2011.

[3] S. H. Halpin, "Home Rule in NJ and Hurricane Sandy Recovery," in American Society for Public Administration 2013 Annual Conference, 2013.

[4] S. Kaufman, C. Qing, N. Levenson, and M. Hanson, "Transportation During and After Hurricane Sandy," 2012.

[5] D. M. Guillaume, R. Zytek, and M. Reza Farzin, "Iran: The Chronicles of the Subsidy Reform," 2011.

[6] H. Rahdari, M. Zargarzadeh, H. Nozari, and L. Soltani, "Gasoline Rationing Plan in Iran : A Symptomatic Solution," in 27th International Conference of the System Dynamics Society, 2009.

[7] P. Hanafizadeh, Z. Navardi, and J. BamdadSoofi, "An attitude study on the environmental effects of rationing petrol in Tehran," Energy Policy, vol. 38, no. 11, pp. 6830–6848, Nov. 2010.

[8] K. Michael and M. G. Michael, "Historical Lessons on ID Technology and the Consequences of an Unchecked Trajectory," Prometheus, vol. 24, no. 4, pp. 365–377, Dec. 2006.

[9] K. Finkernzeller, RFID Handbook, 3ed ed. Wiley, 2010.

[10] Keith E. Mayes and K. Markantonakis, Smart Cards, Tokens, Security and Applications. 2008.

[11] R. Bolle, Guide to Biometrics. Springer, 2004.

[12] R. Bhasker and Raj, Bar Codes. Tata McGraw-Hill Education, 2001.

[13] N. Bartneck, V. Klass, and H. Schoenherr, optemizing processes with RFID and Auto-ID. Publics Publishing, 2009.

[14] Cosit.gov.iq,'Central statistical organization Iraq', 2013. [Online]. Available: http://www.cosit.gov.iq/ar/2013-03-29-08-38-49. [Accessed: 10- Jun- 2015].

[15] S. J. Stolfo, S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, and S. Smith, Insider Attack and Cyber Security. 2008.

[16] CPNI, "CPNI INSIDER DATA COLLECTION STUDY REPORT OF MAIN FINDINGS," 2013.

[17] CONSILIUM, "Technical terms related to security features and to security documents in general." [Online]. Available: http://prado.consilium.europa.eu/en/glossary popup.html.

[18] CardLogix, "Graphics and Security: printing guide," 2011.

[19] K. T. Yeo, "Critical failure factors in information system projects," Int. J. Proj. Manag., vol. 20, no. 3, pp. 241–246, Apr. 2002.

[20] G. Stoneburner, A. Goguen, and and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," 2002.

خطة طوارئ لتوزيع الوقود باستخدام بطاقات RFID الذكية

نور احمد خضر

البريد الالكتروني: noorea04@yahoo.com

الخلاصة

نظم التقنين هي احد اكثر الطرائق الشائعة للتعامل مع نقص الموارد و البضائع الضرورية للمواطنين، في هذا البحث سنتعرف على هذه النظم وطرائق تطبيقها والاليات والمخاطر المصاحبة لها، ثم نقوم بتطوير نظام لتوزيع الوقود يمكن تطبيقه في العراق، مع مراعاة الخروقات الممكن استغلال النظام من خلالها وكيفية معالجتها، ويشترط بالنظام ان يكون لحالات الطواريء ويمكن تطبيقه خلال ثلاثه اشهر بكلفة واطئة وبدون تغييرات جذرية في البنى التحتية.