Journal of Uncertain Systems
Vol.10, No.1, pp.57-60, 2016
Online at: www.jus.org.uk

How to Distribute Security Efforts Between Different Units of an Industrial System

Beverly Rivera[1],*; Francisco Zapata[2]

[1] *Computational Science Program, University of Texas at El Paso, El Paso, TX 79968, USA*

[2] *Department of Industrial, Manufacturing, and Systems Engineering*
University of Texas at El Paso, El Paso, TX 79968, USA

Received 1 April 2015; Revised 12 June 2015

Abstract

In an industrial system, it is important to protect both the industrial units – the ones that actually manufacture new objects or generate energy – *and* the auxiliary units that are necessary for the industrial units to function. Since security resources are limited, it it important to properly distribute security efforts between different units of the industrial system. In this paper, we show that the existing method of distributing security effort sometimes leads to counter-intuitive effort distributions, and we describe a new method for distributing effort which is in better accordance with our intuition.

Keywords: industrial security, distributing security effort

1 How to Distribute Security Efforts Between Different Units of an Industrial System: Formulation of the Problem

What is an industrial system. The main purpose of an industrial system is to generate something new:

- manufacturing systems generate new objects,
- power systems generate electricity, etc.

From this viewpoint, the main part of an industrial system are the *industrial units* that perform the corresponding generation.

Some industrial systems consist only of industrial units. However, most industrial systems, in addition to industrial units, also have additional *auxiliary* units that provide support for such systems. For example:

- a power-generating unit may be controlled by a separate controller unit.
- A manufacturing units may get its power from a separate auxiliary power-supply unit, which, in its turn, may be controlled by a separate controller unit.

The relation between different units may be complicated; for example:

- the same power-generating unit may supply several industrial units;
- vice versa, an industrial unit may be supplied by several power-generating units.

One of the reasons for this complexity is to provide duplication and thus, an addition reliability: if two power units supply the same industrial unit, then, even when one of these power units break down, the industrial unit will still be supplied by another power unit and will, thus, be able to function.

The dependence between different units can be described by a layered graph:

*Corresponding author.
Emails: barivera1975@gmail.com (B. Rivera), fazg74@gmailcom (F. Zapata).

- The first layer of this graph is formed by vertices that represent industrial units, i.e., units that perform the desired generation.
- The second layer is formed by vertices that represent auxiliary units which directly influence the units of the first layer. This influence is described by edges that go from an auxiliary unit to the corresponding industrial unit.
- If needed, we can have the third layer, which is formed by auxiliary units:
  - that do not directly influence industrial units (units from the first layer),
  - but that directly influence units from the second layer, etc.

Need to distribute security efforts. The main objective of industrial system security is to prevent the adversary from disrupting the functioning of the system. Traditionally, most disruptions occurred on the level of industrial units. As a result, these units are usually heavily protected.

Experts know how to estimate relative importance of different industrial units and thus, how to distribute security efforts between these units.

However, if only industrial units are heavily protected, then the adversary can potentially disrupt the system by launching a cyber-attack on one of its (less protected) auxiliary units. Thus, we:

- no only need to protect the industrial units themselves,
- we also need to protect all the auxiliary units in an industrial system.

Our resources are limited. So, we need to reasonably distribute these limited resources between different units. The need to decide how to best distribute our efforts between different units was formulated, e.g., in [1, 3].

How efforts are distributed now. One of the most widely used effort distribution schemes is based on analyzing *critical paths*, i.e., minimal subsets of units whose disruption prevents the system from functioning normally. The recommendation is to distribute the effort to each unit proportionally to the number of critical paths containing this unit; see, e.g., [2].

In most practical situations, the currently used approach leads to reasonable distribution of security efforts.

What we do in this paper. In this paper, we show that the existing method of distributing security efforts has a limitation: namely, in some situations, the resulting distribution of efforts is not the most effective one. We also propose a new method of distributing efforts which is free of this limitation.

2 How to Distribute Security Efforts Between Different Units of an Industrial System: Limitations of the Existing Approach

Example. To illustrate the limitations of the current method of distributing security efforts, let us consider a simple industrial system with two equally important industrial units A and B:

- the unit A has ten duplicating controllers $a_1, \ldots, a_{10}$, while
- the unit B has a single controller b.

For a normal functioning of a plant, we need both industrial units to function. Each industrial unit, in its turn, needs to have at least one related functioning controller to function normally.

Let us apply the currently used methodology to this example. According to the currently used methodology, the security effort concentrated on each auxiliary unit should be proportional to the number of critical paths containing this unit. A critical path is the smallest set of units disrupting which will disrupt the system.

The minimal disruption means that we either incapacitate the first industrial unit or the second one but not both. To incapacitate the first industrial unit, we need:

- either to directly disrupt this unit A
- or to disrupt all ten controllers corresponding to this unit; indeed:
  - if at least one of them is not disrupted,
  - the industrial unit A will still be able to function.

Thus, in this case, we have two minimal sets (= critical paths):

$$\{A\} \text{ and } \{a_1, \ldots, a_{10}\}.$$

Similarly, to incapacitate the second industrial unit, we need:

- either to disrupt this unit B
- or to disrupt is controller b.

So, in this case, we also have two critical sets:

$$\{B\} \text{ and } \{b\}.$$

In this case, for each of the 11 controllers $a_1, \ldots, a_{10}$, and b, there is exactly one critical path containing this controller. Thus, according to the currently used methodology, we should assign the exact same amount of security effort to all 11 controllers.

The resulting distribution of efforts is not very efficient. In the above arrangement, we spend 10 times more efforts to protect controllers related to the industrial unit A than to protect a controller related to the industrial unit B. Thus, overall, the controllers related to the unit A will be much more heavily guarded than the controller related to unit B. However, from the common sense viewpoint, it should be the other way around: the duplication of A's controllers provides additional security for the unit A, so the B-related controller should be more heavily protected.

3 How to Distribute Security Efforts Between Different Units of an Industrial System: A New Proposal

Need for a new method for distributing security efforts. The above example shows that the existing method of distributing security efforts is not always reasonable, and thus, a new method is needed.

In this section, we will show that a natural analysis of the corresponding problem leads to such a new method.

Simplest case: one industrial unit, one auxiliary unit. Let us start with the simplest situation, when we have one industrial unit with weight w, and this unit is controlled by a single controller.

In this case, the security importance (= vulnerability) of the controller is approximately the same as the object itself.

It is reasonable to argue that the security importance of the controller is probably slightly smaller than the security importance of the original industrial unit: after all, it is easier for the adversary to destroy the object itself then to find a way to do it indirectly, by hacking into a controller.

So, let us allocate, in this case, the effort $a \cdot w$ to the controller, where $a < 1$ and a is close to 1.

Next case: one industrial unit, several duplicating auxiliary units. Let us now consider a slightly more complex situation, when we have several ($k > 1$) auxiliary units supplying the same industrial unit. For example, we may have several controllers controlling the same industrial unit.

In this case, it is reasonable to require that the overall effort to protect these several (k) auxiliary units should be the same as the effort of protecting a single auxiliary unit in the previous case. Thus, to find the effort corresponding to each auxiliary unit, we need to divide the single-auxiliary effort $a \cdot w$ equally between all k auxiliary units. As a result, each auxiliary unit gets the effort

$$\frac{a \cdot w}{k}.$$

What if an auxiliary unit supports several industrial units? If an auxiliary unit supports several industrial units, then, to find the security effort reasonable for protecting this auxiliary unit, we simply add the efforts coming from several industrial units that it supplies.

For example, if:

- an auxiliary unit is one of the 3 units supporting an industrial unit 1 (whose effort is w_1) and
- this same auxiliary unit is also one of the two auxiliary units supplying industrial unit 2 (whose effort is w_2),

then the overall effort needed to protect this auxiliary unit should be equal to

$$\frac{a \cdot w_1}{3} + \frac{a \cdot w_2}{2}.$$

This takes care of the second-layer units. The above description enables us to assign efforts to all the auxiliary efforts from the second layer.

Example. In the above example, we have two industrial units A and B of the same effort $w_A = w_B = w$, in which:

- the industrial unit A is supported by $k = 10$ auxiliary units $a_1, \ldots, a_n$, while
- the industrial unit B is supported by only one ($k = 1$) auxiliary unit b.

In this example, the procedure that we have just described leads to the following distribution of security efforts:

- to each unit a_i, we assign security effort $(a \cdot w)/10$, while
- to the unit b, we assign ten times larger security effort $a \cdot w$.

Here, the overall security effort for A-related auxiliary units is the same as the overall security effort for protecting all B-related auxiliary units.

This makes much more sense than the current recommendation (described in the previous section), according to which A-related auxiliary units get ten time more effort than B-related ones.

How to distribute efforts: general case. So far, we have only described how to assign efforts to the units from the second layer.

However, if there are units in the third, etc., layers, the same idea can be used to assign effort to these units. Namely, if an auxiliary unit from the second layer – a unit to which we assigned effort w – is supported by one or several ($k \geq 1$) units from the third layer, then we assign, to each of these units, the effort $(a \cdot w)/k$. If a unit u from the third layer supports several units from the second layer, then, to compute the effort for this unit u, we add up the values coming from all these second-layer units.

This way, we assign the effort to all the units in the third layer. If the corresponding graph has a fourth layer, then we can use the same idea to propagate the efforts from the third layer to to this fourth layer, etc.

Acknowledgments

The authors are thankful to Dr. Irbis Gallegos for formulation of the problem and for valuable discussions.

References

[1] de la Villa Jaén, A., and A. Gómez-Expósito, Implicitly constrained substation model for state estimation, *IEEE Transactions on Power Systems*, vol.17, no.3, pp.850–856, 2002.

[2] Mohajerani, Z., Farzan, F., Jafary, M., Lu, Y., Wei, D., Kalenchits, N., Boyer, B., Muller, M., and P. Skare, Cyber-related risk assessment and critical asset identification within the power grid, *Proceedings of the 2010 IEEE Transmission and Distribution Conference and Exposition*, pp.1–4, 2010.

[3] Wei, D., Lu, Y., Jafari, M., Rohde, K., Muller, M., Turke, A., Skare, P., and C. Sastry, *An Investigation of Potential Cyber Attacks and Their Impacts on the Power Grid*, Technical Report, Siemens Corporate Research, 2008.