Chapter 4

Calculation of system reliability metrics

This document is basically a motivated by chapter 4-8 in the textbook *Reliability of Safety-Critical Systems* by Marvin Rausand.

4.1 Introduction

In this chapter we introduce methods and approaches for calculation of the following system reliability metrics

- PFD = Probability of Failure on Demand
- PFH = Probability of Failure per Hour
- STR = Spurious Trip Rate

Note that these terms are time dependent and are changing during a proof test interval. The objective is usually to find average values during the proof test interval. When these terms are given with out any time dependency, it is implicitly assumed that we are presenting average value. In same cases we also use the subscript "avg" to emphasize that the value is the average value during one proof test interval

4.2 PFD calculations for systems

To obtain PFD for a system we may follow the following procedure:

1. Find PFD for the system as a function of t in an interval, i.e., $0 \leqslant t \leqslant \tau$, and denote the result PFD(t)
2. To obtain PFD(t) we often utilize the system survivor function, say $R(t)$

3. Find the average PFD(t) by integration: PFD $= \frac{1}{\tau}\int_0^\tau \text{PFD}(t)\,dt = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,dt$

The classical example is one component proof tested at point of times τ,2τ,3τ,..., and time to failure is exponentially distributed, i.e., $R(t) = e^{-\lambda t}$.

$$\text{PFD} = 1 - \frac{1}{\tau}\int_0^\tau R(t)dt = 1 - \frac{1}{\tau}\int_0^\tau e^{-\lambda t}dt = 1 + \frac{1}{\lambda\tau}\int_0^\tau -\lambda e^{-\lambda t}dt = 1 + \frac{1}{\lambda\tau}e^{-\lambda t}\Big|_0^\tau = \tag{4.1}$$

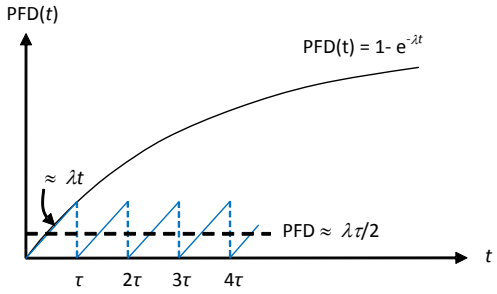
$$1 + \frac{1}{\lambda\tau}\left(e^{-\lambda\tau} - 1\right) \tag{4.2}$$

If $\lambda\tau$ is small, i.e., (<0.01) we utilize that $e^{-x} \approx 1 - x + x^2/2$, and inserting in the expression for PFD(t) yields:

$$\text{PFD} = 1 + \frac{1}{\lambda\tau}\left(e^{-\lambda\tau} - 1\right) \approx 1 + \frac{1}{\lambda\tau}\left(1 - \lambda\tau + (\lambda\tau)^2/2 - 1\right) = \lambda\tau/2 \tag{4.3}$$

Note that λ is the rate of DU-failures. In some presentations the notation λ_{DU} is used, but for simplicity we only use λ. In general we also need to add contribution of DD failures, but this is not further discussed in this presentation.

Another way to obtain the same result is to use that $e^{-x} \approx 1 - x$ for small x-values directly, hence we have that PFD(t) $= 1 - e^{-\lambda t} \approx \lambda t$ in an each proof test interval:



which yields PFD $\approx \lambda\tau/2$.

Such an argument we may also use for two identical components in parallel that are proof tested at the same time. The time dependent PFD of the two components is found by

$$\text{PFD}(t) = \text{PFD}_1(t) \cdot \text{PFD}_2(t) \approx (\lambda t)^2$$

yielding:

$$\text{PFD} = 1/\tau \int_0^\tau \text{PFD}_1(t) \cdot \text{PFD}_2(t)dt \approx 1/\tau \int_0^\tau (\lambda t)^2 dt = \frac{(\lambda\tau)^2}{3}$$

The PFDs of some *koon* systems of identical and independent components with constant failure rate λ and test interval τ are found to be:

$k \backslash n$	1	2	3	4
1	$\frac{\lambda\tau}{2}$	$\frac{(\lambda\tau)^2}{3}$	$\frac{(\lambda\tau)^3}{4}$	$\frac{(\lambda\tau)^4}{5}$
2	–	$\lambda\tau$	$(\lambda\tau)^2$	$(\lambda\tau)^3$
3	–	–	$\frac{3\lambda\tau}{2}$	$2(\lambda\tau)^2$
4	–	–	–	$2\lambda\tau$

The general formula for PFD is

$$\text{PFD} = \binom{n}{n-k+1} \frac{(\lambda\tau)^{n-k+1}}{n-k+2} \tag{4.4}$$

The argument for this formula is as follows. We have a $k\,oo\,n : G$ system corresponding to an $n-k+1\,oo\,n : F$ system. This means that if $n-k+1$ components are in a fault state, the system will be in a fault state. The minimal cut sets will all contain $n-k+1$ components, and there are $\binom{n}{n-k+1}$ such minimal cut sets. At time $t, 0 \le t < \tau$ the probability that one such cut set is in a fault state is $\text{PFD}_j(t) \approx (\lambda t)^{n-k+1}$ with an average $\text{PFD}_j = \frac{(\lambda\tau)^{n-k+1}}{n-k+2}$. Multiplying with the number of minimal cut sets gives the above formula.

4.2.1 Staggered Testing

Now, consider the case with the two components in a 1oo2 voting having the same λ and τ, but where the testing is not carried out simultaneously. The situation is illustrated in Figure 4.1.

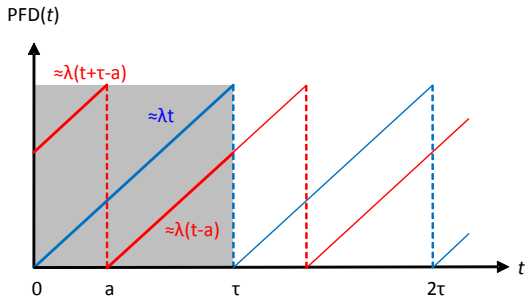


Figure 4.1: Staggered testing

Assuming that component 2 is tested at time (a) inside the test interval of component 1, it can

be shown that:

$$\text{PFD}(a) \approx \frac{(\lambda\tau)^2}{3}\left(1 - \frac{3a}{2\tau} + \frac{3a^2}{2\tau^2}\right) \tag{4.5}$$

PFD(a) attains its maximum value

$$\text{PFD}_{max} \approx \frac{(\lambda\tau)^2}{3} = \frac{4}{3} \cdot \frac{\lambda\tau}{2} \cdot \frac{\lambda\tau}{2} \tag{4.6}$$

when $a = 0$ or $a = \tau$, i.e., when the components are tested simultaneously.

PFD(a) attains its minimum value when $a = \tau/2$, i.e., when component 2 is tested in the middle of the test interval of component 1:

$$\text{PFD}_{min} \approx \frac{5}{8}\frac{(\lambda\tau)^2}{3} = \frac{5}{6} \cdot \frac{\lambda\tau}{2} \cdot \frac{\lambda\tau}{2} \tag{4.7}$$

Note that this minimum PFD is actually smaller than the PFD obtained when simply multiplying the average PFD values of the individual components. Compared to the case of simultaneous testing, we obtain a PFD reduction of 38% in the case of "optimal" testing. Hence, there is a great potential for improvement in the total PFD if components are tested at different times. This is exploited in staggered testing. Also note that the minimum value is obtained when $a = \tau/2$ for a 1oo2 system, for general configuration it is more complicated to set up the optimal staggered testing regime.

4.3 More about the test regime

There are three different test regimes that are considered

- Simultaneous testing, i.e., $a = 0$ in Figure 4.1
- Optimal staggered testing, i.e., $a = \tau/2$ in Figure 4.1
- Independent testing

If the components are tested independently we can calculate PFD for each component by the formula $\text{PFD}_i = \lambda_i\tau_i/2$ and proceed with the structure function. Due to the independent test regime, it is reasonable to argue that the components are independent, and we proceed with the standard approach which here means to replace x_i in the structure function with $p_i = 1 - \text{PFD}_i$. If common cause failures are relevant, we may add an artificial block to represent the common cause "part" of the components.

It is important to understand the difference between independent *testing* and independent *components*. Independent *testing* means that if we know that one of the component is in a fault

state this will have no information regarding if the other component is in a fault state. This is not true for e.g., simultaneous testing. For simultaneous testing we have: If one component is known to be in a fault state it is more likely that we are at the end of the test interval compared to if it was functioning. Hence, it is also more likely that the other component is in a fault state because the likelihood of being at the end of the test interval is higher. The components performance are dependent not because of any physical reasons, only due to the testing regime.

4.4 RBD-approach

Reliability block diagrams (RBDs) are valuable when we want to visualise the performance of a system comprised of several (binary) components. The basic theory for RBD analysis is introduced in Appendix F.

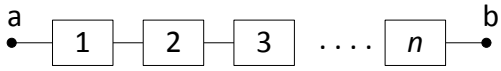


Figure 4.2: Reliability block diagram for a series structure

Figure 4.2 shows the reliability block diagram for a series structure. In general the interpretation of the diagram is that the system is functioning if it is a connection between a and b, i.e., there exists a path of functioning components from a to b. The system is in a fault state (is not functioning) if it does not exist a path of functioning components between a and b.

4.4.1 Structure function

For components we have:

$$x_i(t) = \begin{cases} 1 \text{ if component } i \text{ is functioning at time } t \\ 0 \text{ if component } i \text{ is in a fault state at time } t \end{cases} \tag{4.8}$$

For the system we now introduce

$$\phi(\mathbf{x}, t) = \begin{cases} 1 \text{ if the system is functioning at time } t \\ 0 \text{ if the system is in a fault state (not functioning) at time } t \end{cases} \tag{4.9}$$

ϕ denotes the structure function, and depends on the x_is ($\mathbf{x}$ is a vector of all the x_i's). $\phi(\mathbf{x}, t)$ is thus a mathematical function that uniquely determines whether the system functions or not for a given value of the $\mathbf{x}$ -vector.

To simplify notation we skip the index t in the following.

4.4.2 The structure function for some simple structures

In the following we omit the time dependence from the notation.

For a series structure we have:

$$\phi(\mathbf{x}) = x_1 \cdot x_2 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i$$

For a parallel structure we have

$$\phi(\mathbf{x}) = 1 - (1 - x_1)(1 - x_2)\ldots(1 - x_n) = 1 - \prod_{i=1}^{n}(1 - x_i) = \coprod_{i=1}^{n} x_i$$

Note that we for two components in parallel may simplify:

$$\phi(x_1, x_2) = 1 - (1 - x_1)(1 - x_2) = x_1 + x_2 - x_1 x_2$$

We may combine the results for series and parallel structures to obtain the structure function for more complex structures.

To obtain system reliability we introduce the component reliability metric $p_i(t)$ for component i. There are various ways we can establish the component reliability metric. One way is to consider the probability that the component has survived the time interval $[0, t)$. In this case we usually assume that time-to-failure is exponentially distributed, and we have:

$$p_i(t) = e^{\lambda_i t} \tag{4.10}$$

In other situations we consider the average probability of functioning in an interval or a time period. In this situation p is not depending on time. For components that are proof-tested with interval of length τ we obtain from Equation (4.3):

$$p_i = 1 - \text{PFD}_i \approx 1 - \lambda_i \tau / 2 \tag{4.11}$$

4.4.3 General approach utilizing the structure function

1. Map the physical system into a reliability block diagram or another representation as a starting point

2. Use various approaches (series, parallels, bridges, k-out-of-n's etc) to derive the structure function

3. Multiply out any parentheses, collect terms, and remove any exponents, yielding a structure function as a sum of products

4. The system reliability, $p_S(t)$ is now found by replacing all the x_i's with corresponding $p_i(t)$'s in the sum of product version of the structure function

Note that exponents in the structure function can always be removed because $x^n = x$ for all binary variables. Further exponents shall always be removed since our expectation results above is not valid if there are exponents corresponding to dependent variables, for example $X^2 = X \cdot X$ is the product of the same variable.

Note that the assumption for this approach is that components are stochastically independent. If two or more components are proof tested at the same time, these components will be stochastic dependent if an arbitrary point of time is considered. Therefore the average approach by using $p_i = 1 - \lambda_i \tau/2$ can not be used. In this situation we can calculate $p_S(t)$ for n points of time in the interval $[0, \tau)$ and take the average of these numbers to obtain an approximation for:

$$\text{PFD} = 1 - \frac{1}{\tau} \int_0^\tau p_S(t) dt \tag{4.12}$$

4.5 FTA apporach

A fault tree is a logic diagram that displays the relationships between a potential critical event (accident) in a system and the reasons for this event. The reasons may be environmental conditions, human errors, normal events (events which are expected to occur during the life span of the system) and specific component failures. A properly constructed fault tree provides a good illustration of the various combinations of failures and other events which can lead to a specified critical event. The fault tree is easy to explain to engineers without prior experience of fault tree analysis. Appendix D introduce the required theory for fault tree analysis (FTA).

4.6 The fault tree construction

To construct a fault tree we need:

1. A precise definition of the critical event (the accident) to be analysed.

2. A definition of the boundary conditions for the analysis.

The critical event (accident) to be analysed is called the TOP event. To give the TOP event is given a clear and unambiguous definition should always answer the questions: **What, where** and **when**?

What: Describes what type of critical event (accident) is occurring, e.g., collision between two trains.

Where: Describes where the critical event occurs, e.g., on a single track section.

When: Describes when the critical event occurs, e.g., during normal operation.

When the TOP event is defined start developing the fault tree by asking what are the direct reasons for the TOP event to occur. We combine those causes by logical gates, i.e.,:

- An AND gate if all direct reasons have to occur in order to have the TOP event occurring
- An OR gate if one or more of the direct reasons will lead to the TOP event
- An $k$oo$n$ gate if k or more of the n direct reasons will lead to the TOP event

Then we proceed to investigate each of the direct causes, i.e., gates, and proceed in the same way. The analysis is in other words deductive and is carried out by repeated asking "What are the reasons for...?"

4.6.1 Qualitative analysis

A fault tree provides valuable information about possible combinations of fault events which can result in a critical failure (TOP event) of the system. Such a combination of fault events is called a cut set.

*A**cut set** in a fault tree is a set of Basic events whose (simultaneous) occurrence ensures that the TOP event occurs. A cut set is said to be **minimal** if the set cannot be reduced without loosing its status as a cut set.*

Computer codes exist to obtain the minimal cut sets. In this course we do not expect the students being able to find the minimal cut sets, but if they are given, the students should be able to explain each of the cut set based on the fault tree diagram.

Cut sets with only one component are very critical cut sets since there are no barriers to prevent the TOP event to occur if there is a component failure.

4.6.2 Quantitative analysis

In the quantitative part of a fault tree analysis the main objective is to calculate the following metrics:

- $Q_0(t)$ = Probability that the TOP-event occurs at time t
- $F_0(t)$ = Expected number of TOP-event occurrence per unit time at time t
- $I(i \mid t)$ = Importance metric for basic event i at time t

In this course we only focus on $Q_0(t)$. The approach for calculating $Q_0(t)$ is the following:

- Find the cut set contribution to $Q_0(t)$ for each cut set

- Add the cut set contributions

The probability that cut set number j is occurring at time t is found by:

$$\check{Q}_j(t) = \prod_{i \in K_j} q_i(t) \tag{4.13}$$

where $q_i(t)$ is the probability that component i is in a fault state at time t. For PFD calculations we usually consider time-to-failure to be exponentially distributed, and we have

$$q_i(t) = 1 - e^{\lambda_i t} \tag{4.14}$$

The TOP event probability is then found by:

$$Q_0(t) \approx \sum_{j=1}^{k} \check{Q}_j(t) \tag{4.15}$$

where k is the number of minimal cut sets.

4.6.3 PFD calculations

As for the RBD analysis, we can take the average of $Q_0(t)$ to obtain the PFD:

$$\text{PFD} = \frac{1}{\tau} \int_0^{\tau} Q_0(t)\, dt \tag{4.16}$$

4.7 Common cause failures

The equation above assumes that components in a SIS fail independent of each other. In practice components may fail due to common causes. Common cause failure may be due to maintenance introduced failures, design failures, excessive stress etc. To model common cause failures the total failure rate of one component (i.e., rate of DU failures) is split into an independent part and a dependent part:

$$\lambda = \lambda_{(i)} + \lambda_{(c)} = (1 - \beta)\lambda + \beta\lambda \tag{4.17}$$

where $\beta = \lambda_{(c)} / \lambda$ is the common cause factor. This (beta factor) model now yields:

- For the dependent part, use PFD = $\frac{\beta\lambda\tau}{2}$
- For the independent part, use the independent failure rate $(1-\beta)\lambda$ in the PFD formulas of the $k$oo$n$ system of identical and independent components

- Add the contributions:

$$\text{PFD} = \frac{\beta\lambda\tau}{2} + \binom{n}{n-k+1}\frac{\left[(1-\beta)\lambda\tau\right]^{n-k+1}}{n-k+2} \tag{4.18}$$

4.8 The PDS method

The PDS method is developed by SINTEF Safety. The method has two main features:

1. It proposes a more realistic way to model common cause failures (CCF). In the β-factor model a CFF will always cause all components to fail. This is often not realistic. The PDS method therefore proposes a correction factor to adjust the β-factor to account for the situation where not all components fail due to the CCF situation.

2. In IEC 61508 only random hardware failures are quantified. The PDS method also quantifies systematic failures by the so-called test independent failure term, p_{TIF}. Systematic failures are not treated in this presentation.

The idea behind adjusting the β-factor is that if we have a CFF causing two components to fail, it is not certain that the remaining components will fail. Some assumptions are then made regarding the probability that a third component fails given that two components have failed due to a CFF and so on. The correction factor is dependent on k and n, and is generally denoted C_{koon}, and is presented in Table 4.1 for some combinations:

Table 4.1: C_{koon} correction factors

$k \backslash n$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
$k=1$	$C_{\text{1oo2}}=1.0$	$C_{\text{1oo3}}=0.5$	$C_{\text{1oo4}}=0.3$	$C_{\text{1oo5}}=0.20$	$C_{\text{1oo6}}=0.15$
$k=2$	-	$C_{\text{2oo3}}=2.0$	$C_{\text{2oo4}}=1.1$	$C_{\text{2oo5}}=0.8$	$C_{\text{2oo6}}=0.6$
$k=3$	-	-	$C_{\text{3oo4}}=2.8$	$C_{\text{3oo5}}=1.6$	$C_{\text{3oo6}}=1.2$
$k=4$	-	-	-	$C_{\text{4oo5}}=3.6$	$C_{\text{4oo6}}=1.9$
$k=5$	-	-	-	-	$C_{\text{5oo6}}=4.5$

A configuration specific β-factor is now calculated by multiplying the original β-factor with the correction factor C_{koon} found in Table 4.1. Note that the baseline β-factor is assumed to be specified for a 1oo2 system.

4.9 PFH calculations

In the following we present the simple approximation formula proposed in the PDS method for the probability of failure per hour, PFH:

$$\text{PFH} = C_{\text{koon}}\beta\lambda + \frac{n![\lambda(1-\beta)\tau]^{n-k+1}}{(n-k+1)!(k-1)!\tau} \tag{4.19}$$

Note that the correction factor C_{koon} only applies for the PDS method. To obtain eq. (4.19) we treat CCF failures and independent failures individually. For the CCF failures the results is rather obvious. For independent failures, let $p(t,k,n)$ be the probability that the first $n-k$ components are in a fault state assuming they are numbered $1,2,\ldots,n$. If the the first $n-k$ components are in a fault state and the remaining k components are functioning, then they are *critical*. A system failure will occur if one of remaining k components fails. We have that $p(t,k,n) \approx \left[\lambda(1-\beta)t\right]^{n-k}$. To find the contribution to the PFH for this situation we calculate the average of $p(t,k,n)$ in a proof test period, and multiply with $f_k = k\lambda(1-\beta)$. f_k is the total frequency of the event that one of the remaining k components fails. The above argument is valid when we consider the numbered $n-k$ components. There are $\binom{n}{n-k} = \frac{n!}{(n-k)!k!}$ ways to chose $n-k$ components, and adding up we obtain eq. (4.19). Note that the probability that the k remaining components being in a *functioning* state is considered to be close to one, so we do not take this into account.

4.10 STR calculations

In the following we present the simple approximation formula proposed in the PDS method for the spurious trip rate, STR:

$$\text{STR} = C_{(\text{n-k+1})\text{oon}}\beta\lambda_{\text{SU}}$$

Note that the correction factor $C_{(\text{n-k+1})\text{oon}}$ only applies for the PDS method. We have here explicitly indicated that the failure rate to go into the formula is the rate of SU failures. In some presentations λ_{SO} is used to reflect the rate of spurious operations on component level.

4.11 Markov approach

We have seen that the Markov equations may be written on matrix form:

$$\mathbf{P}(t)\cdot\mathbf{A} = \dot{\mathbf{P}}(t) \tag{4.20}$$

which may be approximated by:

$$\dot{\mathbf{P}}(t) = \frac{\mathbf{P}(t+\Delta t) - \mathbf{P}(t)}{\Delta t} = \mathbf{P}(t) \cdot \mathbf{A} \tag{4.21}$$

yielding

$$\mathbf{P}(t+\Delta t) = \mathbf{P}(t)[\mathbf{A}\Delta t + \mathbf{I}] \tag{4.22}$$

where $\mathbf{I}$ is the identity matrix. This equation may now be used iteratively with a sufficient small time interval Δt and starting point $\mathbf{P}(0)$ to find the time dependent solution. Only simple matrix multiplication is required for this approach.

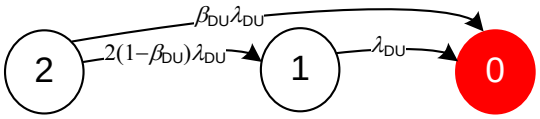
4.11.1 PFD

Assume that we know the state vector $\mathbf{P}(0)$ just after a proof test, and that we have established a Markov transition model for the SIS with respect to a given SIF. Then it is straight forward to find $\mathbf{P}(t)$ within a proof test interval by the approach presented above. Typically the probability of being in a state where all components are functioning (state r) is assumed to be one, and probabilities for the other states are equal to zero. Let F be the set of failed states with respect to the actual safety function of the SIS. We then have:

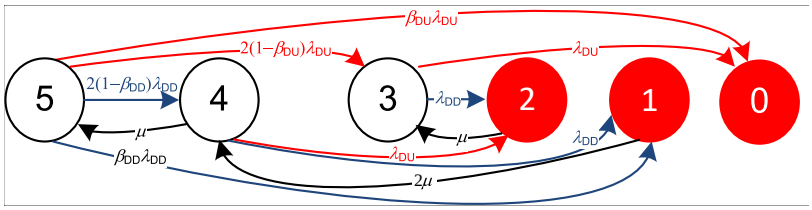
$$\text{PFD} = \frac{1}{\tau}\int_0^\tau \text{PFD}(t)\,dt = \frac{1}{\tau}\int_0^\tau \sum_{i\in F} P_i(t)\,dt \tag{4.23}$$

The integral is replaced by a sum in the numerical calculations since we are already solving the time dependent solution iteratively by time steps Δt.

The following figure shows the Markov diagram for a 1oo2 system considering DU-failures only:



Note that whereas the closed form formulas for PFD presented earlier only takes DU failures into account. With the Markov approach, DD failures may also be included. The Markov diagram for the 1oo2 systems now reads:



where the following system states are defined:

5: Both components OK

4: One OK, one DD-failure

3: One OK, one DU-failure

2: One DU-failure and one DD-failure

1: Two DD-failures

0: Two DU-failures

Red arrows are DU failures, blue arrows are DD failures, and black arrows are repairs.

4.11.2 PFH

The procedure is now similar to the approach for PFD, but we are seeking a rate, i.e., the rate of transition from a functioning state to a fault state for the SIS safety function is found by averaging:

$$\text{PFH} = \frac{1}{\tau}\int_0^\tau \text{PFH}(t)dt = \frac{1}{\tau}\int_0^\tau \sum_{i\notin F}\sum_{j\in F} a_{ij}P_i(t)dt \tag{4.24}$$

where a_{ij} is the transition rate from state i to state j measured in expected number of transitions *per hour*. Note that we can interchange the integration and summation operators, i.e., we may first calculate the average state probabilities, then calculate the appropriate transition rates.

4.11.3 STR

The procedure for the spurious trip rate is now similar to the approach for PFH, but we need to consider the spurious trip system failure mode. Therefore, we typically need to draw a new Markov diagram. Let F be the set of system failure states representing a spurious trip state. STR is found by averaging:

$$\text{STR} = \frac{1}{\tau}\int_0^\tau \text{STR}(t)dt = \frac{1}{\tau}\int_0^\tau \sum_{i\notin F}\sum_{j\in F} a_{ij}P_i(t)dt \tag{4.25}$$